World Journal of Advanced Engineering Technology and Sciences
eISSN: 2582-8266
Cross Ref DOI: 10.30574/wjaets
Journal homepage: https://wjaets.com/

(RESEARCH ARTICLE)

Check for updates

The privacy awareness behavior gap in young adult technology users

Victoria Imafidor * and Lois Adade

Department of Mathematics and Computer Science, Southwest Minnesota State University, Marshall, Minnesota, United States.

World Journal of Advanced Engineering Technology and Sciences, 2026, 19(03), 312-319

Publication history: Received on 18 May 2026; revised on 27 June 2026; accepted on 29 June 2026

Article DOI: https://doi.org/10.30574/wjaets.2026.19.3.0338

Abstract

Digital privacy is an important concern as individuals rely on mobile applications, social media platforms, and online services that routinely collect and process personal information. Despite growing awareness of privacy risks, many users continue to engage in behaviors that may expose their personal data. This study examined the privacy awareness behavior gap among young adult technology users by investigating technology confidence, awareness of data collection practices, perceptions regarding the seriousness of data misuse, and engagement in privacy protective behaviors. A quantitative survey methodology was employed using an online questionnaire distributed through both physical and digital recruitment methods. A total of 108 participants aged 18 years and older completed the survey.

Approximately 69.4% of respondents reported technology confidence ratings of four or five on a five point scale, while 68.6% rated application data misuse as a serious concern. Despite this awareness, 59.3% of participants reported that they rarely or never read privacy policies before installing or using digital applications. These results indicate a disconnect between privacy awareness and privacy protective behavior. The findings are consistent with existing privacy paradox research, which suggests that privacy concerns do not always translate into actions that protect personal information.

Keywords: Privacy Awareness; Privacy Paradox; Cybersecurity Behavior; Digital Privacy; Privacy Literacy

1. Introduction

The purpose of this research is to examine the gap between what young adult technology users know about digital privacy and the privacy protective behaviors they actually practice. There are many apps downloaded and used on people's smartphones as well as many online platforms and websites used regularly by people all over the world. Almost every activity completed online today leaves a trail or record of some sort. So, why do so many people continue to hand over their information without thinking about the potential consequences of it being misused by companies? This research aims to reveal the gap between what young adults know about digital privacy and their behavior and to understand mobile phone users' decisions with regard to privacy on their phones, and how digital privacy could be designed, educated and communicated to better support users of digital technology. Why don't individuals behave in a way that protects their information in most cases of their online behavior? These questions are not only of a technical nature but also of a human nature. They can be explained by the online habits of individuals, their trust in other online actors, their preference for convenience over other values and their risk assessment of online situations.

Digital privacy has become an increasingly important issue as individuals rely on online platforms, mobile applications, and internet connected services for communication, entertainment, education, and commerce. Although users frequently express concerns regarding how organizations collect, store, and share personal information, research has consistently shown that privacy concerns do not always translate into privacy protective actions. This phenomenon is

* Corresponding author: Victoria Imafidor

commonly described as the privacy paradox, where individuals report valuing privacy while simultaneously engaging in behaviors that expose personal data. One explanation for this paradox involves users' perceptions of risk and benefit when interacting with digital technologies. Dinev and Hart [1] found that individuals often perform a security cost benefit analysis before disclosing personal information online. Users may recognize potential privacy risks but still choose to share information when they perceive that the benefits of using a service outweigh the potential consequences. This finding suggests that privacy decisions are often influenced by convenience, functionality, and perceived value rather than privacy concerns alone.

Research has highlighted the role of trust in shaping privacy behavior. Beldad et al. [2] reported that trust in online organizations can significantly influence willingness to disclose personal information. When users believe that companies or platforms are trustworthy, they may be less likely to engage in privacy protective behaviors, even when they understand the risks associated with data collection. Trust can therefore reduce perceived vulnerability and contribute to a gap between privacy awareness and actual behavior.

Technology confidence may further influence privacy related decision making. Individuals who are comfortable using digital technologies often believe they possess sufficient knowledge to manage online risks effectively. However, confidence does not necessarily correspond with safe behavior. Debatin et al. [3] examined privacy attitudes among social networking users and found that individuals who expressed concerns about privacy frequently continued to disclose personal information online. The authors suggested that social rewards, convenience, and perceived control may encourage information sharing despite awareness of privacy risks. Privacy literacy has also been identified as an important factor in online privacy behavior. Individuals with greater knowledge of privacy settings, data collection practices, and online risks are generally more aware of potential threats. However, literacy alone does not guarantee protective action. Many users continue to ignore privacy notices, accept default settings, and provide personal information without carefully evaluating potential consequences. These findings suggest that behavioral, psychological, and contextual influences play a substantial role in privacy decision making.

Furthermore, existing research indicates that privacy behavior is shaped by a complex interaction of risk perception, trust, technology confidence, convenience, and perceived benefits. Although users may understand privacy risks and express concern regarding data misuse, they do not always engage in behaviors that protect personal information. These findings provide important context for examining the privacy awareness behavior gap among young adult technology users and support the need for research exploring why privacy knowledge often fails to produce privacy protective action.

2. Materials and Methods

This study employed a quantitative survey research methodology to examine the privacy awareness behavior gap among young adult technology users. The research focused on determining whether individuals who report high levels of technology confidence and awareness of privacy risks consistently engage in privacy protective behaviors when interacting with digital applications and online services. Quantitative survey methodology was selected because it allowed for the systematic collection of measurable participant attitudes, perceptions, and self-reported behaviors related to digital privacy, data collection practices, and cybersecurity decision making. The study examined participant perceptions regarding technology confidence, awareness of application data collection practices, perceived seriousness of data misuse, privacy policy reading behaviors, and user responses to personal data sharing. Descriptive statistical analysis was utilized to identify trends and behavioral patterns associated with privacy awareness and cybersecurity decision making among participants.

Participants were recruited using both physical and digital distribution methods over a three month data collection period. Eligibility requirements specified that all participants must be at least 18 years of age prior to participation. Consent confirmation was included at the beginning of the survey instrument to ensure ethical participation standards and voluntary engagement. Recruitment strategies involved distributing survey flyers across multiple social and educational environments including student cafeterias, classrooms, campus buildings, conferences, student organizations, and public bulletin boards. Two flyer formats were utilized, including standard board sized flyers and smaller portable handout versions intended to increase accessibility and participant reach. Digital survey links were additionally distributed through electronic copies, group chats, peer networks, and social media communication channels to increase participation diversity beyond exclusively in person recruitment environments.

Participation remained entirely voluntary throughout the study. No financial compensation, academic incentives, or coercive recruitment methods were used to influence participation. Participants were informed that survey responses would remain anonymous and that no personally identifiable information would be collected during the study. The

absence of personal identifiers was intended to encourage honest responses regarding privacy concerns, technology usage, and cybersecurity behaviors. At the conclusion of the collection period, the survey produced 108 complete responses eligible for final analysis. Following completion of data collection, the survey instrument was unpublished from Google Forms and closed for further submissions to preserve dataset integrity and prevent further modification.

Primary data collection was conducted using Google Forms as the survey administration platform. The survey instrument included demographic questions, multiple choice questions, Likert scale measurements, and behavioral perception items designed to evaluate privacy awareness and cybersecurity behaviors among technology users.

The survey specifically examined:

- Technology confidence levels;
- Understanding of application data collection and usage practices;
- Perceptions regarding the seriousness of data misuse;
- Frequency of privacy policy reading;
- Awareness of application tracking and data collection practices
- Participant experiences following the discovery of data sharing practices.

The final participant population consisted primarily of younger adult users with high levels of digital engagement. Most participants were between the ages of 18 to 24 years (72.2%), followed by participants between the ages of 25 to 34 years (18.5%). Smaller participant groups represented older demographic categories. The participant population was heavily student dominated, with students representing 82.4% of all respondents. Educational backgrounds varied from high school education through doctoral level attainment. Participant self reported technology confidence remained relatively high, with most respondents reporting confidence levels of four or five on a five number scale.

Table 1 Demographic characteristics of participants (N = 108)

Category	**n**	**%**
18–24	78	72.2
25–34	20	18.5
35–44	5	4.6
45–54	1	0.9
55–64	2	1.9
≥65	2	1.9
Student	89	82.4
Full-time employed	11	10.2
Part-time employed	3	2.8
Self-employed	3	2.8
Unemployed	2	1.9
High school or equivalent	25	23.1
Some college	34	31.5
Associate degree	5	4.6
Bachelor's degree	31	28.7
Master's degree	10	9.3
Doctoral degree	3	2.8

3. Results and Discussion

The survey findings revealed a notable gap between privacy awareness and privacy protective behavior among young adult technology users. As shown in Figure 1, participants generally reported high levels of confidence when using technology. Approximately 69.4% of respondents selected confidence ratings of four or five on a five number scale, while only 1.8% selected ratings of one or two. These findings suggest that the majority of participants possess substantial familiarity and comfort with digital technologies and online platforms.

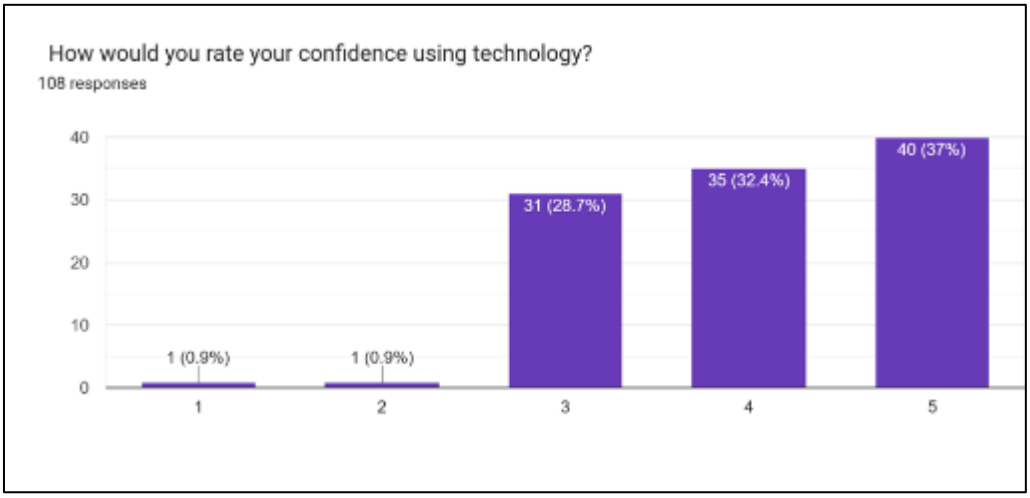

Figure 1 Self Reported Technology Confidence Among Participants

Participants also demonstrated strong awareness of privacy related risks. Figure 2 shows participant perceptions regarding the seriousness of application data misuse. More than two thirds of respondents (68.6%) rated data misuse as either four or five on a five point scale, indicating that most participants recognized the potential consequences associated with inappropriate collection, sharing, or handling of personal information. Only 9.3% of respondents rated data misuse as one or two, suggesting that concern regarding digital privacy was widespread throughout the participant population.

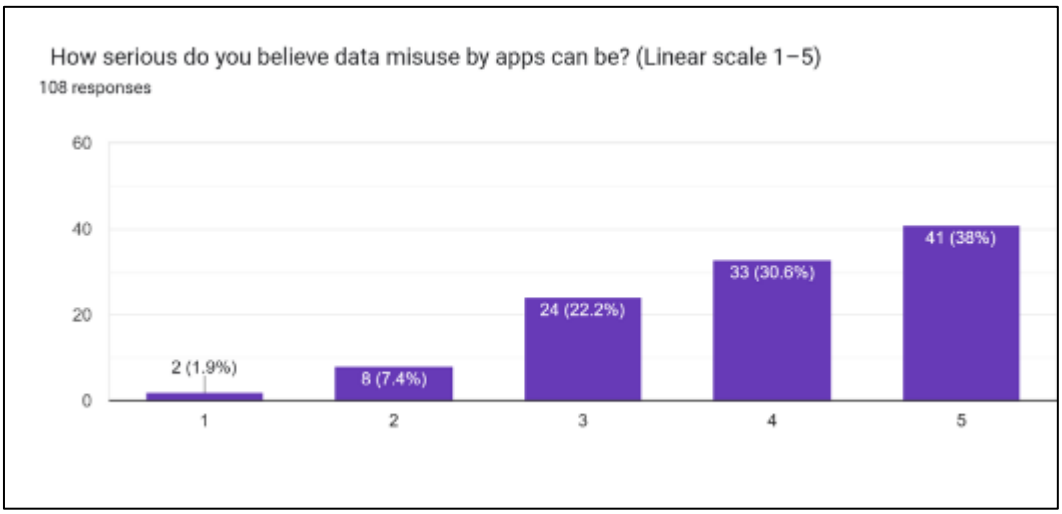

Figure 2 Participant perceptions regarding the seriousness of application data misuse. Higher ratings indicate stronger recognition of privacy and security risks associated with improper handling of personal information.

However, the results revealed that awareness of privacy risks did not consistently translate into privacy protective behavior. Figure 3 illustrates participant privacy policy reading habits prior to installing or using digital applications. d 59.3% of respondents reported that they either never (32.4%) or rarely (26.9%) read privacy policies. In contrast, only a small proportion of participants reported reading privacy policies often or always. These findings indicate that

although participants generally understood privacy risks and recognized the seriousness of data misuse, many did not routinely engage in one of the most basic privacy protective behaviors available to users.

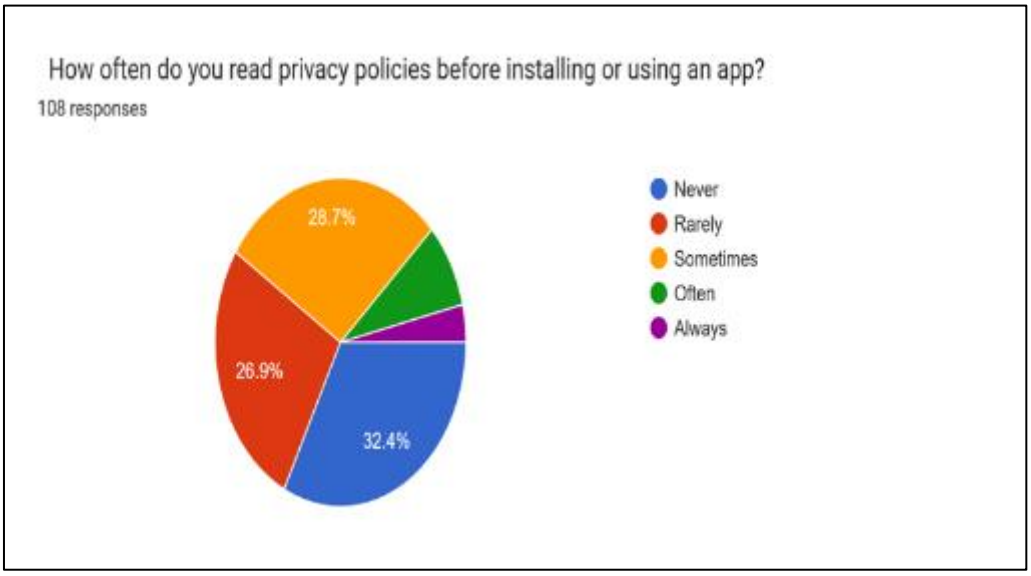

Figure 3 Frequency with which participants reported reading privacy policies before installing or using digital applications. Responses provide an indicator of privacy protective behavior.

This discrepancy between privacy awareness and actual behavior is consistent with the privacy paradox, a phenomenon in which individuals express concern about privacy while simultaneously engaging in behaviors that expose personal information (Norberg et al., [4]; Barth & de Jong, [5]; Kokolakis, [6]). The current findings provide evidence of this phenomenon among young adult technology users. Participants appeared knowledgeable about privacy risks and confident in their ability to navigate digital environments, yet many continued to avoid reviewing privacy information before accepting application terms and conditions. Several explanations may account for this behavior; one explanation is convenience bias. Digital services are often designed to prioritize speed, accessibility, and immediate access to functionality. As a result, users may choose convenience over careful evaluation of privacy disclosures. Acquisti et al. [7] argued that privacy decisions are frequently influenced by cognitive limitations, competing priorities, and contextual factors rather than deliberate evaluation of risk. Similarly, Martin [8] noted that users often place practical value on convenience and service functionality even when they recognize privacy concerns.

Technology confidence may also contribute to the awareness behavior gap observed in this study. Participants who are highly confident in their technology skills may believe they can identify or manage risks without carefully reviewing privacy information. This perception may create a false sense of security that reduces motivation to engage in protective actions. Adjerid et al. [9] reported that privacy decisions are often influenced by subjective perceptions of risk rather than objective assessments of potential consequences. Consequently, individuals may underestimate their personal vulnerability despite acknowledging broader privacy threats.

Another possible explanation involves optimism bias. Weinstein [10] described optimism bias as the tendency for individuals to believe that negative events are less likely to happen to them than to others. Participants in the present study may recognize that data misuse represents a serious societal concern while simultaneously assuming that they are unlikely to experience adverse consequences themselves. Such perceptions can reduce motivation to engage in preventative privacy behaviors despite awareness of potential risks. The findings are also consistent with previous privacy paradox literature. Sabrina et al. [11] and Lee and Cranage [12] reported that users frequently continue interacting with digital services despite expressing privacy concerns. Kokolakis [6] further concluded that privacy attitudes and privacy behaviors often fail to align, particularly when users perceive benefits such as convenience, personalization, or ease of use.

The results support the study thesis that awareness alone is insufficient to motivate cybersecurity protective action. Participants reported high levels of technology confidence and recognized the seriousness of data misuse, yet many did not consistently engage in privacy protective behaviors such as reading privacy policies. These findings suggest that improving cybersecurity outcomes may require approaches beyond awareness campaigns alone. Privacy by default

system designs, simplified consent mechanisms, and targeted cybersecurity education may help bridge the gap between privacy knowledge and privacy behavior among technology users.

4. Conclusion

The findings of this study provide evidence of a privacy awareness behavior gap among young adult technology users. Participants reported high levels of technology confidence, demonstrated awareness of application data collection practices, and recognized the seriousness of data misuse. Despite this awareness, many respondents reported that they rarely or never read privacy policies before installing or using digital applications. These results indicate that awareness of privacy risks does not necessarily translate into privacy protective behavior.

The findings are consistent with previous studies that have identified a disconnect between privacy concerns and actual privacy related behaviors. Individuals frequently express concern regarding the collection and use of personal information while continuing to engage in behaviors that may expose their data. The present study demonstrates that this gap remains evident among a population characterized by high levels of technology confidence and digital engagement.

The findings suggest that privacy related decision making is influenced by factors beyond awareness and knowledge. Participants generally understood that data misuse can have serious consequences, yet many did not consistently engage in one of the most accessible privacy protective behaviors available to users. Privacy decisions are often shaped by cognitive limitations, competing priorities, perceived benefits, and contextual influences. Digital environments are designed to provide immediate access to information and services, often encouraging users to prioritize convenience over careful evaluation of privacy implications.

Convenience appears to play a significant role in the awareness behavior gap identified in this study. Digital applications frequently require users to accept terms of service and privacy policies before accessing desired functionality. Reading lengthy privacy disclosures can require substantial time and effort, creating incentives for users to bypass these materials in favor of immediate access. Users often accept privacy risks in exchange for convenience, personalization, and rapid access to services. These factors help explain why awareness of privacy risks may not consistently result in privacy protective behavior.

Technology confidence may also contribute to the observed gap. Participants reported substantial confidence in their ability to use digital technologies, which may create a perception that privacy risks can be managed without careful review of privacy information. Individuals who perceive themselves as technologically competent may underestimate their vulnerability to privacy threats or the potential consequences of data collection and sharing practices. Public education campaigns often focus on increasing awareness of privacy threats and encouraging users to adopt safer behaviors. While awareness remains important, the results of this study suggest that knowledge alone may not be sufficient to produce meaningful behavioral change. Many individuals possess an understanding of privacy risks and available protection strategies but do not consistently apply those strategies in practice. Educational initiatives remain valuable but should be combined with approaches that address behavioral and environmental influences on decision making.

Organizations and software developers should adopt privacy by design principles that reduce reliance on user action. Privacy protective settings should be enabled by default whenever possible, limiting the burden placed on users to identify and activate protections independently. Simplified privacy notices, layered consent mechanisms, and transparent explanations of data collection practices may improve user engagement with privacy information. Designers should also consider reducing the complexity and length of privacy policies to improve accessibility and comprehension. Educational institutions and cybersecurity professionals should continue promoting privacy literacy while incorporating behavioral considerations into training programs. Instruction that focuses solely on awareness may be insufficient if users continue to encounter environments that reward convenience over privacy protection. Educational efforts should emphasize practical decision making strategies, risk evaluation skills, and methods for recognizing situations in which privacy may be compromised. The results of this study demonstrate that privacy awareness, technology confidence, and recognition of privacy risks do not automatically lead to privacy protective behavior. Improving cybersecurity outcomes requires approaches that address both knowledge and behavior. Privacy by design practices, user centered privacy protections, and targeted educational interventions may help reduce the gap between awareness and action, ultimately supporting more effective protection of personal information in increasingly digital environments.

Limitations

Several limitations should be considered when interpreting the findings of this study. First, the participant population was heavily student dominated, with individuals between the ages of 18 to 24 representing most respondents. As a result, the findings may not fully represent broader demographic populations with different educational backgrounds, technology usage behaviors, or digital literacy levels.

Compliance with ethical standards

Acknowledgments

The authors would like to thank all survey participants who contributed to this study.

Disclosure of conflict of interest

The authors declare no conflict of interest.

Statement of informed consent

Informed consent was obtained from all individual participants included in the study.

References

[1] Dinev T and Hart P. (2006). An extended privacy calculus model for ecommerce transactions. Information Systems Research, 17(1), 61-80.

[2] Beldad A, De Jong M and Steehouder M. (2011). I trust not therefore it must be risky: Determinants of the perceived risks of disclosing personal data for e government transactions. Computers in Human Behavior, 27(6), 2231-2240.

[3] Debatin B, Lovejoy JP, Horn AK and Hughes BN. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. Journal of Computer Mediated Communication, 15(1), 83-108.

[4] Norberg PA, Horne DR and Horne DA. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. Journal of Consumer Affairs, 41(1), 100-126.

[5] Barth S and de Jong MDT. (2017). The privacy paradox: Investigating discrepancies between expressed privacy concerns and actual online behavior. Telematics and Informatics, 34(7), 1038-1058.

[6] Kokolakis S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. Computers and Security, 64, 122-134.

[7] Acquisti A, Brandimarte L and Loewenstein G. (2015). Privacy and human behavior in the age of information. Science, 347(6221), 509-514.

[8] Martin K. (2020). Breaking the privacy paradox: The value of privacy and associated duty of firms. Business Ethics Quarterly, 30(1), 65-96.

[9] Adjerid I, Acquisti A, Brandimarte L and Loewenstein G. (2018). Beyond the privacy paradox: Objective versus relative risk in privacy decision making. MIS Quarterly, 42(2), 465-488.

[10] Weinstein ND. (1980). Unrealistic optimism about future life events. Journal of Personality and Social Psychology, 39(5), 806-820.

[11] Sabrina N et al. (2017). Beyond the personalization privacy paradox: Privacy valuation, transparency features, and service personalization. Journal of Management Information Systems, 34(2), 369-400.

[12] Lee CH and Cranage DA. (2011). Personalisation privacy paradox: The effects of personalisation and privacy assurance on customer responses to travel web sites. Tourism Management, 32(5), 987-994.

[13] Sutanto J, Palme E, Tan CH and Phang CW. (2013). Addressing the personalization privacy paradox: An empirical assessment from a field experiment on smartphone users. MIS Quarterly, 37(4), 1141-1164.

[14] Kehr F, Kowatsch T, Wentzel D and Fleisch E. (2015). Blissfully ignorant: The effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. Information Systems Journal, 25(6), 607-635.

[15] Park YJ. (2013). Digital literacy and privacy behavior online. Communication Research, 40(2), 215-236.

[16] Trepte S, Teutsch D, Masur PK, Eicher C, Fischer M, Hennhöfer A and Lind F. (2015). Do people know about privacy and data protection strategies? Towards the online privacy literacy scale (OPLIS). In: Reforming European Data Protection Law. Springer, 333-365.