Jurnal The Messenger, Vol. 17, No. 3 (2025), pp. 293-315
P-ISSN: 2086-1559, E-ISSN: 2527-2810
DOI: 10.26623/themessenger.v17i3.11648

Knowledge, Attitudes, and Practices towards Personal Data Protection in Social Media among Indonesian College Students

Rulli Nasrullah[1], Oktaviana Purnamasari[2], Tria Patrianti [3], Makroen Sanjaya[4], Study Rizal Lolombulan Kontu[5], Jumroni[6]

[1]ORCID iD: 0000-0002-9856-2671, Syarif Hidayatullah State Islamic University of Jakarta, Jl. Ir. Djuanda No. 95, South Tangerang, Banten 15412, Indonesia
[2]ORCID iD: 0000-0003-2536-1235, Universitas Muhammadiyah Jakarta, Jl. K.H. Ahmad Dahlan, South Tangerang, Banten 15419, Indonesia
[3]ORCID iD: 0000-0002-1897-233X, Universitas Muhammadiyah Jakarta, Jl. K.H. Ahmad Dahlan, South Tangerang, Banten 15419, Indonesia
[4]ORCID iD: 0000-0002-1836-8757, Universitas Muhammadiyah Jakarta, Jl. K.H. Ahmad Dahlan, South Tangerang, Banten 15419, Indonesia
[5]ORCID iD: 0009-0005-6994-1639, Syarif Hidayatullah State Islamic University of Jakarta, Jl. Ir. Djuanda No. 95, South Tangerang, Banten 15412, Indonesia
[6]ORCID iD: 0000-0003-4835-9947, Syarif Hidayatullah State Islamic University of Jakarta, Jl. Ir. Djuanda No. 95, South Tangerang, Banten 15412, Indonesia
*Corresponding author, e-mail: rulli.nasrullah@uinjakarta.ac.id

Abstract

Purpose: This study examines the awareness of Indonesian college students from diverse regions regarding personal data protection, focusing on the dimensions of knowledge, attitudes, and practices. The research is exploratory in nature and does not aim to generalize findings beyond the studied cases.

Methods: A purposive sampling technique was employed in this study. Given the unknown population size, an infinite sample formula was applied with the assumption p=0.5 and 95% confidence interval. With a margin of error of ±5.43%, the final sample consisted of 325 respondents. The survey measured three variables: knowledge, attitudes, and practices related to personal data protection. College students were chosen as they are the most active social media users and vulnerable to data sharing, with the sample providing demographic diversity and a representative overview of personal data protection awareness.

Findings: Results reveal a persistent lack of understanding among Indonesian college students regarding personal data protection. Most respondents expressed little concern about publishing personal information on social media, with many continuing to share personal data despite potential risks.

Originality: This study advances theoretical novelty by integrating Social Information Processing Theory with identity fluidity to explain students' disclosure of personal data on social media despite existing legal safeguards. Unlike prior research that focused primarily on global privacy paradoxes or platform-specific behaviors, it situates the analysis within Indonesia's regulatory context, thereby exposing the gap between law and practice and enriching discourse on digital literacy and mediated identity.

Keywords: Personal Data, Social Media, New Media, Digital Literacy.

Introduction

This research is essential because social media allows anyone to upload personal data, which may be confidential. This condition is directly or indirectly one of the considerations for the emergence of regulations related to personal data. Regulations related to personal data protection were issued through Law Number 27 of 2022. This law

Article History: *Received January 29, 2025; Revised June 21, 2025; Accepted December 24, 2025; Published December 31, 2025.*

was passed on October 17, 2022 and came into full effect on October 17, 2024, after a transition period. This regulation is a response to the many cases of personal data leakage on the internet and also serves as a legal basis for individuals and institutions that manage personal data on the internet.

The issue of personal data became a trending topic on the internet after millions of Indonesians' data were found and sold in various marketplaces. Even during 2022 alone, seven significant cases related to the sale and purchase of personal data (Nurhadi, 2022). One is data from patients and Covid-19 test results containing full names, hospitals, patient photos, and X-ray scans with a document size of 720 GB. The leak also hit state-owned companies such as Pertamina, and customer data from PLN (*Perusahaan Listrik Negara*) or the State Electricity Company customer data.

Apart from the security issues on the platform created by the Government, for example, on the *Peduli Lindungi* platform as an application that must be used by Indonesian residents during the Covid-19 pandemic even today, the issue of personal data is one of the severe problems on the internet, especially with the presence of social media (Adjei et al., 2020; Couldry & van Dijck, 2015; Luceri et al., 2020; Osatuyi, 2015; Sarikakis & Winter, 2017; Stoilova et al., 2021). Jordan (1999) even mentioned that the internet is a flood of information (Dyer-witheford, 2010; Hesmondhalgh, 2010; Ritzer & Jurgenson, 2010). Social media operates as an open arena accessible to all, where user-generated content--whether intentionally or unintentionally shared--frequently contains personal data. Such information not only becomes easily constructed and accessed by others but also risks commodification, transforming personal identity into exploitable digital assets within the broader information economy (Barabasi, 2011; Castells, 2010; Nasrullah, 2014; Papacharisi, 2011).

Social media constitutes a contemporary communication medium that facilitates user interaction and the dissemination of information through user-generated content even in the context of digital journalism practice (Barnes et al., 2018; Krebs & Lischka, 2019; Ksiazek, 2018; Nah et al., 2017; O'Regan, 2021; Soffer & Gordoni, 2018; Tenenboim, 2022). At the same time, it transforms such content into an economic commodity, positioning personal data and identity markers as assets within the digital information economy (Boyd, 2009; Mandiberg, 2012) to form a social network or community (Blanchard & Horan, 1998; Epstein & Klinkenberg, 2002; Matei, 2005; Van Dijk, 2006). It is important to recognize that social media platforms fundamentally operate on information, like personal identity, voluntarily uploaded by users themselves (Bayer et al., 2016; Goodell & Aste, 2019; Han et al., 2023; Hölbl et al., 2015; Seidman, 2013; Zhu & Xiong, 2022). This user-driven structure not only facilitates interaction and community formation but also creates significant vulnerabilities, as personal data embedded in user-generated content becomes accessible to third parties. In many cases, such information is commodified, transforming individual identity markers into exploitable assets within the digital economy and raising critical concerns regarding privacy, surveillance, and regulatory enforcement (Castells, 2010; Gane & Beer, 2008). The information then becomes raw material or commodity on social media itself. Meikle (2016) characterizes social media as 'the sharing industry,' where user-uploaded information is commodified and circulated across networks. This dynamic underscores the urgent need for robust online security, particularly as many users--especially children--remain unaware that their personal data can be exploited for criminal purposes. Such vulnerabilities highlight the critical role of regulatory frameworks, including Indonesia's Personal Data Protection Law (Regulation No. 27 of 2022), in safeguarding digital

identities and mitigating risks associated with oversharing in mediated environments (Stoilova et al., 2021).

The fundamental problem is that the information uploaded on social media by users can be categorised as personal. It started from clear names, home addresses, and educational information to publications that are videos or photos related to individual activities. In the context of personal data information and social media as new media, Jordan (1999) asserts that one of the cultures that emerged in this internet era is 'identity fluidity.' Although this mention affirms that it is a process of identity being constructed, the published identity is not necessarily a reflection of offline identity. In fact, on social media, personal data or information of users becomes open or can be easily found (Adjei et al., 2020; Bruns et al., 2013; Costera Meijer & Groot Kormelink, 2015; Hille & Bakker, 2014). Identity is understood as a social construction. On the internet, identity takes the form of text, the structure of words/sentences, identity descriptions, avatars, images, and virtual bodies in interactive games. According to Wood and Smith (2005), text-based media have introduced new forms of forums for identity communication. The experiences derived from engaging with these media highlight the ways in which identities are constructed and reveal how individuals complicitly articulate themselves within mediated environments.

The different environment of computer-mediated communication then provides a kind of shift in how we view the characteristics and relationships between individuals. As computer and internet users, identities are mainly presented through text alone, so how one constructs oneself and how other users perceive one depends on the text itself. In many cases, perceptions can result in different identities depending on how much the text provides the information that is constructed/needed. This perception is then based on what is called 'telepresence' (Wood & Smith, 2005). This concept refers to an idea to indicate that the audience is in cyberspace or 'being there'. Telepresence is a level of presence in a mediated environment rather than a physical environment. A person has the power to organise/control identity construction through the choice of identifiers reflected through the internet. The basis of this concept is how vividly the audience represents itself and the choice of medium in interaction that can be felt in reality based on the stimuli presented in cyber media. However, as Turkle (1995) explains, in a computer-mediated world, the self can be anyone and multiply, change, and be shaped through interactions involving machine connections and transformed through language. It happens because, in the online world, someone can be anyone, with a different image and representation than offline (Driscoll & Gregg, 2010; Katie J. Ward, 1999; Methodology, 2014; Schroeder, 1994).

Cyberspace generates expansive public arenas that foster citizen participation beyond traditional boundaries. The notion of public space on the internet has often been likened to that of a nation, where collective engagement shapes shared meanings. As Castells observes, individual communication through social networking platforms produces 'communal identities', analogous to the way citizens constitute the identity of a nation (Castells, 2007). However, this does not mean that a nation or state disappears with the emergence of this communal identity. The redefinition of the public sphere and the medium of the internet, which mediates between individuals and communities in large numbers, provides a new depiction of what is meant by identities based on communalism and individualism.

Across many societies, the tension between communalism and individualism shapes cultural identity as a process of construction intertwined with historical and geographical contexts as well as the formation of individual subjects. Communal culture

is grounded in collective markers such as religion, nation, territory, ethnicity, gender, and environment. In contrast, individualist culture emerges through consumerist practices, new forms of association within individualist networks, and the pursuit of personal autonomy in defining one's place in life (Castells, 2007).

Related to identity, Wood and Smith (2005) offer two types of identity in interacting on the internet apart from the identity in the real world (Real-Life Identity): Pseudonymity and Anonymity. Anonymity is a new form of identity that is entirely separate and cannot be referred to as who the identity belongs to. This identity model was initially used for those who placed dating advertisements in the print media, as a reporter of criminal acts to the authorities, or actions that require a hidden identity. For Monica Whitty and Adam Johnson (2009), anonymous identity manifests in several distinct effects, the first being visual anonymity, which refers to the reduction of identifiable cues during interaction and the attempt to minimize vulnerability through limited recognition. This condition illustrates how online audiences exercise control over their digital appearance, often engaging in gradual self-disclosure as relationships develop. On social media, for instance, new connections are frequently established with minimal background identification, and uncertainty reduction in computer-mediated communication occurs through progressive levels of self-disclosure, beginning with anonymity and expanding through ongoing exchanges of questions and answers. In contrast, pseudonymity blurs the boundaries of original identity, sometimes producing fabricated personas while in other cases still reflecting aspects of a user's true self. Unlike complete anonymity, pseudonymity allows individuals to adopt alternative identities, effectively becoming someone else in mediated environments. A notable example is gender-swapping, where users deliberately exchange social identities based on gender differences, demonstrating the fluidity and performative nature of identity construction in digital spaces (Wood & Smith, 2005) Therefore, it is essential to know digital literacy, especially regarding data usage. The amount of information related to personal data uploaded either intentionally or unintentionally on social media provides a kind of false awareness to users that their personal data will be safe. In fact, according to Pangrazio and Selwyn (2019), social media platform providers or other parties can collect this personal data.

The many cases of personal data leaks on the internet are one of the reasons why the Indonesian Government issued Regulation No. 27 of 2022 concerning Personal Data Protection, inaugurated on October 17, 2022, including the behaviour of users who deliberately upload personal information on social media accounts. This regulation not only explains the definition of what personal data is to the misuse of personal data but also discusses the category of personal data itself that should be of concern to citizens including the possibility of its misuse. The regulation is not only aimed at individuals or institutions regarding the publication, use and storage of personal data but also provides a kind of awareness to citizens about personal data and the risks that may arise from deliberately publishing personal data.

However, these regulations will not be effective if there is a lack of digital literacy from social media users themselves (Fang & Nie, 2022; Kang et al., 2023; Milenkova & Lendzhova, 2021). Various cases seem very easy to find when looking at one publication after another on social media (Drury et al., 2022). Age, occupation, family, education, and even health data in text, photos, and videos are easy to find on social media. This context occurs due to social media users' lack of understanding of digital literacy. This context occurs due to social media users' lack of digital literacy knowledge (Munger et al., 2021; Park, 2013; Pietrass, 2007; Stoilova et al., 2021).

The novelty of this study lies in its positioning as one of the earliest empirical investigations into the implications of Indonesia's newly enacted Regulation No. 27 of 2022 on Personal Data Protection. While previous scholarship has largely focused on global perspectives of privacy, cybercrime, or platform governance, this research uniquely applies the Knowledge, Attitudes and Practices (KAP) framework to the Indonesian context, specifically targeting college students as a digitally active demographic. By adapting a model widely used in health and pandemic studies to the field of communication and digital literacy, the study introduces a methodological innovation that bridges disciplines and offers fresh insights into how regulatory awareness translates into everyday online behavior.

KAP is a quantitative research model developed by Zhong et al. (2020) to see how the Chinese population behaved during the development of Covid-19. This survey then became popular in the health sector to find information, for example, in mental health, how a person believes and behaves towards an illness or during therapy for the disease itself (Andrade et al., 2020). Several studies using this model are related to the Covid-19 pandemic in various populations, such as Malaysia (Mat Din et al., 2020), Indonesia (Sulistyawati et al., 2021), Ethiopia (Bukata et al., 2022), Venezuela (Bates et al., 2021), Central Nigeria (R. C. Reuben et al., 2021), and South Korea (Lee et al., 2021). This KAP model has previously been used to examine pandemic situations such as Lassa fever in and around Lafia, Central Nigeria (C. R. Reuben & Gyar, 2016). Not only that, the KAP model for Badran (1995) can also be used as a pillar in health professional practice, including for nursing students (Etokidem et al., 2018).

Methods

In the context of this research, the KAP model is used, along with statistical calculations, to see how respondents from across Indonesia respond to personal data protection on social media. All the data are analysed based on the respondents' answers to various questions. Binary logistic regression was used to identify demographic factors associated with each attitude and practice. Afterwards, Odds ratios (ORs) were used to assess the relations between variables with knowledge-attitude-practice. With a purposive sampling technique, the population size in this study is unknown and uses an infinite sample formula with the assumption p=0.5 and CI (Confidence Interval) 95%. With a margin of error of ±5.43%, the sample size is 325 respondents (Krejcie & Morgan, 1970; Wang et al., 2023). Since the population of Indonesian college students actively using social media is unknown, this approach ensures a sufficiently large sample to produce reliable estimates and enables inferential analysis such as logistic regression with adequate confidence. College students were selected as respondents because they are the group most active on social media and most vulnerable to personal data sharing practices. By involving 325 students from various provinces, the study captures demographic diversity (age, educational status, occupation, and marital status), allowing analysis of differences in knowledge, attitudes, and practices across socio-demographic variables, while positioning students as a strategic target for digital literacy. As an exploratory study, the sample of 325 respondents is considered sufficiently representative to provide an initial overview of students' awareness of personal data protection. This number is realistic to collect within a limited research period, yet large enough to yield valid data and enable in-depth quantitative analysis, thereby balancing resource constraints with academic requirements.

The KAP model is important in this study because it provides a comprehensive analytical framework for understanding how Indonesian students perceive personal data protection on social media, not only in terms of normative knowledge about regulation but also in relation to the attitudes and actual behaviors they demonstrate in everyday online activities. By positioning knowledge as the foundation, KAP allows researchers to assess the extent to which students are familiar with Law No. 27 of 2022 on Personal Data Protection; through the attitude dimension, the model reveals perceptions, awareness, and levels of concern regarding data leakage risks; while the practice dimension highlights actual habits of sharing or protecting personal information on social media. This approach is relevant because the gap between knowledge, attitudes, and practices often serves as a key indicator of weak digital literacy and regulatory effectiveness. Thus, KAP functions not only as a behavioral measurement tool but also as a methodological bridge that connects communication theory, digital literacy concepts, and data protection policy with the empirical realities of students as the most active yet most vulnerable demographic to personal data exploitation.

Results

This cross-sectional survey was conducted by distributing questionnaires to students from various universities in almost all parts of Indonesia from November 16 to December 17, 2022. Of these, 325 respondents filled out and collected the questionnaires. The geographical origin of the informants is as follows (Figure 1). In addition to the criteria that informants come from universities, the requirements set by this study also require ownership of social media accounts.

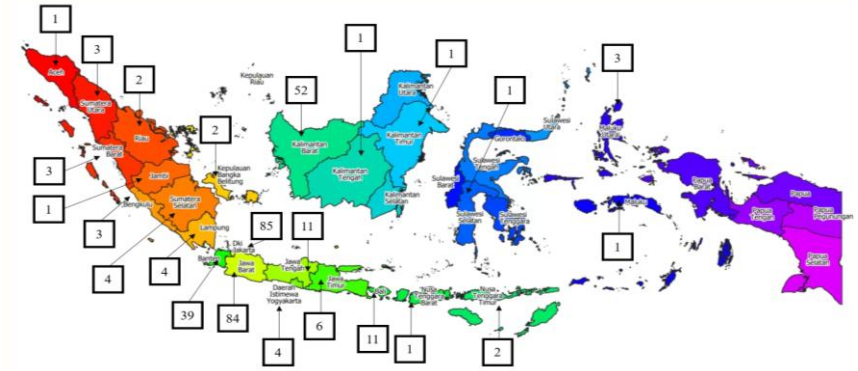

Figure 1. Maps of Indonesia and the colours represent the provinces. The number shows how many respondents are from each province
(source: derived from the collected research data)

Measures

The questionnaire consisted of two parts: demographics and KAP. Demographic variables included age, gender, marital status, place of current residence, college student level, and occupation. According to government regulation No. 27 of 2022 on Personal Data Protection, the authors developed the first part, questions related to personal data protection knowledge. Answers to questions about knowledge are given three options, ranging from correct, incorrect, and the alternative explanation like I don't know. As for the attitude and practices category, the second part was given with two answers: true and false.

There were ten questions in the knowledge category: 5 questions related to information and types of personal data (K1-K5) and five questions related to the

prohibition of private data publication and its legal impact (K6-K10). Attitudes are represented by two inquiries (A1-A4) associated with publishing personal data on social media. Practices are related to the habit of posting personal data (P1-P2), both personal data and personal data of family or close people (see Table 1).

Table 1. Questionnaire of KAP towards personal data protection

Questions	Options
Knowledge (K)	
K1: The Government has issued a regulation regarding personal data protection on Law No. 27 of 2022 on Personal Data Protection.	True, false, I don't know
K2: Personal data is data regarding an individual that are/can be identified as it is or combined with other information either directly or indirectly through an electronic or non-electronic system.	True, false, I don't know
K3: Subject of Personal Data is an individual who is attached to Personal Data.	True, false, I don't know
K4: Specific personal data such as medical, genetic, criminal, or financial data.	True, false, I don't know
K5: General personal data such as full name, gender, nationality, religion, or marital status.	True, false, I don't know
K6: Each person is prohibited, as it is against the law, from obtaining or collecting other individuals' Personal Data with self-advantageous intention or to put Subject of Personal Data in an unfavorable situation.	True, false, I don't know
K7: Each person is prohibited from revealing Personal Data that is not their own as it is against the law.	True, false, I don't know
K8: Each person is prohibited to create fake or forge Personal Data with self-serving intention or to cause harm to others.	True, false, I don't know
K9: Dispute settlements regarding personal data protection conducted through arbitration, court, or other alternative dispute settlement institution in accordance with the provision of the legislation.	True, false, I don't know
K10: Each person who is using personal data, especially data that is not their own or fake can subject to criminal sanctions in the form of prison or criminal fines.	True, false, I don't know
Attitudes (A)	
A1: You have accidentally or intentionally published specific personal data such as medical, genetic, criminal, or financial data on social media.	Yes, No
A2: You have accidentally or intentionally published general personal data such as full name, gender, nationality, religion, or marital status on social media.	Yes, No
A3: Do you agree if published personal data on social media can be misused by others for digital crime?	Yes, No

A4: Are you confident that your personal data is not shown on a private social media account?	Yes, No
Practices (P)	
P1: In the future, will you not publish personal data on private social media account?	Yes, No
P2: In the future, will you protect your core family's personal data to keep them off from published on a private social media account?	Yes, No

Note: a matrix of questions derived from the elaboration of KAP categories from Researcher

Respondents were gathered from the spread of areas, as seen in Figure 1. The highest number of respondents based on age are those at age <20 (46.8%) and 21-29 (40.9%). Meanwhile, based on educational status, from diploma to doctoral, the highest number of respondents are taken by those pursuing an undergraduate with 262 respondents or 80.6%. Lastly, those who have unemployment status are the ones with the highest amount of respondents, with 220 people or 67.7% as Table 2 below:

Table 2. Socio-demographic characteristics of Indonesian college student participants

Variables	Categories	Number	Percent
Sex	Male	130	40%
	Female	195	60%
	Total	325	
Age in years	<20	152	46.8%
	21-29	133	40.9%
	30-39	21	6.5%
	40-49	12	3.7%
	≥50	7	2.2%
	Total	325	
Marital status	Single	277	85.2%
	Married	47	14.5%
	Divorced/separated	1	0.3%
	Total	325	
Student Status	Diploma	10	3.1%
	Undergraduate	262	80.6%
	Postgraduate/Master	32	9.8%
	Doctoral	21	6.5%
	Total	325	
Occupation Scope	Unemployed/Independent	220	67.7%
	Worker	7	2.2%
	Government Sector	21	6.5%
	Private Sector	40	12.3%
	Freelance	37	11.4%
	Total	325	

Note: Processed from the results of the answers of research respondents

Respondents' ownership of social media is shown in Figure 2. It shows that the average respondent has at least three social media accounts: Facebook, Instagram, YouTube, Twitter, or TikTok. The Figure 2 also shows that the respondents are accustomed to using social media.

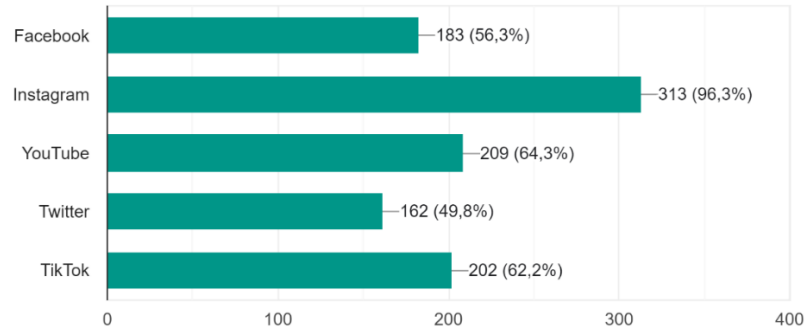

Figure 2: Social media account of the participant (source: Processed from the results of the answers of research Respondents)

The following is a summary of respondents' answers regarding questions about knowledge aspects according to government regulations in Law No. 27 of 2022 on Personal Data Protection. Questions taken from parts of the regulations, if compared with the respondents' answers, show that most of them understood the context of the regulation. The lowest amount on one of the knowledge questions is at 75.1% or 244 respondents; meanwhile, the highest is at 95.7% or 311 respondents (Table 3).

Table 3. Questionnaire of knowledge towards personal data protection

Questions	Response categories	Number	Per cent
The Government has issued a regulation regarding personal data protection on Law No. 27 of 2022 on Personal Data Protection.	True	286	88%
	False	3	0.9%
	I don't know	36	11.1%
Personal data is data regarding an individual that are/can be identified as it is or combined with other information either directly or indirectly through an electronic or non-electronic system.	True	296	91.1%
	False	3	0.9%
	I don't know	26	8%
The subject of Personal Data is an individual who is attached to Personal Data.	True	309	95.1%
	False	4	1.2%
	I don't know	12	3.7%
Specific personal data such as medical, genetic, criminal, or financial data.	True	249	76.6%
	False	28	8.6%
General personal data such as full name, gender, nationality, religion, or marital status.	I don't know	48	14.8%
Each person is prohibited, as it is against the law, from obtaining or collecting other individuals' Personal Data with self-advantageous intention or to put Subject of Personal Data in an unfavourable situation.	True	295	90.8%
	False	23	7.1%
	I don't know	7	2.2%
Each person is prohibited from revealing Personal Data that is not their own as it is against the law.	True	301	92.6%
	False	8	2.5%
	I don't know	16	4.9%

Each person is prohibited to create fake or forge Personal Data with self-serving intention or to cause harm to others.	True	291	89.5%
	False	11	3.4%
	I don't know	23	7.1%
Dispute settlements regarding personal data protection conducted through arbitration, court, or other alternative dispute settlement institution in accordance with the provision of the legislation.	True	311	95.7%
	False	5	1.5%
	I don't know	9	2.8%
Each person who is using personal data, especially data that is not their own or fake can subject to criminal sanctions in the form of prison or criminal fines.	True	244	75.1%
	False	6	1.8%
	I don't know	75	23.1%
Each person who is using personal data, especially data that is not their own or fake can subject to criminal sanctions in the form of prison or criminal fines.	True	290	89.2%
	False	5	1.5%
	I don't know	30	9.2%

Note: Processed from the results of the answers of research respondents

On the other hand, answers' frequency regarding questions about attitudes can be seen in the Table 4 below:

Table 4. Questionnaire of attitudes towards personal data protection

Questions	Response categories	Number	Percent
You have accidentally or intentionally published specific personal data such as medical, genetic, criminal, or financial data on social media.	Yes	90	27.7%
	No	235	43.7%
You have accidentally or intentionally published general personal data such as full name, gender, nationality, religion, or marital status on social media.	Yes	199	61.2%
	No	126	38.7%
Do you agree if published personal data on social media can be misused by others for digital crime?	Yes	251	77.2%
	No	74	22.8%
Are you confident that your personal data is not shown on private social media account?	Yes	104	32%
	No	221	68%

Note: Processed from the results of the answers of research respondents

On the other hand, answers' frequency regarding questions about practices can be seen in the Table 5 below:

Table 5. Questionnaire of practices towards personal data protection

Questions	Response categories	Number	Percent
In the future, will you not publish personal data on a private social media account?	Yes	283	87.1%
	No	42	12.9%

In the future, will you protect your core family's personal data to keep them from being published on private social media account?	Yes	321	98.8%
	No	4	1.2%

Note: Processed from the results of the answers of research respondents

In this section, aggregation was conducted for all the answers to each question about Attitude and cross-tabulation was conducted for demographic variables. In Table 6, by percentage (%), more females answered Yes than males. Based on age range, those who answered Yes had the highest percentage (%) in the age group >50 years. Meanwhile, those who are married are the ones who mostly answered Yes, making them the highest percentage out of others based on marital status. The highest percentages (%) of people who answered Yes based on student status are the ones with diplomas, while the highest percentages based on occupation status are freelancers.

Table 6. Odds Ratio Demographic Variable towards Attitude

		No	Yes	AOR (CI 95%)
Sex	Female	136 (69.74)	59 (30.26)	1
	Male	98 (75.38)	32 (24.62)	0.813 (0.804, 2.196)
Age	<20	111 (73.03)	41 (26.97)	1
	21-29	96 (72.18)	37 (27.82)	1.043 (0.619, 1.758)
	30-39	14 (66.67)	7 (33.33)	1.354 (0.51, 3.59)
	40-49	10 (83.33)	2 (16.67)	0.541 (0.114, 2.576)
	>50	3 (42.86)	4 (57.14)	3.61 (0.774, 16.825)
Marital Status	Single	200 (72.2)	77 (27.8)	1
	Married	33 (70.21)	14 (29.79)	1.102 (0.559, 2.171)
	Divorced	1 (100)	0 (0)	0 (0.000, 0.000)
Student Status	Diploma	5 (50)	5 (50)	1
	Undergraduate	192 (73.28)	70 (26.72)	0.365 (0.102, 1.297)
	Postgraduate/Master	23 (71.88)	9 (28.13)	0.391 (0.091, 1.684)
	Doctoral	14 (66.67)	7 (33.33)	0.500 (0.108, 2.323)
Occupation Scope	Unemployed	160 (72.73)	60 (27.27)	1
	Freelance	24 (64.86)	13 (35.14)	1.444 (0.691, 3.019)
	Independent Worker	6 (85.71)	1 (14.29)	0.444 (0.052, 3.769)
	Private Sector	26 (65)	14 (35)	1.436 (0.703, 2.933)
	Government Sector	18 (85.71)	3 (14.29)	0.444 (0.126, 1.563)

Note: AOR (Adjusted Odds Ratio), Processed from the results of the answers of research respondents

Based on the odds ratio values obtained from the partial test output (Table 6), notable differences emerge across predictor variables in relation to Attitude. Male respondents were 0.813 times as likely as females to answer *"Yes."* Respondents aged 21–29 were 1.043 times more likely to answer *"Yes"* compared to those under 20, while those aged 30–39 were 1.354 times more likely. In contrast, respondents aged 40–49 were only 0.541 times as likely, whereas those aged 50 and above showed the strongest tendency, being 3.61 times more likely than the <20 group.

Marital status also influenced responses: married respondents were 1.102 times more likely to answer *"Yes"* compared to singles, while divorced respondents showed no likelihood (0 times) relative to singles. Educational attainment revealed that

undergraduates were 0.365 times as likely to answer *"Yes"* compared to diploma holders, postgraduates 0.391 times, and doctoral students 0.500 times.

Occupational status further shaped attitudes. Freelancers were 1.444 times more likely to answer *"Yes"* compared to unemployed respondents, private sector workers 1.436 times more likely, while independent workers and government employees were less likely, at 0.444 times each. In addition to odds ratio analysis, aggregation was conducted for practice-related questions and cross-tabulated with demographic variables. Table 6 indicates that a higher percentage of females answered *"Yes"* compared to males, with respondents under 20 years old showing the highest proportion. Divorced individuals recorded the highest percentage of *"Yes"* responses by marital status, postgraduate students by educational level, and independent workers by occupation.

The demographic variations observed in attitudes and practices toward personal data protection underscore the uneven distribution of digital literacy among Indonesian college students. Gender differences suggest that female respondents demonstrate greater caution, while age effects reveal that older participants are more aware of risks, aligning with broader findings that maturity often correlates with heightened sensitivity to privacy concerns. Educational status presents a paradox: although undergraduates and postgraduates showed lower odds in attitude measures, cross-tabulation indicates stronger protective practices among advanced degree holders, suggesting that higher education fosters behavioral awareness even when attitudinal responses appear weaker. Occupational differences further highlight how exposure to diverse work environments influences perceptions of data security, with freelancers and private sector workers showing stronger tendencies to acknowledge risks compared to government employees.

These findings reinforce the importance of Regulation No. 27 of 2022 as a legal framework, but they also reveal that regulation alone is insufficient without targeted efforts to strengthen digital literacy. The persistence of low awareness among younger students and those with limited occupational exposure suggests that educational institutions must play a central role in embedding personal data protection into curricula and social media practices. By linking demographic insights to regulatory imperatives, the study demonstrates that effective implementation of personal data protection requires not only legal enforcement but also cultural and educational interventions that address gaps in knowledge, attitudes, and practices.

Table 7. Odds Ratio Demographic Variable towards Practice

		No	Yes	AOR (CI 95%)
Sex	Female	24 (12.31)	171 (87.69)	1
	Male	18 (13.85)	112 (86.15)	0.873 (0.453, 1.683)
Age	<20	19 (12.5)	133 (87.5)	1
	21-29	17 (12.78)	116 (87.22)	0.975 (0.484, 1.963)
	30-39	3 (14.29)	18 (85.71)	0.857 (0.230, 3.187)
	40-49	2 (16.67)	10 (83.33)	0.714 (0.145, 3.511)
	>50	1 (14.29)	6 (85.71)	0.857 (0.098, 7.514)
Marital Status	Single	35 (12.64)	242 (87.36)	1
	Married	7 (14.89)	40 (85.11)	0.826 (0.344, 1.988)
	Divorced	0 (0)	1 (100)	2336 (0.000 ,0000)
Student Status	Diploma	3 (30)	7 (70)	1
	Undergraduate	33 (12.6)	229 (87.4)	2.974 (0.733, 12.071)

	Postgraduate/ Master	2 (6.25)	30 (93.75)	6.429 (0.897, 46.064)
	Doctoral	4 (19.05)	17 (80.95)	1.821 (0.321, 10.342)
Occupation scope	Unemployed	31 (14.09)	189 (85.91)	1
	Freelance	4 (10.81)	33 (89.19)	1.353 (0.448, 4.086)
	Independent Worker	0 (0)	7 (100)	0.00, 0.00
	Private Sector	3 (7.5)	37 (92.5)	2.023 (0.588, 6.965)
	Government Sector	4 (19.05)	17 (80.95)	0.697 (0.22, 2.209.563)

Note: AOR (Adjusted Odds Ratio), Processed from the results of the answers of research respondents

Based on the odds ratio values derived from the partial test output (Table 7), notable differences emerge across predictor variables in relation to Practice. Male respondents were 0.873 times as likely as females to answer *"Yes."* Respondents aged 21–29 were 0.975 times as likely as those under 20, while those aged 30–39 and 40–49 were less likely, at 0.857 and 0.714 respectively. Respondents aged 50 and above showed a likelihood of 0.857 compared to the <20 group.

Marital status also influenced practice-related responses. Married respondents were 0.826 times as likely to answer *"Yes"* compared to singles, while divorced respondents showed an exceptionally high likelihood (2336 times) relative to singles. Educational attainment revealed stronger effects: undergraduates were 2.974 times more likely to answer *"Yes"* compared to diploma holders, postgraduates 6.429 times more likely, and doctoral students 1.821 times more likely.

Occupational status further shaped practices. Freelancers were 1.353 times more likely to answer *"Yes"* compared to unemployed respondents, private sector workers 2.023 times more likely, while government employees were less likely at 0.697. Independent workers showed an extremely high odds ratio, though the magnitude suggests potential statistical distortion due to sample size.

In addition to odds ratio analysis, aggregation was conducted for knowledge-related questions and cross-tabulated with demographic variables. Table 7 indicates that respondents aged over 50 recorded the highest percentage of *"Yes"* responses, divorced individuals had the highest proportion by marital status, doctoral students by educational level, and private sector workers by occupation.

The demographic variations identified in both attitudes and practices toward personal data protection highlight the complex interplay between regulation, digital literacy, and socio-cultural factors. Differences across gender, age, marital status, education, and occupation suggest that awareness and protective behaviors are not evenly distributed, but shaped by lived experiences and social positioning. Younger respondents, despite being the most active social media users, often demonstrated lower concern, while older participants and those with advanced education showed stronger protective practices. Similarly, occupational contexts influenced perceptions, with freelancers and private sector workers more attuned to risks than government employees. These findings underscore that Regulation No. 27 of 2022 provides a necessary legal framework, yet its effectiveness depends on how diverse demographic groups internalize and act upon its provisions. Bridging statistical evidence with theoretical perspectives, the study affirms

that personal data protection is not merely a matter of law but of digital literacy, identity construction, and cultural adaptation in mediated environments.

Table 8. Odds Ratio Demographic Variable towards Knowledge

		Bad	Good	AOR (CI 95%)
Sex	Female	35 (17.95)	160 (82.05)	1
	Male	19 (14.62)	111 (85.38)	1.278 (0.695, 2.349)
Age	<20	22 (14.47)	130 (85.53)	1
	21-29	28 (21.05)	105 (78.95)	0.635 (0.343, 1.174)
	30-39	2 (9.52)	19 (90.48)	1.608 (0.350, 7.391)
	40-49	2 (16.67)	10 (83.33)	0.846 (0.174, 4.124)
	>50	0 (0)	7 (100)	273388050 (0.000, 0.000)
Marital	Single	49 (17.69)	228 (82.31)	1
Status	Married	5 (10.64)	42 (89.36)	1.805 (0.679, 4.797)
	Divorced	0 (0)	1 (100)	347185382 (0.000, -)
Student	Diploma	3 (30)	7 (70)	1
Status	Undergraduate	43 (16.41)	219 (83.59)	2.183 (0.543, 8.776)
	Postgraduate/ Master	6 (18.75)	26 (81.25)	1.857 (0.368, 9.364)
	Doctoral	2 (9.52)	19 (90.48)	4.071 (0.558, 29.725)
Occupation	Unemployed	36 (16.36)	184 (83.64)	1
Scope	Freelance	9 (24.32)	28 (75.68)	0.609 (0.265, 1.398)
	Independent Worker	1 (14.29)	6 (85.71)	1.174 (0.137, 10.047)
	Private Sector	4 (10)	36 (90)	1.761 (0.590, 5.253)
	Government Sector	4 (19.05)	17 (80.95)	0.832.264, 2.616

Note: AOR (Adjusted Odds Ratio), Processed from the results of the answers of research respondents

Based on the odds ratio values derived from the partial test output (Table 8), several notable differences emerge across predictor variables in relation to knowledge. Male respondents were 1.278 times more likely than females to answer *"True"* on knowledge items. Respondents aged 21–29 were less likely (0.635) compared to those under 20, while those aged 30–39 were more likely (1.608). Participants aged 40–49 showed a lower likelihood (0.846), whereas those aged 50 and above displayed an extremely high odds ratio (273,388,050), which likely reflects statistical distortion due to small sample size.

Marital status also influenced knowledge responses. Married respondents were 1.805 times more likely to answer *"True"* compared to singles, while divorced respondents showed an exceptionally high odds ratio (347,185,382), again suggesting possible data imbalance. Educational attainment revealed consistent effects: undergraduates were 2.183 times more likely to answer *"True"* compared to diploma holders, postgraduates 1.857 times more likely, and doctoral students 4.071 times more likely. Occupational status further shaped knowledge outcomes. Freelancers were less likely (0.609) to answer *"True"* compared to unemployed respondents, while independent workers were slightly more likely (1.174). Private sector workers showed a stronger likelihood (1.761), whereas government employees were less likely (0.832).

These findings highlight how demographic characteristics shape knowledge of personal data protection among Indonesian college students. Gender and age differences suggest that younger and female respondents may require more targeted awareness initiatives, while higher education levels consistently correlate with stronger knowledge, underscoring the role of academic exposure in fostering digital literacy. The extreme odds ratios observed for older and divorced respondents point to statistical anomalies, yet they also signal that life experience and social circumstances may influence awareness. Occupational differences reveal that private sector exposure enhances knowledge, while government employees and freelancers may face gaps in understanding. Taken together, these patterns emphasize that Regulation No. 27 of 2022 cannot be effective in isolation; its success depends on complementary educational and cultural interventions that address uneven knowledge distribution across demographic groups.

Finally, the findings reveal a contrast between high levels of understanding in the prohibition aspect and lower comprehension of technical procedures. Respondents demonstrated the strongest awareness (95.7%) regarding the prohibition of falsifying personal data for personal gain or to harm others. This aligns with the theory of the deterrence effect (Piquero, 2019), which posits that the threat of criminal sanctions--such as those stipulated in Articles 67–72 of the Personal Data Protection Law (UU PDP)--can heighten public awareness. Similar research by Wahyudi (2023) in the *Indonesian Law Journal* confirms that criminal sanctions are effective in shaping legal consciousness about cybercrime.

By contrast, the lowest level of understanding (75.1%) was observed in relation to dispute resolution mechanisms, particularly arbitration and court procedures. This suggests that respondents may be less familiar with alternative dispute resolution (ADR) frameworks. Nurjaya (2022) found that only 30% of Indonesians understand arbitration processes, a finding consistent with the Kominfo report (RI, 2023), which notes that PDP Law socialization has largely emphasized prohibitions rather than technical procedures.

In addition, uncertainty remains regarding the definition of specific personal data, with 23.1% of respondents selecting *"Don't Know."* This reflects ambiguity in distinguishing between general and specific categories of data, such as medical, genetic, or financial information. Setyawan (2021), in the *Journal of Personal Data Protection*, observed that the public often confuses these categories due to the absence of concrete examples in socialization efforts.

Discussion

The question is, why do many social media users publish their identities? Related to interaction and self-disclosure in computer-mediated communication (CMC), several factors can be seen according to Walther's (1996) explanation, as cited by Whitty and Joinson (2009), and call it hyperpersonal interaction. *First*, mostly in online communication, social categorisation is shared to see if they are compatible or similar. The more similarities that appear in online communication, there will be a tendency for audiences to feel like or be comfortable with their interlocutors.

Second, message senders can optimize their self-presentation to appear more positive and create favorable impressions, thereby increasing the likelihood that message recipients will accept them. Computer-mediated communication (CMC) offers features distinct from nonverbal cues in face-to-face interaction. As a result, the messages conveyed in online exchanges often reproduce personal information--whether thoughts or feelings—that recipients use to construct impressions of the sender.

Third, the hyperpersonal format of CMC, particularly in asynchronous communication, allows interactions to occur (1) at any time regardless of temporal constraints, (2) with ample opportunities to edit and refine message texts, (3) through the blending of task-related and social content, and (4) with deliberate delays in responding, enabling greater attention to message quality before replying.

The internet and social media thus provide alternative communication channels where users are not only consumers of information but also active producers. This digital reality significantly influences the role of audiences, who now participate in shaping discourse and meaning. In journalism studies, social media is recognized as both an additional distribution channel and a key element of media convergence, extending the reach of news and transforming audience engagement. Social media then becomes a place for audiences not only as consumers of media products, but can also actively provide additional information, express their opinions on an event (Ben-David & Soffer, 2019; Masullo Chen et al., 2019; Tenenboim, 2022)to create a digital public space among each other (Hille & Bakker, 2014; Kangaspunta, 2018; Marchionni, 2015; Zamith & Lewis, 2014).

These observations underscore how CMC reshapes interpersonal and mass communication by amplifying self-presentation strategies, enabling hyperpersonal interactions, and positioning audiences as co-creators of meaning. The asynchronous nature of online communication fosters reflection and editing, while the participatory affordances of social media blur the boundaries between sender and receiver. In the context of journalism, this convergence challenges traditional one-way dissemination models, situating audiences as active nodes in the communication network. Consequently, the study of CMC and social media highlights not only technical affordances but also cultural shifts in how identity, credibility, and information flows are constructed in digital environments.

Although the involvement of the audience in the information production-consumption process becomes more of a role in certain contexts, it should be noted that the accounts used contain various features with self-information. Profile photos and occupations posted on social media platforms like Instagram enable other users to identify and profile individuals, which can lead to criminal activity (Drury et al., 2022; Shariff, 2011). This happens because of the characteristics of social media that connect users (Gane & Beer, 2008; Mancosu & Vegetti, 2020; Sarikakis & Winter, 2017). These relationships and networks allow users to explore various information from others. Activities such as publishing photos on Instagram, posting videos about houses on TikTok, or announcing a college graduation on Facebook often unwittingly reveal information about the users themselves.

The principles of SIPT--verbal cue substitution and extended time in relationship building--help explain why personal data protection becomes increasingly critical in digital environments. Impression management through text-based communication often encourages users to disclose personal thoughts, feelings, or identifiers to construct favorable impressions, yet this very disclosure heightens the risk of oversharing sensitive information. Similarly, the asynchronous nature of CMC, which allows for repeated and edited exchanges over time, fosters intimacy and relational bonds but also prolongs the circulation of personal data across platforms. In this context, the enactment of Indonesia's Personal Data Protection Law underscores the need to balance relational motivations with regulatory safeguards. Awareness that personal data is not merely social content but a

protected asset reframes online interaction, reminding users that identity construction in mediated spaces must be accompanied by caution and responsibility.

According to Social Information Processing Theory (SIPT), two key principles explain how relationships can develop through computer-mediated communication (CMC). *First*, verbal cues serve as substitutes for nonverbal signals typically available in face-to-face interaction. While impressions offline are shaped by facial expressions, voice intonation, eye gaze, and body posture, in CMC these impressions are constructed through text and the way language conveys emotion and intent. Experimental studies with foreign audiences illustrate this process: contrasting messages--one friendly and one hostile--elicited textual replies that reflected emotional responses, demonstrating how impressions can be formed purely through verbal (Walther, 2004; Walther & Addario, 2001).

Second, SIPT emphasizes the role of extended time in relationship development. The exchange of social information in CMC occurs more slowly than in face-to-face communication, yet relational bonds are not necessarily weakened. Instead, the timing of message delivery shapes intimacy and interaction. Online communication allows for asynchronous exchanges, where messages can be composed, edited, and sent periodically. Continuous or repeated messaging fosters stronger relational ties, particularly when audiences anticipate future interactions. Chronological cues--how individuals perceive and respond over time--thus function as nonverbal indicators that remain salient in CMC.

In the Indonesian context, the presence of personal data protection regulations provides not only legal certainty but also raises awareness that information shared online cannot be published indiscriminately. Personal data is increasingly recognized as a valuable asset that must be safeguarded rather than treated as mere content for likes or comments.

Despite its contributions, this study has several limitations that must be acknowledged. *First*, the use of purposive sampling and an infinite population formula means that the sample of 325 respondents cannot be considered fully representative of all Indonesian college students. The reliance on self-reported survey data also introduces potential biases, such as social desirability and inaccurate recall, which may affect the validity of responses regarding knowledge, attitudes, and practices of personal data protection. Furthermore, the cross-sectional design captures perceptions and behaviors at a single point in time, limiting the ability to observe changes or causal relationships between regulatory awareness and online practices.

Second, the scope of the research is constrained by its focus on college students, excluding other vulnerable demographics such as high school students, working professionals, or older adults who also actively use social media. The questionnaire items, while derived from Regulation No. 27 of 2022 and the KAP framework, may not fully encompass the complexity of digital literacy and identity management in mediated environments. Additionally, the study does not account for platform-specific differences in privacy settings or cultural variations in data-sharing practices across Indonesia's diverse regions. These weaknesses highlight the need for future research employing longitudinal designs, broader demographic coverage, and mixed methods to provide a more comprehensive understanding of personal data protection behaviors in the Indonesian digital landscape.

While these limitations constrain the generalizability of findings, they do not diminish the study's originality and contribution. On the contrary, by positioning college students as a digitally active yet vulnerable demographic, this research provides an early empirical lens into how Regulation No. 27 of 2022 intersects with everyday online

practices. The methodological adaptation of the Knowledge–Attitudes–Practices (KAP) framework to the field of communication and digital literacy offers a novel approach that bridges disciplines and highlights the gap between regulatory safeguards and lived behaviors. Thus, despite sampling and scope restrictions, the study advances scholarly discourse on mediated identity and personal data protection, while offering actionable insights for policymakers, educators, and civil society to strengthen digital literacy and cultivate responsible digital citizenship in Indonesia's evolving media environment.

Conclusion

Although the Indonesian Government enacted Regulation No. 27 of 2022 on Personal Data Protection as the first comprehensive legal framework to safeguard citizens against misuse of personal data, the findings of this study demonstrate that regulatory presence alone is insufficient, as personal data--by its very nature--constitutes sensitive information that should not be freely shared on social media platforms which, as borderless media, enable rapid circulation and exploitation of uploaded content; the empirical evidence, showing that 87.1% of respondents would still publish personal data online while only 12.9% expressed reluctance, underscores limited awareness and highlights a critical gap between regulatory intent and public behavior, thereby revealing the urgent need for more effective socialization, education, and digital literacy initiatives; these findings carry broader implications by emphasizing that legal instruments must be complemented by cultural and educational interventions to foster responsible digital citizenship, embedding personal data protection into everyday social media practices particularly among younger demographics, and requiring sustained collaboration between government, educational institutions, civil society, and media outlets to ensure that the regulation is not only legally binding but socially internalized; ultimately, while Regulation No. 27 of 2022 represents a milestone in Indonesia's digital governance, its effectiveness depends on bridging law, literacy, and lived practice, moving beyond compliance toward cultivating a deeper culture of digital responsibility, supported by awareness campaigns that clarify dispute resolution mechanisms and distinctions between categories of personal data, integration of digital literacy modules into higher education curricula to build normative and practical competencies, and cross-sector collaboration to design culturally resonant interventions that transform legal mandates into socially embedded behaviors, ensuring that personal data protection becomes a cornerstone of responsible digital citizenship in Indonesia's evolving information society.

Conflict of Interest

We certify that there is no conflict of interest with any financial, personal, or other relationships with other people or organisations related to the material discussed in the manuscript.

Acknowledgements

The authors would like to express their gratitude and appreciation to fellow lecturers from various regions who helped distribute the research questionnaires to their students.

References

Adjei, J. K., Adams, S., Mensah, I. K., Tobbin, P. E., & Odei-Appiah, S. (2020). Digital identity management on social media: Exploring the factors that influence personal information disclosure on social media. *Sustainability (Switzerland)*, *12*(23), 1–17.

https://doi.org/10.3390/su12239994

Andrade, C., Menon, V., Ameen, S., & Kumar Praharaj, S. (2020). Designing and Conducting Knowledge, Attitude, and Practice Surveys in Psychiatry: Practical Guidance. *Indian Journal of Psychological Medicine*, *42*(5), 478–481. https://doi.org/10.1177/0253717620946111

Badran, I. G. (1995). Knowledge, Attitude and Practice, the three pilars of excellence and wisdom: a place in the medical profession. *Eastern Mediterranean Health Journal*, *1*(1), 8–16. https://www.emro.who.int/emhj-volume-1-1995/volume-1-issue-1/article1.html

Barabasi, A.-L. (2011). Introduction and Keynote to A Networked Self. In Z. Papacharissi (Ed.), *A Networked Self: Identity. Comunity, and Culture on Social Networ Sites* (pp. 1–14). Routledge.

Barnes, R., Mahar, D., Cockshaw, W., & Wong, I. (2018). Personality and online news commenting behaviours: uncovering the characteristics of those below the line. *Media International Australia*, *169*(1), 117–130. https://doi.org/10.1177/1329878X18798695

Bates, B. R., Tami, A., Carvajal, A., & Grijalva, M. J. (2021). Knowledge, attitudes, and practices towards covid-19 among venezuelans during the 2020 epidemic: An online cross-sectional survey. *PLoS ONE*, *16*(4 April), 1–16. https://doi.org/10.1371/journal.pone.0249022

Bayer, J. B., Cin, S. D., Campbell, S. W., & Panek, E. (2016). Consciousness and Self-Regulation in Mobile Communication. *Human Communication Research*, *42*, 71–97. https://doi.org/10.1111/hcre.12067

Ben-David, A., & Soffer, O. (2019). User comments across platforms and journalistic genres. *Information Communication and Society*, *22*(12), 1810–1829. https://doi.org/10.1080/1369118X.2018.1468919

Blanchard, A., & Horan, T. (1998). Virtual communities and social capital. *Social Science Computer Review*, *16*(3), 293–307. https://doi.org/10.1177/089443939801600306

Boyd, D. (2009). *Social media is here to stay ... now what?* Microsoft Tech Fest.

Bruns, A., Highfield, T., & Burgess, J. (2013). The Arab Spring and Social Media Audiences. *American Behavioral Scientist*, *57*(7), 871–898. https://doi.org/10.1177/0002764213479374

Bukata, I. T., Dadi, L. S., Ayana, A. M., Mengistu, D., Yewal, D., Gizaw, T. S., & Woldesenbet, Y. M. (2022). Knowledge, Attitudes, and Practice Toward Prevention of COVID-19 Among Jimma Town Residents: A Community-Based Cross-Sectional Study. *Frontiers in Public Health*, *10*(April), 1–10. https://doi.org/10.3389/fpubh.2022.822116

Castells, M. (2007). Communication, power and counter-power in the network society. *International Journal of Communication*, *1*, 238–266. https://ijoc.org/index.php/ijoc/article/view/46

Castells, M. (2010). *The Information Age, Economy, Society, and Culture*. Blackwell Publishing Ltd.

Costera Meijer, I., & Groot Kormelink, T. (2015). Checking, Sharing, Clicking and Linking: Changing patterns of news use between 2004 and 2014. *Digital Journalism*, *3*(5), 664–679. https://doi.org/10.1080/21670811.2014.937149

Couldry, N., & van Dijck, J. (2015). Researching Social Media as if the Social Mattered. *Social Media and Society*, *1*(2). https://doi.org/10.1177/2056305115604174

Driscoll, C., & Gregg, M. (2010). My profile: The ethics of virtual ethnography. *Emotion*,

Space and Society, *3*(1), 15–20. https://doi.org/10.1016/j.emospa.2010.01.012

Drury, B., Drury, S. M., Rahman, M. A., & Ullah, I. (2022). A social network of crime: A review of the use of social networks for crime and the detection of crime. *Online Social Networks and Media*, *30*(April), 100211. https://doi.org/10.1016/j.osnem.2022.100211

Dyer-witheford, N. (2010). Digital labour, species-becoming and the global worker. *Ephemera*, *10*(3/4), 484–503. http://www.ephemerajournal.org/contribution/digital-labour-species-becoming-and-global-worker

Epstein, J., & Klinkenberg, W. D. (2002). Journal of Technology in Human Services Collecting Data via the Internet : The Development and Deployment of a Web-Based Survey Collecting Data via the Internet : The Development and Deployment of a Web-Based Survey. *Journal of Technology in Human Services*, *19*(2–3), 33–47. https://doi.org/10.1300/J017v19n02

Etokidem, A. J., Ago, B. U., Mary, M., Affiong, E., Eno, U., & Anastasia, I. (2018). Ebola virus disease: Assessment of knowledge, attitude and practice of nursing students of a Nigerian University. *African Journal of Health Science*, *18*(1), 55–56. https://doi.org/10.4314/ahs.v18i1.9

Fang, W., & Nie, C. (2022). Inequalities in digital literacy : exploring the disparity in tangible outcomes of internet use among college students in China. *Frontiers in Communication*, *June*, 1–12. https://doi.org/10.3389/fcomm.2025.1601240

Gane, N., & Beer, D. (2008). *New Media: The Key Concepts*. Berg.

Goodell, G., & Aste, T. (2019). A Decentralized Digital Identity Architecture. *Frontiers in Blockchain*, *2*(November), 1–19. https://doi.org/10.3389/fbloc.2019.00017

Han, N., Li, S., Huang, F., Wen, Y., & Su, Y. (2023). How social media expression can reveal personality. *Frontiers in Psychiarty*, *March*, 1–12. https://doi.org/10.3389/fpsyt.2023.1052844

Hesmondhalgh, D. (2010). User-generated content, free labour and the cultural industries. *Ephemera*, *10*(3/4), 267–284. http://www.ephemerajournal.org/contribution/user-generated-content-free-labour-and-cultural-industries

Hille, S., & Bakker, P. (2014). Engaging the social news user. *Journalism Practice*, *8*(5), 563–572. https://doi.org/10.1080/17512786.2014.899758

Hölbl, M., Zlatolas, L. N., Welzer, T., & Heric, M. (2015). Computers in Human Behavior Privacy antecedents for SNS self-disclosure : The case of Facebook. *Computers in Human Behavior Journal*, *45*, 158–167. https://doi.org/10.1016/j.chb.2014.12.012

Jordan, T. (1999). Cyberpower: The culture and politics of cyberspace and the internet. In *Contemporary Sociology* (Vol. 31, Issue 3). Routledge.

Kang, H., Baek, J., Chu, S. H., & Choi, J. (2023). Digital literacy among Korean older adults : A scoping review of quantitative studies. *Digital Health*, *9*, 1–23. https://doi.org/10.1177/20552076231197334

Kangaspunta, V. (2018). Online news comments: Social network and emergent public. *Information Society*, *34*(5), 275–288. https://doi.org/10.1080/01972243.2018.1497741

Katie J. Ward. (1999). Cyber-Ethnography and the Emergence of the Virtually New Community. *Journal of Information Technology*, *4*(1), 95–105. http://www.tandfonline.com/doi/abs/10.1080/026839699344773

Krebs, I., & Lischka, J. A. (2019). Is audience engagement worth the buzz? The value of audience engagement, comment reading, and content for online news brands.

Journalism, *20*(6), 714–732. https://doi.org/10.1177/1464884916689277

Krejcie, Robert V, & Morgan, Daryle W. (1970). Determining Sample Size for Research Activities. *Educational and Psychological Measurement*, *30*(3), 607–610. https://doi.org/10.1177/001316447003000308

Ksiazek, T. B. (2018). Commenting on the News: Explaining the degree and quality of user comments on news websites. *Journalism Studies*, *19*(5), 650–673. https://doi.org/10.1080/1461670X.2016.1209977

Lee, M., Kang, B. A., & You, M. (2021). Knowledge, attitudes, and practices (KAP) toward COVID-19: a cross-sectional study in South Korea. *BMC Public Health*, *21*(1), 1–10. https://doi.org/10.1186/s12889-021-10285-y

Luceri, L., Andreoletti, D., Tornatore, M., Braun, T., & Giordano, S. (2020). Measurement and control of geo-location privacy on Twitter. *Online Social Networks and Media*, *17*. https://doi.org/10.1016/j.osnem.2020.100078

Mancosu, M., & Vegetti, F. (2020). What You Can Scrape and What Is Right to Scrape: A Proposal for a Tool to Collect Public Facebook Data. *Social Media and Society*, *6*(3). https://doi.org/10.1177/2056305120940703

Mandiberg, M. (2012). Introduction. In M. Mandiberg (Ed.), *The Social Media Reader*. New York University Press.

Marchionni, D. (2015). Online story commenting: An experimental test of conversational journalism and trust. *Journalism Practice*, *9*(2), 230–249. https://doi.org/10.1080/17512786.2014.938943

Masullo Chen, G., Fadnis, D., & Whipple, K. (2019). Can We Talk About Race? Exploring Online Comments about Race-Related Shootings. *Howard Journal of Communications*, *0*(0), 1–15. https://doi.org/10.1080/10646175.2019.1590256

Mat Din, H., Raja Adnan, R. N. E., Nor Akahbar, S. A., & Minhat, H. S. (2020). Assessment of Knowledge, Attitudes, and Practices towards COVID-19 among Malaysian Older Adults during the Pandemic (Preprint). *JMIR Formative Research*, *3*(1), 1–12. https://doi.org/10.2196/21888

Matei, S. A. (2005). A Sounding Board for The Self: Virtual Community as Ideology. *Technical Writing and Communication*, *35*(May 2004), 345–365. https://doi.org/10.2190/402T-KPLQ-V5QD-PCFX

Meikle, G. (2016). *Social Media: communication, sharing, and visibility*. Routledge. https://www.unodc.org/southasia/en/topics/frontpage/2009/trafficking-in-persons-and-smuggling-of-migrants.html

Methodology, S. (2014). *Researching Virtual Worlds* (U. Plesner & L. Phillips (eds.)). Routledge.

Milenkova, V., & Lendzhova, V. (2021). Digital Citizenship and Digital Literacy in the Conditions of Social Crisis. *Computers*, *10*(40), 1–14. https://doi.org/10.3390/computers10040040

Munger, K., Gopal, I., Nagler, J., & Tucker, J. A. (2021). Accessibility and generalizability: Are social media effects moderated by age or digital literacy? *Research and Politics*, *8*(2). https://doi.org/10.1177/20531680211016968

Naab, T. K., & Sehl, A. (2016). Studies of user-generated content : A systematic review. *Journalism*, *1*(18). https://doi.org/10.1177/1464884916673557

Nah, S., Namkoong, K., Record, R., & Van Stee, S. K. (2017). Citizen journalism practice increases civic participation. *Newspaper Research Journal*, *38*(1), 62–78. https://doi.org/10.1177/0739532917698444

Nasrullah, R. (2014). "Selling" Self-Image in the Era of New Media. *Jurnal Humaniora*,

26(1), 3–12. https://doi.org/10.22146/jh.4642

Nurhadi. (2022). *Inilah 7 Kasus Dugaan Kebocoran Data Pribadi Sepanjang 2022*. Tempo.Co.

O'Regan, T. (2021). Re-reading Personal Influence in an age of social media. *Continuum*, *35*(3), 437–454. https://doi.org/10.1080/10304312.2021.1902156

Osatuyi, B. (2015). Personality traits and information privacy concern on social media platforms. *Journal of Computer Information Systems*, *55*(4), 11–19. https://doi.org/10.1080/08874417.2015.11645782

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

Papacharisi, Z. (2011). Concluasion: A Networked Self. In Z. Papacharissi (Ed.), *A Networked Self: Identity. Comunity, and Culture on Social Networ Sites* (pp. 304–318). Routledge.

Park, Y. J. (2013). Digital Literacy and Privacy Behavior Online. *Communication Research*, *40*(2), 215–236. https://doi.org/10.1177/0093650211418338

Pietrass, M. (2007). Digital Literacy Research from an International and Comparative Point of View. *Research in Comparative and International Education*, *2*(1), 1–12. https://doi.org/10.2304/rcie.2007.2.1.1

Reuben, C. R., & Gyar, S. D. (2016). Knowledge, attitudes and practices of Lassa fever in and around Lafia, Central Nigeria. *International Journal of Public Health and Epidemiology Research*, *2*(1), 14–21. https://www.researchgate.net/publication/311455681_Knowledge_attitudes_and_practices_of_Lassa_fever_in_and_around_Lafia_Central_Nigeria

Reuben, R. C., Danladi, M. M. A., Saleh, D. A., & Ejembi, P. E. (2021). Knowledge, Attitudes and Practices Towards COVID-19: An Epidemiological Survey in North-Central Nigeria. *Journal of Community Health*, *46*(3), 457–470. https://doi.org/10.1007/s10900-020-00881-1

Ritzer, G., & Jurgenson, N. (2010a). Production, Consumption, Prosumption: The nature of capitalism in the age of the digital "prosumer." *Journal of Consumer Culture*, *10*(1), 13–36. https://doi.org/10.1177/1469540509354673

Ritzer, G., & Jurgenson, N. (2010b). Production, Consumption, Prosumption. *Journal of Consumer Culture*, *10*(1), 13–36. https://doi.org/10.1177/1469540509354673

Sarikakis, K., & Winter, L. (2017). Social Media Users' Legal Consciousness About Privacy. *Social Media and Society*, *3*(1). https://doi.org/10.1177/2056305117695325

Schroeder, K. C. (1994). Audience Semiotics, Interpretive Communities and the Ethnographic Turn in Media Research. *Media, Culture & Society*, *16*(2), 337–347. https://doi.org/10.1177/016344379401600208

Seidman, G. (2013). Self-presentation and belonging on Facebook : How personality influences social media use and motivations. *Personality and Individual Differences*, *54*(3), 402–407. https://doi.org/10.1016/j.paid.2012.10.009

Shariff, S. (2011). *Cyber Bullying*. Routledge. https://doi.org/10.1201/b10718-26

Soffer, O., & Gordoni, G. (2018). Opinion expression via user comments on news websites: analysis through the perspective of the spiral of silence. *Information Communication and Society*, *21*(3), 388–403. https://doi.org/10.1080/1369118X.2017.1281991

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

Sulistyawati, S., Rokhmayanti, R., Aji, B., Wijayanti, S. P. M., Hastuti, S. K. W., Sukesi, T. W., & Mulasari, S. A. (2021). Knowledge, attitudes, practices and information needs during the covid-19 pandemic in indonesia. *Risk Management and Healthcare Policy*, *14*, 163–175. https://doi.org/10.2147/RMHP.S288579

Tenenboim, O. (2022). Comments, shares, or likes: What makes news posts engaging in different ways. *Social Media + Society*, *8*(4), 1–17. https://doi.org/10.1177/20563051221130282

Turkle, S. (1995). *Life on screen: Identity in the age of the internet*. Simon & Schuster.

Van Dijk, J. (2006). *The network society*. SAGE Publications, Ltd.

Walther, J. B. (2004). Language And Communication Technology Introduction to the Special Issue. *Journal of Language and Social Psychology*, *23*(4), 384–397. https://doi.org/10.1177/0261927X04269584

Walther, J. B., & Addario, K. P. D. (2001). The Impacts of Emoticons on Message Interpretation in Computer-Mediated Communication. *Social Science Computer Review*, *19*(3), 324–347. https://doi.org/10.1177/089443930101900307

Wang, B. Y., Sherrington, C., Fairhall, N., Kwok, W. S., Michaleff, Z. A., Tiedemann, A., Wallbank, G., & Pinheiro, M. B. (2023). Exercise for fall prevention in community-dwelling people aged 60+: more effective in trials with higher fall rates in control groups. *Journal of Clinical Epidemiology*, *159*, 116–127. https://doi.org/10.1016/j.jclinepi.2023.05.003

Whitty, M., & Joinson, A. (2009). *Truth , Lies and Trust on the Internet*. Routledge.

Wood, A. F., & Smith, M. J. (2005). *Online Communication, Lingking Technology, Identity, & Culture*.

Zamith, R., & Lewis, S. C. (2014). From public spaces to public sphere. *Digital Journalism*, *2*(4), 558–574. https://doi.org/10.1080/21670811.2014.882066

Zhong, B. L., Luo, W., Li, H. M., Zhang, Q. Q., Liu, X. G., Li, W. T., & Li, Y. (2020). Knowledge, attitudes, and practices towards COVID-19 among chinese residents during the rapid rise period of the COVID-19 outbreak: A quick online cross-sectional survey. *International Journal of Biological Sciences*, *16*(10), 1745–1752. https://doi.org/10.7150/ijbs.45221

Zhu, X., & Xiong, Z. (2022). Exploring Association Between Social Media Addiction , Fear of Missing Out , and Self-Presentation Online Among University Students : A Cross-Sectional Study. *Frontiers in Psychiarty*, *13*(May), 1–9. https://doi.org/10.3389/fpsyt.2022.896762