Thin privacy boundaries: proximity and accessibility of E-commerce privacy policy in young consumers of Indonesia

Ananda Dwitha Yuniar
Department of Communication Science, Universitas Negeri Malang, Malang, Indonesia

Abstract

Purpose – Privacy is a sensitive issue in business because it involves how a platform uses consumer personal data. In terms of consumer rights, personal information needs to be protected in the privacy policy (PP). This study describes several aspects of the PP that consumers need to pay attention to, especially points prone to misuse of personal information.

Design/methodology/approach – This research used a taxonomy of consumer privacy concerns in e-commerce to reveal general and specific privacy concerns. The privacy calculus theory was also applied to explore consumer rationalization using (1) consumer knowledge about PP, (2) subjective perception, and (3) proximity to the PP features. Furthermore, the netnographic approach was used to combine the interrelation between technology and social construction. A sample of 378 young consumers in several major cities in Indonesia participated online and offline. Semi-structured interviews were also conducted to gain more in-depth comprehension.

Findings – The results showed that most young consumers have sufficient basic knowledge of the important points of PP. Furthermore, they tend not to read the PP because it is long and cumbersome, and therefore do not wish to expend much cognitive effort on it.

Originality/value – This study provides several results that can be utilized by policymakers or e-commerce companies to pay more attention to PPs for young groups. In addition, e-commerce companies can increase the knowledge of the privacy situation of Internet users in general.

Peer review – The peer review history for this article is available at: https://publons.com/publon/10.1108/IJSE-11-2022-0740

Keywords Privacy policy, E-commerce, Personal data, Business, Privacy

Paper type Research paper

1. Introduction

In the last decade, the exponential growth of information and communication technology, particularly the Internet, has transformed the way we live (Zhu et al., 2020). Most Internet users spend a lot of time online, including online shopping. E-commerce is one of Indonesia’s most widely used Internet platforms for online shopping consumers (Rahman et al., 2022). The growth of e-commerce start-ups cannot be separated from the use of data, as data submission is important for continuous transactions and interactions. Furthermore, big data records and collates large data sets in a database platform. Based on research from Krämer and Schawel (2020) stated that big data included shopping history, location, contacts, personal identity, diagnostics, user content, and other data.

Several studies examined the challenges of privacy issues in e-commerce transactions Oghazi et al. (2020) and which provides a comprehensive view of security and privacy problems in Big Data. The aim was to enable every user to permit the platform to use their data responsibly. Hermes et al. (2021) showed that security and privacy issues hinder users...
and businesses which create future obstacles to big data. With one click, users can provide various information in a system, therefore they constitute a basis for market analysis through an algorithmic system. For example, an algorithm can expand its business by including shopping preferences and locations or use personal data as ad-targeting. Baruh and Popescu (2017) state that the use of data helps marketers to target consumers online by personalizing these platforms or rendering advertisements.

Data is created from the interaction of Internet users in cyberspace through any software or platform. These data include conversations on Facebook, the interactions of online gamers, and online transactions, which are accessed via smartphones, computers, and laptops, respectively (Haviluddin and Alfred, 2019). Therefore, daily routines through cyberspace can be used as databases for certain interests, whether in business, government, or others. The image below shows how much people’s engagement with the Internet creates trillions of data daily. Large organizations then use this data to make decisions (Krämer and Schäwel, 2020).

Data has an important role in strategic decision-making, as parties that can process and utilize the data available in large, fast, and diverse volumes can make big profits. Use of big data in the private sector is mainly used for marketing activities. Aji and Aliyu (2021) stated that telecommunications companies use digital information monitoring systems from the web, Twitter, and others, to easily determine customer problems related to products and build commitment to follow up on these problems. However, there are potential privacy security problems, e.g. privacy violations, and breaches. Consumers often do not realize that their data is used for ad-targeting. This is known as thin privacy boundaries, which are a form of revealing and concealing private information. Parihar (2021) observed that in collecting, storing, and using this data, there is a vulnerability to personal information leakage, therefore privacy is difficult to predict. An increased trust, security, and privacy system are important mechanisms to focus on for e-platforms. Furthermore, data privacy is highly important as humans are increasingly dependent on the Internet, and almost all data is recorded through it.

In terms of consumer privacy, the platform used in this study has its policy. The privacy policy (PP) informs users about how their information is used, processed, and collected. Meier et al. (2020) stated that privacy policies inform Internet users of the website usage of their disclosed personal data. Fabian et al. (2017) mentioned that privacy policies are supposed to inform consumers about how personal information is handled by a platform. However, users often do not read the PP meticulously and choose to skip and agree. This is due to a lot of information presented, which is important to know before using the platform’s various features. It also occurs due to low reading desire and user indifference which is caused by long PP features alongside formal, ambiguous language.

Privacy policies must be accessible and intelligible to expand consumer proximity. Consumers may forget the right to their privacy due to low sensitivity and familiarity with technical terms such as phishing, cookies, platform privacy preferences, privacy policies, etc. which are often used by e-commerce platforms (Yuniar and Fibrianto, 2019). Therefore, this research aims to explore the understanding of the PP features by online shopping users on several e-commerce platforms they use.

2. Privacy calculus: subjective online privacy perception

In the age of information, activities that were once private or discussed with a small group of individuals now leave a data trail that shows our interests, personalities, opinions, and intentions, including shopping (Das Chaudhury and Choe, 2023; Zhu et al., 2020). Privacy is a sensitive issue in the business context as it involves user data and how a platform uses it. This data is often used for the personalization of a customer's experience and improvement of the e-commerce site. However, in terms of consumer rights, personal information needs to be protected and cannot be misused (Bandara et al., 2020). To maximize the benefits of the Internet, consumers often need to
disclose personal information to online companies. According to the privacy calculus theory (PCT) approach, decisions regarding such disclosure are based on the perception of disclosure benefits and privacy costs (Gutierrez et al., 2019). However, they are also thought to be dependent on the subjective perception of the current privacy level (Dienlin et al., 2020).

In another study, consumer privacy of college students on social media Facebook has different limits depending on the information (Xie and Karan, 2019). Privacy is defined contextually, as an individual’s ability to control personal information used for certain purposes. According to Sadikoglu (2017), privacy involves the willingness of consumers to share information via the Internet to enhance purchase decisions. This indicates that privacy is information that the user can fully control before distributing it on the Internet. Therefore, communication on the Internet should involve an optimizing process to achieve ideal levels of privacy. In the context of consumer subjective perception, there is a close relationship between risk factors and the trust felt by consumers during online shopping. The perceived risk and trust are interpreted by consumers when quality is compared during shopping. Especially, in Indonesia’s e-commerce, consumers can either choose to trust or distrust Internet shopping service providers, see Figure 1. Consumers are able to feel the risk attached to the technology used by the vendor. This factor explains the difference between risk and trust, therefore, consumers cannot trust Internet technology (Majumdar and Bose, 2016).

Some literature stated that the issue of privacy has become an important topic among Internet users both in social media applications and during online purchases. According to Walsh et al. (2017) many concerns have arisen in the United States because current laws are inadequate to protect the privacy of data collected when we process financial transactions. This is because, each user or consumer has different perceptions and knowledge regarding privacy in Internet use. Online privacy is interpreted as an individual act of selective disclosure in online media. In addition, it is often defined as a user or consumer concern that includes their control over the collection of information during online activity and control over the usage of the information collected. There are several ways and levels in which platforms obtain personal information from users. This consideration, built on several relevant theories and theoretical enhancements with limitations, is referred to as the privacy calculus (Gutierrez et al., 2019).

Source(s): Figure created by author

Figure 1. Integrative taxonomy model Consumer’s proximity in E-commerce privacy policy
The Privacy Calculus was used alongside the expectancy theory that proposes that human agents act in ways that maximize positive outcomes and minimize negative results (Bandara et al., 2020). The term privacy calculus was first introduced to measure human behavior. This calculus governs the decision-making process of individuals to decide whether to disclose personal information or not. However, the rational assumption is not accurate, as scientific literature has identified some influencing factors. Privacy is an ancient concept, but its interpretation and application in e-commerce are still new. It is also widely accepted that by giving precedence to consumer privacy, bigger benefits can be reaped by all parties involved (Strycharz et al., 2021).

3. Methodology
This study focuses on the PP features of several major e-commerce platforms in Indonesia. Specifically, it describes the significant portions of the PP that consumers need to be aware of. E-commerce in Indonesia already had the PP to protect its consumers. The question is, can they protect consumer data to prevent third-party misuse? This study will also describe and analyze the proximity of e-commerce consumers to privacy policies, alongside its related problems.

(1) Consumer awareness about substantial portions of the PP
(2) How to protect personal information
(3) Privacy breaches/consumer violations experienced.

To perform this objective, this study applied a netnographic that can combine the interrelation between technology and social construction. According to (Heinonen and Medberg, 2018; Kozinets, R.V. and Gambetti, 2021), netnography enhances subject knowledge with greater explicit recognition of different subject and domain perspectives. Therefore, data was observed and collected with online interviews, and the respective data was classified. The interviews involved open-ended questions adopted from previous studies which consist of data collection and surveillance practices, legal protection of users’ personal information, and the risks of personal information in a system. The study questions included an awareness that data parsimony can be a form of passive privacy regulation and how to implement preventive data protection strategies against privacy risks, see Table 1.

3.1 Sampling
Researchers used a cross-sectional design to capture several populations. Cross-sectional design carried out over three months (July–September 2022). Interviews with several samples are conducted using a longitudinal method to see changes; data is collected several times, and some of the same questions are asked at two or more different times. The target is several samples who have experienced a privacy breach experience.

3.1.1 Data collection.
(1) Observations were carried out both offline and online. Several points classified in the PP features were listed on several e-commerce platforms in Indonesia (last updated January 2022). In addition, observations were made through the Avast app on several respondents’ emails to recheck whether specific platforms had misused their online shopping emails. This was a data collection tool that can be profoundly explored through this observation.

(2) Semi-structured Interview. 30 young consumers were interviewed from a small number of survey targets. This structured interview was used to obtain a comprehensive understanding to enhance the data. The aim was to determine
various aspects such as consumer knowledge of PP, the subjective perception of online privacy, and consumer proximity to the PP features. These interviews consisted of approximately 15 open-ended questions.

(3) A mini-survey was conducted on 378 young people on their understanding of some essential points in the PP. Mini-surveys were also conducted to measure respondents’ knowledge and proximity to several important portions often emphasized in privacy policies. 2 answer choices were provided as either true or false. Each right answer will be worth one point and if the answer was incorrect, the value is zero. Furthermore, as a data amplifier, 8 important and common questions were compiled for the participants. The answers to the question items were used to measure the extent to which they are familiar with policies concerning personal data protection. The average age is 18–21, which is included in the category of digital natives.

4. Results
This mini-survey research was conducted through an online form for young consumers and compiled based on the important aspects of privacy policies. However, most of the questions
were answered questions correctly, which indicates that young consumers in Indonesia already understand privacy policies, see Table 2. Although after conducting interviews, some admitted they never read it comprehensively as it was long and convoluted.

In this context, the meaning of privacy, according Boerman et al. (2021), is the willingness of consumers to share private information over the Internet for purchasing decisions. Therefore, privacy is information that the user can fully control before distributing it online. There is a close relationship between risk factors and the trust felt by consumers in online shopping. Perceived risk and trust are interpreted by consumers when they compare quality at the time of shopping. In the context of e-commerce, consumers either trust or do not trust Internet shopping service providers. However, if consumers are worried about the technology, this signifies that they are able to feel the risk of the technology or platform. This factor explains the difference between risk, trust, and skepticism in Internet technology. The risk of data mining is felt by consumers when registered personal data can be used by e-commerce parties who easily provide access to third parties for various purposes. Fortes and Rita (2016) stated that a dimension of information misuse risk occurs when the consumer suffers a loss of privacy during an online purchase. In conducting transactions through e-commerce, consumers are required to provide personal information such as complete home address alongside phone number, email, and location.

Based on interviews with 10 individuals who use online shopping services more than five times a month, most stated that they read and knew the PP features, but did not truly understand the contents. According to the given answers, this is because the PP was too long and cumbersome, low reading literacy, was considered not essential, and therefore trusted their personal information in the platform. Consumers who enjoy online shopping are not counterbalanced by a cognitive effort to read substantial privacy policies. When registering for a platform, they skip and immediately tick the consent column. Further responses stated that they are unaware of the technical aspects related to privacy protection, i.e. cookie,

<table>
<thead>
<tr>
<th>Item</th>
<th>Consumer’s perception</th>
<th>Correct answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>The government already has an official law that protects the security of consumer information in EP transactions</td>
<td>% 56.5 43.5 0.43   False</td>
<td></td>
</tr>
<tr>
<td>The government has set a regulation to restrain EP from storing consumer personal information for a certain period</td>
<td>% 15.5 84.5 0.84 True</td>
<td></td>
</tr>
<tr>
<td>EP is not responsible for the misuse of consumer personal data that has been submitted to the system</td>
<td>% 54.4 45.6 0.46 True</td>
<td></td>
</tr>
<tr>
<td>The EP utilizes consumers’ personal data only for the purpose of shipping goods</td>
<td>% 53.4 46.6 0.47 False</td>
<td></td>
</tr>
<tr>
<td>It’s legal for EP sellers to charge different prices to different people at the same time</td>
<td>% 29.0 71.0 0.71 True</td>
<td></td>
</tr>
<tr>
<td>The Minister of communication and information regulation requires e-commerce to have electronic system certification</td>
<td>% 12.4 87.6 0.88 True</td>
<td></td>
</tr>
<tr>
<td>From a legal point of view, EP is required to provide consumers to see the information that has been collected</td>
<td>% 14.1 85.9 0.86 True</td>
<td></td>
</tr>
<tr>
<td>Consumers have rights under applicable law (such as exercising the right to opt out of data processing at a certain cost)</td>
<td>% 9.9 90.1 0.90 True</td>
<td></td>
</tr>
</tbody>
</table>

Table 2. Consumers’ understanding in the privacy policy features in March, 2022
Source(s): Table created by the author
firewall, IP Address, Cache, etc. (Yuniar and Fibrianto, 2019). Therefore, shopping ability is not accompanied by technological adaptability, as privacy is important but disregarded. There is no proximity between the consumer and the PP feature.

The PP is considered too long, convoluted, and not user-friendly, this causes consumers to easily ignore it. Knijnenburg et al. (2017) stated that the security system and PP do not follow standards, causing unequal treatment of consumer privacy. Furthermore, Meier et al. (2020) observed that participants who see a short PP will acquire greater knowledge about the SNS’s privacy practices than participants who see a long PP. Therefore, the platform needs to shorten the PP as many consumers believe that a shorter one is better.

4.1 Consumer privacy protection behavior

Table 3 shows that semi-structured interviews were conducted with several youths who are digital natives, as evidenced by their proximity to online shopping. Of the 30 interviewees, 21 had shopped on more than 2 platforms on their smartphones. About 4–5 a week, they also rely on online platforms to purchase required items. Online shopping is very fun and addictive, and apart from being able to compare prices, the platform can be accessed whenever they want (KH, KT). In addition, some of them are also discouraged from shopping at physical stores because they preferred the variety offered in various online stores (HS, IA, YN). For example, in physical stores, there were only certain flavors of packaged popcorn, but online they can choose more flavors. This is also true for purchasing the latest models of clothes that have not been made available at physical stores.

EG stated that shopping on large e-commerce platforms is relatively safe from crimes such as online buying and selling fraud. The system works to prevent the sale of goods that do not match the description. However, EG did not rule out the possibility of theft of personal information. During transactions, personal information including ID card data is submitted,

<table>
<thead>
<tr>
<th>Pseudonym</th>
<th>Age (years)</th>
<th>Sex</th>
<th>Kind of school/Bachelor degree</th>
</tr>
</thead>
<tbody>
<tr>
<td>AG</td>
<td>20</td>
<td>W</td>
<td>Politeknik Negeri Jakarta</td>
</tr>
<tr>
<td>DF</td>
<td>22</td>
<td>M</td>
<td>Universitas Pancasila</td>
</tr>
<tr>
<td>FH</td>
<td>19</td>
<td>M</td>
<td>Universitas Indonesia</td>
</tr>
<tr>
<td>RM</td>
<td>22</td>
<td>W</td>
<td>Universitas Indonesia</td>
</tr>
<tr>
<td>SD</td>
<td>18</td>
<td>W</td>
<td>Universitas Indonesia</td>
</tr>
<tr>
<td>ZK</td>
<td>18</td>
<td>M</td>
<td>Universitas Indonesia</td>
</tr>
<tr>
<td>DF</td>
<td>19</td>
<td>M</td>
<td>Universitas Muhammadyah Jakarta</td>
</tr>
<tr>
<td>EG</td>
<td>19</td>
<td>W</td>
<td>Universitas Muhammadyah Jakarta</td>
</tr>
<tr>
<td>SR</td>
<td>19</td>
<td>W</td>
<td>Universitas Muhammadyah Jakarta</td>
</tr>
<tr>
<td>ARI</td>
<td>21</td>
<td>M</td>
<td>Universitas Pancasila</td>
</tr>
<tr>
<td>FR</td>
<td>20</td>
<td>W</td>
<td>Universitas Trisakti</td>
</tr>
<tr>
<td>HS</td>
<td>19</td>
<td>W</td>
<td>Universitas Trisakti</td>
</tr>
<tr>
<td>IA</td>
<td>18</td>
<td>W</td>
<td>SMK 50 Jakarta</td>
</tr>
<tr>
<td>YN</td>
<td>22</td>
<td>M</td>
<td>Universitas Pancasila</td>
</tr>
<tr>
<td>RR</td>
<td>21</td>
<td>W</td>
<td>Universitas Indonesia</td>
</tr>
<tr>
<td>PN</td>
<td>19</td>
<td>W</td>
<td>UHAMKA</td>
</tr>
<tr>
<td>AND</td>
<td>22</td>
<td>M</td>
<td>Trisakti University</td>
</tr>
<tr>
<td>EVT</td>
<td>18</td>
<td>W</td>
<td>Universitas Indonesia</td>
</tr>
<tr>
<td>NA</td>
<td>21</td>
<td>W</td>
<td>Trisakti University</td>
</tr>
<tr>
<td>KH</td>
<td>21</td>
<td>W</td>
<td>Universitas Indonesia</td>
</tr>
<tr>
<td>KT</td>
<td>19</td>
<td>W</td>
<td>SMK Pariwisata</td>
</tr>
</tbody>
</table>

Source(s): Table created by the author
which must be kept confidential. According to RR, when privacy is compromised and
misused by third parties, it is dangerous because it involves personal data. Furthermore, RR
highlighted the possibility of personal data being stolen and misused for nefarious interests.

Digital technology is an infrastructure utilized by people in many countries for seeking
information, socializing, or entertainment (Dutton and Graham, 2014). Advances in
technology in the last few decades have ushered users into the era of big data. Data is an
important material in producing social and economic value, and previous research state that
data is the new oil. This is evident in the growing number of business start-ups and
government organizations that use big data regularly for market analysis. Although the
definition of big data has not been agreed upon, the term is often used to describe the
exponential growth and availability of data that is produced and transferred (Gutierrez et al.,
2019). Furthermore, “big data” is different from traditional data sets, as most of the data
collected in “big data” is raw but produces greater speed. According to (Knijnenburg et al.,
2017) big data analysis can apply smart algorithms and artificial intelligence to determine
relevant hidden insights and optimize data-driven decisions.

5. Discussions
5.1 Privacy breach/violation experienced among young consumers
Personal information contains valuable details that need to be protected, to prevent thieves
from accessing and stealing it. However, this awareness has not been widely realized due to
the ease of access of online services that require users to provide personal information. Online
shopping consumers should be able to optimize user settings, opt out, or delete the personal
information to ensure privacy (Baruh and Popescu, 2017). Therefore, the logic of big data
analytics which promotes an aura of unchallenged objectivity to the algorithmic analysis of
quantitative data, preempts individual ability to self-define and closes off any opportunity for
those inferences to be challenged or resisted. It is emphasized that the predominant privacy
protection regimes based on the privacy self-management framework of “notice and choice”
not only fail to protect individual privacy, but also underplay privacy as a collective good.
This is illustrated by discussing two possible individual strategies: Firstly, how withdrawal
from the market or avoidance, and secondly, how complete reliance on market-provided
privacy protections or assimilation, may result in fewer privacy options available to society at
large. The conclusion discussed how acknowledging the collective dimension of privacy
could provide more meaningful alternatives for privacy protection (Barth, 2022). Meanwhile,
consumers feel they know what to share or not, therefore they are in control of their personal
information.

Apart from the data management aspect, the security of personal information is also the
responsibility of the user. Although the data has been submitted and recorded digitally, there
should be limits on which data is shared. When utilizing e-commerce, consumers can use a
special email for shopping where all forms of spamming, advertisements or promotions can
be collected, distinct from personal emails. In addition, identity cards should not be carelessly
uploaded on a platform, passwords/pins must be updated with high complexity and security
increased using fingerprints, and ensure to delete cookies and caches. Online shopping
consumers should also be diligent in reading privacy policies to determine what rights were
violated whenever platforms misuse personal information. Reading the PP will also equip
users with knowledge, if unsure, for example, of the decision to opt out or delete an account
permanently. The responsibility for data security is what the government should be able to
guarantee through a PP on e-commerce, therefore the responsibility is not on users but on the
e-commerce platform, which is regulated by government policy (Maseeh et al., 2021).

Big data systems facilitate choices for users because the Internet will direct
recommendations according to the preferences and interests of consumers. However, it
may mislead, limit user insight, and affect independence. Consumers want to believe they have the authority to choose what they want to view even though the machine has unknowingly set it (Pan et al., 2017; Xie and Karan, 2019). That is the initial gap in the potential for leakage of consumer privacy data, which can be accessed by providers or other irresponsible parties. In addition, privacy data will also be traded without the user's knowledge, for example, incoming emails containing offers or promotions without ever registering or opening the site. A lot of online shopping consumers are unaware of these factors (Fortes and Rita, 2016). Discussion about risk, information control dan policy, it is in line with taxonomy by Bandara et al. (2020) in the privacy concerns in e-commerce.

The protection of digital identity and personal data is still an issue worldwide (Ameen et al., 2022). Some countries, including Indonesia, have regulations governing personal data protection, therefore, the legal aspects of citizens’ rights in the digital world can be guaranteed. By default, a device is designed with a myriad of safety features to ensure that user activities while utilizing digital media are safe and comfortable. Every technology has various loopholes that irresponsible people can take advantage of, which triggers cybercrimes such as hacking, phishing, doxing, or other privacy breaches. Furthermore, several consumers stated that they had never experienced a serious and harmful privacy breach, but are often bothered by an algorithmic system that limits their activities. For example, when they search for products/services on a false e-commerce platform, causing advertisements appear on social media, on web browsing, in emails, and even on mobile numbers. During the experiment, the emails of young consumers were checked using avast.com/hackcheck to determine how often an email has been leaked on the black market. This application also informs on leaked emails when connected to any site, for example, social media with e-commerce. However, due to user privacy and security reasons, all the e-commerce details cannot be displayed, only a few snippets.

5.2 The privacy policy (PP) feature and E-commerce

Table 4 shows e-commerce unicorns that already have an enormous market in Indonesia. From the observations, each platform has a user PP with different names, e.g. Personal data protection policy (Online Fashion), Privacy Settings (Commercial Electronic Platform), and the PP (Transportation). Until the observation in this study was carried out, some platforms were quite concerned about updating their privacy policies, as they had not been updated for a long time. The PP is an important feature that must be updated for users periodically (Song

<table>
<thead>
<tr>
<th>Type of E-commerce</th>
<th>Indonesia’ context</th>
<th>Substantial point that triggers invasion of privacy</th>
</tr>
</thead>
</table>
| Online fashion     | Last modified: Sept 2019 | (1) The platform is not responsible for unauthorized use by third parties caused by conditions that are beyond their control  
(2) The platform uses the services of third-party vendors who may use cookies on the Website |
| Commercial electronic platform | Last modified: June 2021 | 1. The platform will or may need to disclose user data to third party service providers, agents, and affiliates, or other parties |
| Transportation service online | Last modified: March 2021 | 1. In the website view, the privacy policy feature appears on the front but you have to scroll to the bottom. While in the application, the privacy policy feature display is not visible on the front screen, you have to open it |

Source(s): Table created by the author

Table 4. Substantial aspects of the privacy policy feature in Indonesia
et al., 2021). This will indicate that the platform is concerned about consumers’ personal information (Chen et al., 2023).

These market data and preferences are considered to provide benefits in increasing efficiency, innovation, productivity, and the creation of new policies. The information collected will be used as recommendations for marketing products and services. E-commerce parties are often guaranteed full security of personal data, as the Internet is accessible to anyone, including hackers. Furthermore, in Indonesia, well-known e-commerce sites such as *BL and *TP were hacked by irresponsible individuals who gained broad access to retrieve important consumer data such as email addresses and passwords (Zhu et al., 2020). This showed that full access capability from hackers causes consumer personal data to be misused.

Another risk in providing personal information is that e-commerce platforms can exchange or sell this information to other parties (Park, 2015). Personal information that has been submitted can be used for other purposes other than only as a complete process of consumer transaction data. This is often experienced by consumers who have shopped on e-commerce sites because when they browse the Internet there will be lots of pop-ups from advertisers even though they have never visited the advertiser’s site. The appearance of pop-up advertisements or promotions is caused by the provision of personal information such as the user’s IP address, location, email, or number, to third parties. Therefore, the protection and dissemination of consumer personal data rely on the e-commerce side. Consumers are often unaware of the possible dissemination and exchange of their data (Choi, 2022).

By default, a device is designed with a myriad of security features to ensure that online activities are safe and comfortable. However, every technology has various loopholes that can be exploited by irresponsible individuals. Privacy is a serious issue in electronic commerce, and poses a big challenge as e-commerce grows rapidly. Fortes and Rita (2016) highlighted that it is important to realize the concerns of users or consumers about the security of private information to maximize the potential of e-commerce. Furthermore, privacy is defined as an individual’s ability to control the personal information that is used for certain purposes (Park, 2015).

Table 4 shows that PP features are not easily understood, as users may not see and even be unaware of this setting. When this happens, users tend to ignore the personal data that has been provided to the platforms. It is preferable if the PP feature was in the dashboard to enable users to decide whether to accept it or not. Therefore, the PP feature should be set to appear when a user creates an account. Users will be directed to check the consent that contains the PP. Due to the length of privacy policies, all respondents in this study stated that they never read and only scrolled until they found a tick. This was because the features are too long and difficult to understand due to the use of formal, ambiguous language. Moreover, not all users come from economically well-off circles, which has an impact on ignoring the security of personal data when using e-commerce (Ahmad et al., 2022).

6. Conclusion and future research

This research provides new results on online privacy in three main points. First, shorter privacy policies are recommended, as this can increase the readability for younger generations who tend to be instant and more accustomed to short readings. Younger consumers may be more willing to read shorter privacy policies about the potential risks of website privacy, which in turn increases their knowledge. However, the platforms used in this research contained highly detailed privacy policies written in the Indonesian standard language, which makes the information harder to peruse. Second, in subjective perception, factual knowledge of substantial PP aspects is an important factor for the evaluation of one’s current online privacy level as well as the assessment of possible privacy risks. The more participants are aware of their level of privacy, the more realistic their feelings of privacy will
be. The subjective perception of privacy leads to different perceptions of the risks and benefits of self-disclosure. Therefore, situational perceptions can impact and distort the weight of the anticipated negative and positive consequences of disclosure. This study showed that young consumers disclosed more personal information when they experienced the higher benefits of using online shopping platforms. Due to the importance of factual privacy knowledge, policymakers should seek ways to increase this knowledge, as it is a significant factor underlying privacy decisions. Third, personal information is like something of value that must be safeguarded to prevent robbers from easily accessing it. However, due to the ease of access to Internet services that need users to disclose private data, this understanding has not been widely appreciated. It is underlined that the prevalent privacy protection regimes based on the “notice and choice” privacy managing oneself framework not only fail to safeguard individual privacy, but also downplay privacy as a social value. The limitation of this study is that it only reached young consumers in urban cities, therefore, the younger generation living in remote areas did not participate. Due to the privacy trend, the younger generation in areas that have not been too exposed to technology may be the most vulnerable. Further studies should attempt to broadly reach the younger generation to gain a comprehensive understanding.

References


Thin privacy boundaries


About the author
Ananda Dwitha Yuniar is Lecturer as well as Head of the Department of Communication Studies, Faculty of Social Sciences, Universitas Negeri Malang, Indonesia. She got her Master’s Degree from the Universitas Gadjah Mada, Indonesia. She is specialized in areas of media studies and digital literacy. Ananda Dwitha Yuniar can be contacted at: ananda.dwitha.fis@um.ac.id

For instructions on how to order reprints of this article, please visit our website: [www.emeraldgrouppublishing.com/licensing/reprints.htm](http://www.emeraldgrouppublishing.com/licensing/reprints.htm)
Or contact us for further details: permissions@emeraldinsight.com