



Issues in Informing Science + Information Technology

An Official Publication
of the Informing Science Institute
InformingScience.org

IISIT.org

Volume 23, 2026

PRIVACY PERCEPTIONS IN USING GENERATIVE AI TOOLS AMONG ISRAELI STUDENTS

Maor Weinberger*	Bar-Ilan University, Ramat Gan, Israel	maor89@gmail.com
Dan Bouhnik	Jerusalem College of Technology, Jerusalem, Israel	bouhnik@jct.ac.il

* Corresponding author

ABSTRACT

Aim/Purpose	Generative artificial intelligence (GAI) tools based on Large Language Models (LLMs) are increasingly used to enrich knowledge, support decision-making, and generate new content. However, as beneficial as these tools may be, they also store vast amounts of information, which might jeopardize users' privacy and data protection. Thus, users who wish to maximize the benefits of GAI tools must relinquish some of their privacy, a phenomenon known in the literature as the "privacy paradox."
Background	This research aims to determine whether users experience privacy concerns when using GAI tools by examining the relationships among privacy concerns, trust in AI operators, and actual usage patterns among students. It considers different theoretical models (Privacy Calculus, TAM, and UTAUT) to determine if perceived benefits outweigh the risks of information disclosure.
Methodology	To examine this issue, a quantitative pilot study was conducted using closed-ended questionnaires distributed to 121 students in Israel. Data were analyzed using Pearson correlations and a stepwise multivariate linear regression to identify predictors of GAI tool usage.
Contribution	This study contributes to the body of knowledge by being the first to examine GAI privacy perceptions within Israeli academia. It challenges the universal applicability of the privacy paradox by demonstrating that, in this specific context, trust and proficiency are more decisive than privacy concerns.
Findings	The findings indicate that AI-related privacy concerns have no significant correlation with the amount of GenAI tool usage. However, higher levels of trust in the operators of GenAI tools were found to positively affect the amount of GenAI tool use and Internet proficiency.

Editor: Eli Cohen | Received: February 12, 2026 | Revised: April 7, May 16, 2026 | Accepted: June 6, 2026
Cite as: Weinberger, M., & Bouhnik, D. (2026). Privacy perceptions in using generative AI tools among Israeli students. *Issues in Informing Science and Information Technology*, 23, Article 3. <https://doi.org/10.28945/5806>

(CC BY-NC 4.0) This article is licensed to you under a [Creative Commons Attribution-NonCommercial 4.0 International License](https://creativecommons.org/licenses/by-nc/4.0/). When you copy and redistribute this paper in full or in part, you need to provide proper attribution to it to ensure that others can later locate this work (and to ensure that others do not accuse you of plagiarism). You may (and we encourage you to) adapt, remix, transform, and build upon the material for any non-commercial purposes. This license does not permit you to use this material for commercial purposes.

Recommendations for Practitioners	Operators of GAI tools should prioritize transparency regarding data collection and usage to build user trust, which directly influences adoption rates. Educational institutions should integrate AI literacy programs to increase students' proficiency, thereby fostering more confident and effective use of AI tools.
Recommendation for Researchers	Researchers should move beyond simple correlational studies to explore causal links between emotional engagement and data disclosure. It is also recommended to use validated, multidimensional scales to measure privacy concerns rather than broad self-reports.
Impact on Society	The findings suggest that as users feel safe and knowledgeable about digital risks, their intent to utilize GAI increases, potentially accelerating the integration of AI into work and study processes.
Future Research	Future studies should employ larger, more diverse samples across multiple institutions to test the generalizability of these findings. Additionally, a mixed-methods approach, including qualitative interviews, could provide a deeper understanding of the privacy paradox.
Keywords	Generative AI, privacy concern, privacy paradox

INTRODUCTION

The Internet continues to evolve in tandem with the online services it provides. If Web 2.0 revolutionized the Internet, turning users from passive readers to active content creators, the emerging Web 3.0 era has further revolutionized the Internet, incorporating intelligent bots and learning machines into users' workflows (Gan et al., 2023). Today, online users utilize generative artificial intelligence (GAI) tools based on large language models (LLMs) for diverse activities, such as gathering information and writing, editing, or developing content (Tomlinson et al., 2025). However, as beneficial as these tools may be, they also store vast amounts of information that may not be properly protected and may even be disseminated to third parties. This may elevate users' privacy concerns (Zhou & Wu, 2025).

But even if users are concerned about how their data is handled by GAI tools, it might not be enough to change their behavior and keep them from using these extremely beneficial tools. The discrepancy between individuals' stated privacy concerns and their actual behavior is a widely discussed phenomenon in the literature referred to as the "privacy paradox" (Barnes, 2006; Norberg et al., 2007). Past research found that despite their attitudes and intentions, users voluntarily disclose personal information online (Debatin et al., 2009; Dienlin & Trepte, 2015; Guo et al., 2016; Weinberger et al., 2017). Several hypotheses have been suggested to explain users' online self-disclosure behavior, including the knowledge gap hypothesis – a lack of awareness of the risks posed by information disclosure (Barnes, 2006; Debatin et al., 2009) or a lack of knowledge regarding privacy-enhancing tools and techniques (Trepte et al., 2015), and the uses and gratification theory – a lack of willingness to forfeit the benefits of information disclosure, such as social benefits (Debatin et al., 2009; Trepte et al., 2015). In addition, a theory of optimistic bias, also known as unrealistic optimism or comparative risk judgments (Weinstein, 1989), was considered as an explanation of online self-disclosure where users perceive themselves to be less vulnerable to these risks than their peers (Baek et al., 2014; H. Cho, 2012; H. Cho et al., 2010).

Some studies even examined this phenomenon in the context of GAI tools usage. Victor-Nyebuchi (2025) discovered that privacy concerns negatively impact users' trust in AI systems, despite their recognition of the benefits of personalization. However, other studies (Choi et al., 2025; Olatunde & Mohamed, 2025) found that users who distrust AI privacy still engage with AI-powered tools

(Olatunde & Mohamed, 2025) and that the potential benefits of personalization might outweigh privacy concerns (Choi et al., 2025).

This research aims to identify whether users experience privacy concerns while using GAI tools. The research will build on previous studies that investigated these issues and will strive to add to the existing literature by examining them among students, who tend to have a higher digital orientation and proficiency in the online environment and are thus expected to further stress the privacy paradox discrepancy. The main research question sought to verify whether this is indeed the case: do privacy concerns influence engagement with GAI tools (RQ1), and does trust play a role in the decision to use these tools (RQ2)? In addition, as socio-demographic factors were also found in the past to be associated with privacy-protective behavior (e.g., Dinev & Hart, 2005; Thelwall & Vis, 2017), this research examined whether and to what extent socio-demographic factors (gender, age, and education) affect privacy concerns (RQ3a) and GAI tool usage (RQ3b). Finally, the study examined the main factors that predict the amount of GAI tool usage (RQ4). While studies investigating the influence of privacy concerns among university students regarding GAI use (e.g., Wang et al., 2025) are currently very few, as far as we know, this is the first study to examine these issues in Israeli academia.

Despite the growing body of literature on AI adoption, a significant research gap remains regarding how privacy concerns manifest in academic environments, particularly in Israel. This study addresses this gap by examining the interplay between trust, internet proficiency, and GAI usage among students.

RELATED WORK

The literature review consists of two scopes: first, it explores the trade-off between the benefits of self-disclosure and users' willingness to protect their privacy; second, it reviews the rise in the use of generative AI (GAI) tools and surveys the privacy issues related to them.

THE BENEFITS OF SELF-DISCLOSURE VERSUS THE WILLINGNESS FOR PRIVACY PROTECTION

To understand why students use GAI despite potential risks, we must first examine the psychological and economic trade-offs inherent in online interactions.

The online world has become an integral part of our everyday lives and, as such, customer-provider interactions often mirror those in the physical world. Thus, as in "real life," the constant engagement between users and online service providers often raises tensions that result in protective behavior (Chellappa & Sin, 2005). Commercial entities on the Internet routinely examine customers' online behavior to gain insights into their purchasing habits and preferences (Punj, 2017). Furthermore, companies request access to personal data to customize advertisements and product recommendations, aiming to boost sales (Bandara et al., 2020; Dinev & Hart, 2005; Zeng et al., 2021). According to Dinev and Hart (2006), in electronic commerce transactions, users act according to the privacy calculus model, i.e., weighing the risks and benefits of disclosing their information. Previous studies found that users are generally willing to sacrifice a certain degree of their privacy for the benefits of personalization, and this exchange may be beneficial for both the sellers and the consumers (Karwatzki et al., 2017); however, when consumers feel that the invasion of their personal space is excessive and their privacy concern rises, they might forfeit the benefits of online personalization and engage in privacy protective behavior (Awad & Krishnan, 2006; Chellappa & Sin, 2005; Sheng et al., 2008; Smith et al., 2011). Socio-demographic factors might also influence privacy concerns and self-disclosure. Higher levels of education have historically been associated with greater concern about online privacy (Rainie et al., 2013; Sheehan, 2002). Thelwall and Vis (2017) found that women are more concerned about their online privacy than men and tend to engage more in privacy-protective behavior. Van den Broeck et al. (2015) reported that younger adults exhibit higher privacy concerns than older adults.

The equilibrium between self-disclosure and privacy protection is thoroughly discussed in past studies in relation to the personalization-privacy trade-off (Karwatzki et al., 2017; Weinberger & Bouhnik, 2018) and the privacy paradox, i.e., the discrepancy between users' online privacy attitudes and their actual behavior that reflects the opposite (Barnes, 2006; Norberg et al., 2007; Weinberger et al., 2017). These trade-offs have been investigated in the context of different online activities, including e-commerce (Awad & Krishnan, 2006; Chellappa & Sin, 2005), social media engagement (Debatin et al., 2009; Lee et al., 2013; Taddicken, 2014), and even usage of music streaming applications (Weinberger & Bouhnik, 2018).

They were also examined in the context of the Technology Acceptance Model (TAM) (Davis, 1986, 1989), an information systems theory that explains how users come to accept and use a technology. The model suggests that when users are presented with a new technology, certain factors, such as perceived ease of use and perceived usefulness, affect their decision about how and when they will use it (Saadé & Bahli, 2005; Silva, 2015). Pavlou (2003) also integrated trust and perceived risk into TAM, highlighting trust's critical role in reducing the high perceived risk and uncertainty inherent in impersonal, online transactions. The new model suggests that building trust and reducing perceived risk are equally important to ensure user engagement. Venkatesh et al. (2003) developed an even more evolved model that combined eight prominent IT adoption models, including TAM, to determine user acceptance and technology usage behavior. The Unified Theory of Acceptance and Use of Technology (UTAUT) consists of four core elements: Performance Expectancy (the belief using the system will improve job performance), Effort Expectancy (the perceived ease of using the technology), Social Influence (the user's perception that important others believe they should use the new system), and Facilitating Conditions (the belief that an organizational and technical infrastructure exists to support the use of the system). These four elements are moderated by gender, age, experience, and voluntariness of use.

The traditional privacy paradox, largely studied in social media and e-commerce, takes on a new dimension with the emergence of newer technologies based on artificial intelligence (AI) and the Internet of Things (IoT), particularly LLM-powered generative AI platforms, which present an even greater challenge. While these technologies offer significant advantages for personal convenience, they simultaneously introduce new concerns regarding user privacy (Conger et al., 2013).

THE RISE OF GAI TOOLS AND THE DANGERS TO ONLINE PRIVACY

Building on these general privacy theories, the rapid adoption of LLM-based GAI tools presents a unique case study in how users navigate trust and transparency.

The expansion of generative AI algorithms has led to the development of conversational AI services, such as OpenAI's ChatGPT, Google's Gemini, and Anthropic's Claude, which can provide immediate responses on almost any subject (K. Cho et al., 2025). Due to their ease of use, GAI tools are increasingly adopted by online users for tasks such as information retrieval, content creation, editing, and development (Tomlinson et al., 2025). These tools are also used in different fields, including education (Nguyen, 2025), art (Epstein et al., 2023), academic research (Perkins & Roe, 2025), and even healthcare (Updety et al., 2023), to enhance capabilities and develop novel methods to advance them.

Despite their wide utility, GAI tools raise privacy concerns because they store substantial amounts of information that may not be adequately protected or shared with third parties (Zhou & Wu, 2025). This is despite international data protection standards, such as the EU's General Data Protection Regulation (GDPR), pushing for "algorithmic transparency" in AI development and deployment (Chaudhary, 2024). Thus, when the user seeks to use these tools, they might face the aforementioned dilemma: whether to harness the many benefits of GAI tools at the expense of their privacy or to keep their personal information safe while losing some of those benefits.

Previous studies investigated the possible effect of privacy-related issues on users' intent to use GAI tools. Wang et al. (2025), who investigated these issues among university students, found that privacy

concerns are among the most critical ethical issues in the application of GAI tools. Chakraborty et al. (2025) examined how privacy concerns impact the use of GAI tools within the hospitality sector. Their findings indicated that while privacy concerns initially reduce users' likelihood of engaging with GAI tools, this negative effect diminishes as users gain a better understanding of the associated risks. Likewise, Victor-Nyebuchi (2025), who explored AI-driven personalization in social media marketing, found that privacy concerns negatively affect trust in AI systems, despite users' awareness of the benefits of personalization. The study found that privacy awareness might trigger cautious behaviors, such as regularly adjusting privacy settings or limiting interactions with personalized advertisements.

On the other hand, Meng and Liu (2025) reported that emotional engagement with GAI tools can influence users' privacy-related decisions. They found that an emotional connection to a GAI tool, such as feeling understood by the chatbot, can make users disclose information, even when they are aware of privacy risks. Choi et al. (2025) found that while most GAI users experience privacy concerns about data leaks and disclosures without consent, the potential benefits of personalization outweigh these concerns, vividly reflecting the privacy paradox. This phenomenon is further supported by Olatunde and Mohamed (2025), whose research indicated that many users continue to interact with AI-powered tools despite having distrust concerning AI privacy.

This research seeks to determine whether users, particularly students, experience privacy concerns when using GAI tools and whether these concerns influence their intent to use them. In addition, it examines whether trust and socio-demographic factors affect these decisions. Finally, the research variables are used in a predictive model to identify the main factors that predict the amount of GAI tool usage. While previous studies examined these issues in general contexts (such as social media), there is a research gap regarding generative AI within specific cultural and educational frameworks, such as Israeli technical educational institutions. This study fills that gap by examining whether trust and internet proficiency can overcome privacy concerns in a high-stakes academic environment.

METHODOLOGY

To examine the earlier described issues, we conducted a pilot study among 121 students from the Jerusalem College of Technology: (52.1%) men and (47.9%) women (age range: 18-34), via a quantitative method, using online closed-ended questionnaires. Table 1 presents the demographic characteristics of the sample.

Table 1. Demographic distribution of the sample

Variable		N(%)
Sex	Male	63 (52.1%)
	Female	58 (47.9%)
Age	Lower (17-19)	62 (51.2%)
	Intermediate (21-22)	30 (24.8%)
	Upper (23+)	29 (24.0%)
Birth Place	Israel	109 (90.1%)
	Other	12 (9.9%)
Departments	Electrical/Electro-Optics Engineering	34 (28.1%)
	Industrial Engineering	15 (12.4%)
	Computer Science/Software Engineering	62 (51.2%)
	Information Science/Bioinformatics	7 (5.8%)
	Pharmaceutics	3 (2.5%)

The study was conducted in accordance with the American Psychological Association (APA) ethical requirements. The participants were informed that the questionnaire is anonymous and that the gathered information will be used for research purposes only. The closed-ended questionnaire consisted of 14 items.

RESEARCH VARIABLES AND VALIDATION METHOD

The questionnaire used in the study comprised 14 items (see Appendix), organized into five distinct sections. The *first section* (Part A, items 1-5) focused on demographic variables, including gender, age, birthplace, department, and self-reported Internet proficiency. These variables have previously been linked to privacy concerns and privacy-protective behavior (e.g., Dinev & Hart, 2005; Thelwall & Vis, 2017). The *second section* (Part B, item 6) addressed participants' general level of concern about protecting their personal information online. The *third section* (Part C, item 7) sought to verify whether the participant uses GAI tools. Participants who replied "No" did not complete the rest of the questionnaire. The *fourth section* (Part D, items 8-9) explored the extent of participants' use of the GAI tool and whether they have a paid account for any of the tools they use. The *fifth section* (Part E, items 10-14) assessed participants' privacy-related concerns regarding GAI tools and their level of trust in the GAI tool operators. These variables have been examined in the literature (e.g., Olatunde & Mohamed, 2025).

Based on the above-described questionnaire, the following research variables were defined. Research questions that are addressed by specific variables and statistical procedures appear in parentheses. Other variables and statistical procedures were tested for descriptive purposes.

1. Socio-demographic variables:

- Gender – male/female (part A, item 1).
- Age – varied between 17 and 34 (part A, item 2).
- Birthplace – Israel/other (part A, item 3).
- Department – choose one of 12 options (part A, item 4).
- Internet proficiency level (part A, item 5) was measured by a single indicator assessing participants' self-reported proficiency with computers and the Internet. The participants' responses were recorded on a Likert scale with ratings ranging from 1 (not proficient at all) to 5 (very high level of proficiency).

The differences between the socio-demographic subgroups with regard to the dependent variable (tendency toward identity falsification) were examined using a series of t-tests and ANOVA.

2. General privacy concern:

- The level of privacy concern (part B, item 6) was measured using a single indicator assessing participants' concern about protecting their online information. The participants' responses were recorded on a Likert scale with ratings ranging from 1 (not concerned at all) to 5 (very highly concerned).

3. GAI usage:

- GAI usage (Part C, item 7) – a binary variable indicating whether participants used GAI tools. It was mostly used to filter out the participants who do not use these tools. Participants could respond "Yes" (coded as 1) or "No" (coded as 0).

4. GAI usage habits:

- GAI usage frequency (Part D, item 8) was measured using a single indicator that assessed participants' use of GAI tools. The participants' responses were recorded using a Likert scale with ratings ranging from 1 (rarely) to 5 (usually).

- Paid account (Part D, item 9) - this was a binary variable that examined whether the user has a paid account on one of the GAI tools that they use. The participants could either respond “Yes” (coded as 1) or “No” (coded as 0).

5. GAI privacy concern:

- GAI personal information disclosure (Part E, item 10) was a binary variable indicating whether participants had ever disclosed their personal details to the GAI chatbot. Participants could respond “Yes” (coded as 1) or “No” (coded as 0).
- GAI trust (Part E, item 11) was measured by one indicator that examined the participants’ level of trust in the operators of the GAI tools they use. The participants’ responses were recorded on a Likert scale with ratings ranging from 1 (not concerned at all) to 5 (very highly concerned).
- GAI privacy concern (Part E, item 12) was measured by one indicator that examined the participants’ level of concern for the protection of their information while using GAI tools. The participants’ responses were recorded on a Likert scale with ratings ranging from 1 (not concerned at all) to 5 (very highly concerned).
- GAI data dissemination concern (Part E, item 13) was measured by one indicator that examined the participants’ level of concern for the dissemination of the data they provide using GAI tools to external parties. The participants’ responses were recorded on a Likert scale with ratings ranging from 1 (not concerned at all) to 5 (very highly concerned).
- GAI profiling concern (Part E, item 14) was measured by one indicator that examined the participants’ level of concern that the data they reveal to the chatbot will be used to profile their online accounts. The participants’ responses were recorded on a Likert scale with ratings ranging from 1 (not concerned at all) to 5 (very highly concerned).

The scale used to measure privacy concerns (Part B, item 6, Part E, items 12-14) demonstrated high internal consistency, with a Cronbach’s alpha of $\alpha = 0.74$.

To predict the amount of GAI tool usage in the context of privacy preservation, we performed a multivariate linear regression analysis, controlling for gender, age, Internet proficiency, privacy concerns when using GAI tools, and trust in the operators of GAI tools. While the sample size ($N = 121$) is appropriate for a pilot study, it provides sufficient statistical power to detect medium-to-large effect sizes ($f^2 = 0.15$) in a multivariate linear regression.

FINDINGS

Almost 96% of the participants ($N = 116$) reported using GAI tools for various purposes, including work (24%), studies (94%), and personal needs (84%), with 9% having a paid account on at least one service.

The participants reported medium-high levels of general privacy concern while using the Internet ($M = 3.36$, $SD = 1.24$). They showed similar, though slightly lower, levels of concern while using GAI tools ($M = 3.10$, $SD = 1.28$). There is a strong, positive Pearson correlation between these two variables ($r(114) = 0.58$, $p < 0.001$). These findings also align with low-to-medium levels of trust in the operators of the GAI tools ($M = 2.47$, $SD = 1.09$).

The participants also showed medium-high concern about the dissemination of the data they provide using GAI tools to external parties ($M = 3.27$, $SD = 1.37$) and about the possibility that this data will be used to profile their online accounts ($M = 3.25$, $SD = 1.28$). There is a positive, medium Pearson correlation between GAI privacy concern and each of these two variables ($r(114) = 0.46$, $p < 0.001$; $r(114) = 0.33$, $p < 0.001$).

RQ1. Do privacy concerns influence engagement with GAI tools?

RQ2. Does trust play a role in the decision to use GAI tools?

We did not find correlations between participants' privacy concerns when using GAI tools and their usage amount ($r(114) = 0.37, p > 0.05$) or their tendency to reveal personal details to the chatbot ($r(114) = 0.15, p > 0.05$). However, we did find a positive correlation (though weak) between the participants' level of trust in the operators of the GAI tools and their usage amount ($r(114) = 0.29, p < 0.01$), i.e., the higher the level of the participant's trust in the chatbot, the higher the usage amount.

RQ3a. Whether and to what extent socio-demographic factors (gender and age) affect privacy concerns?

RQ3b. Whether and to what extent socio-demographic factors (gender and age) affect GAI tool usage?

As for demographic differences, we did not find significant demographic differences regarding privacy concerns or GAI tool usage. However, we did find significant differences between the age groups regarding the tendency to reveal personal details to the GAI chatbot ($F(2,113) = 5.22, p < 0.01$), with the intermediate age group (21-22) having the highest tendency to reveal details, followed by the lower age group (17-19).

RQ4. What are the main factors that predict the amount of GAI tool usage?

Subsequently, we examined the role of some of the aforementioned factors in predicting the amount of GAI tool usage. A multivariate linear regression analysis was therefore performed, using the various independent variables described in the Methods section. The regression was conducted using the stepwise method, which considers only significant variables. Table 2 presents the regression coefficients for predicting the amount of GAI tool usage in the context of privacy preservation.

Table 2. The linear regression coefficient for predicting the amount of GAI tool usage

Predictors	Dependent variable: The extent of GAI tool usage			
	β	SE	B	t
AI Trust	0.29	0.09	0.29	3.24**
Proficiency	0.18	0.09	0.18	1.99*

* $p < 0.05$, ** $p < 0.01$

Table 2 shows that the regression for predicting the amount of GAI tool usage was significant, $F(2,113) = 7.52, p < 0.01$, with the predictor variables: trust in the operators of GAI tools and Internet proficiency, accounting for 11.7% of the explained variance (trust was found more significant than proficiency).

As participants' trust in GAI tool operators increases, so does usage. Namely, the higher the participants' trust in the operators of GAI tools, the more likely they are to use them. Additionally, the results suggest that participants with higher Internet proficiency tend to use GAI tools more frequently.

DISCUSSION AND CONCLUSION

LLM-based Generative AI tools have become an integral part of our lives, helping users learn, make informed decisions, and create high-quality content with ease. However, along with the widespread benefits of the tools, significant risks to users' privacy also arise. This puts users in a constant dilemma over whether to relinquish their privacy for the benefits of using GAI tools or to preserve it at any cost.

In contrast to previous studies that found privacy concerns negatively affect users' intent to use GAI tools (Chakraborty et al., 2025; Victor-Nyebuchi, 2025), this research found that AI-related privacy concerns have no significant correlation with the amount of GAI tool usage ($r(114) = -0.37, p > 0.05$) or the users' tendency to reveal personal details to the chatbot ($r(114) = 0.15, p > 0.05$) (**RQ1**). Thus, the privacy paradox is not observed in this specific sample. However, we found a positive correlation between participants' level of trust in the operators of the GAI tools and their use of the tools ($r(114) = 0.29, p < 0.01$) (**RQ2**), indicating that users who have higher trust in the chatbot use it more. This finding partially contradicts earlier findings indicating that users continue to interact with AI-powered tools despite having distrust concerning AI privacy (Olatunde & Mohamed, 2025).

As for demographic differences, despite earlier studies that found privacy concerns might be influenced by socio-demographic factors, such as education (Rainie et al., 2013; Sheehan, 2002), gender (Thelwall & Vis, 2017), and age (Van den Broeck et al., 2015), this research did not reveal significant demographic differences regarding privacy concerns or GAI tool usage (**RQ3a** and **RQ3b**); however, we did find significant differences between the age groups regarding the tendency to reveal personal details to the GAI chatbot ($F(2,113) = 5.22, p < 0.01$), with the intermediate age group (21-22) having the highest tendency to reveal details, followed by the lower age group (17-19).

Finally, a multivariate linear regression was employed to examine the main factors that predict the amount of GAI tool usage (**RQ4**). The regression found that as participants' trust in the operators of GAI tools and their internet proficiency increase, so does their use of GAI tools. This shows that as users feel safe and knowledgeable about the dangers to their personal information, their intent to use GAI tools increases. This finding supports IT adoption models, such as Pavlou's (2003) improved TAM model, which claims that trust reduces users' perceived risk and improves user engagement with online platforms.

In light of these findings, we call on the operators of GAI tools to increase transparency about the information their services collect, build user trust, and reduce privacy concerns. This may benefit them and their customers in the long run.

LIMITATIONS AND FUTURE RESEARCH

While this study provides early insights into GAI adoption in Israeli academia, several limitations must be acknowledged. First, as a pilot study with a sample of 121 students from a single technical institution, the findings may not be generalizable to the broader Israeli population or global student bodies. The sample also featured a high concentration of students from engineering and computer science departments (approximately 80%), who likely possess above-average technical literacy. Second, the research relied on self-reported measures for "usage amount" and "internet proficiency," which are subject to subjective bias. Third, the cross-sectional design captures a "snapshot" in time; as GAI tools evolve and regulatory frameworks like the GDPR or local Israeli privacy laws become more prominent, user perceptions may shift. Future research should utilize larger, more diverse samples across multiple institutions and incorporate longitudinal designs to track how trust and privacy concerns change as users gain more experience with these tools. Additionally, a mixed-methods approach, including qualitative interviews, could provide a deeper psychological understanding of the privacy paradox that purely quantitative data may miss.

REFERENCES

- Awad, N. F., & Krishnan, M. S. (2006). The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS Quarterly*, 30(1), 13-28. <https://doi.org/10.2307/25148715>

- Baek, Y. M., Kim, E. M., & Bae, Y. (2014). My privacy is okay, but theirs is endangered: Why comparative optimism matters in online privacy concerns. *Computers in Human Behavior*, 31, 48-56. <https://doi.org/10.1016/j.chb.2013.10.010>
- Bandara, R., Fernando, M., & Akter, S. (2020). Explicating the privacy paradox: A qualitative inquiry of online shopping consumers. *Journal of Retailing and Consumer Services*, 52, 101947. <https://doi.org/10.1016/j.jretconser.2019.101947>
- Barnes, B. S. (2006). A privacy-paradox: Social networking in the United States. *First Monday*, 11(9). <https://doi.org/10.5210/fm.v11i9.1394>
- Chakraborty, D., Gunasekaran, A., & Subramanian, G. (2025). Privacy vs. personalization: GENAI's role in technology adoption. *Journal of Computer Information Systems*. <https://doi.org/10.1080/08874417.2025.2534545>
- Chaudhary, G. (2024). Unveiling the black box: Bringing algorithmic transparency to AI. *Masaryk University Journal of Law and Technology*, 18(1), 93-122. <https://doi.org/10.5817/MUJLT2024-1-4>
- Chellappa, R. K., & Sin, R. G. (2005). Personalization versus privacy: An empirical examination of the online consumer's dilemma. *Information Technology & Management*, 6(2-3), 181-202. <https://doi.org/10.1007/s10799-005-5879-y>
- Cho, H. (2012). Responses to online privacy risks. In Y. Zheng (Ed.), *Encyclopedia of cyber behavior* (pp. 900-910). IGI Global. <https://doi.org/10.4018/978-1-4666-0315-8.ch074>
- Cho, H., Lee, J., & Chung, S. (2010). Optimistic bias about online privacy risks: Testing the moderating effects of perceived controllability and prior experience. *Computers in Human Behavior*, 26(5), 987-995. <https://doi.org/10.1016/j.chb.2010.02.012>
- Cho, K., Park, Y., Kim, J., Kim, B., & Jeong, D. (2025). Conversational AI forensics: A case study on ChatGPT, Gemini, Copilot, and Claude. *Forensic Science International: Digital Investigation*, 52, 301855. <https://doi.org/10.1016/j.fsidi.2024.301855>
- Choi, Y., Zhunis, A., Dong, W., Seering, J., Park, S., Cha, M., & Chin, H. (2025). Privacy disclosure to large language models: A large-scale study on awareness, benefits, and concerns in health contexts across three countries. *Computers in Human Behavior Reports*, 20, 100841. <https://doi.org/10.1016/j.chbr.2025.100841>
- Conger, S., Pratt, J. H., & Loch, K. D. (2013). Personal information privacy and emerging technologies. *Information Systems Journal*, 23(5), 401-417. <https://doi.org/10.1111/j.1365-2575.2012.00402.x>
- Davis, F. D. (1986). *A technology acceptance model for empirically testing new end-user information systems: Theory and results* [Doctoral dissertation, MIT Sloan School of Management]. <http://hdl.handle.net/1721.1/15192>
- Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13(3), 319-339. <https://doi.org/10.2307/249008>
- Debatin, B., Lovejoy, J. P., Horn, A. K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication*, 15(1), 83-108. <https://doi.org/10.1111/j.1083-6101.2009.01494.x>
- Dienlin, T., & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology*, 45(3), 285-297. <https://doi.org/10.1002/ejsp.2049>
- Dinev, T., & Hart, P. (2005). Internet privacy concerns and social awareness as determinants of intention to transact. *International Journal of Electronic Commerce*, 10(2), 7-29. <https://doi.org/10.2753/JEC1086-4415100201>
- Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, 17(1), 61-80. <https://doi.org/10.1287/isre.1060.0080>
- Epstein, Z., Hertzmann, A., Herman, L., Mahari, R., Frank, M. R., Groh, M., Schroeder, H., Smith, A., Akten, M., Fjeld, J., Farid, H., Leach, N., Pentland, A., & Russakovsky, O. (2023). *Art and the science of generative AI: A deeper dive*. PsyArXiv. <https://doi.org/10.48550/arXiv.2306.04141>

- Gan, W., Ye, Z., Wan, S., & Yu, P. S. (2023). Web 3.0: The future of Internet. *Companion Proceedings of the ACM Web Conference* (pp. 1266-1275). Association for Computing Machinery. <https://doi.org/10.1145/3543873.3587583>
- Guo, X. T., Zhang, X. F., & Sun, Y. Q. (2016). The privacy-personalization in mHealth services acceptance of different age groups. *Electronic Commerce Research and Applications*, 16, 55-65. <https://doi.org/10.1016/j.elcrap.2015.11.001>
- Karwatzki, S., Dytyanko, O., Trenz, M., & Veit, D. (2017). Beyond the personalization–privacy paradox: Privacy valuation, transparency features, and service personalization. *Journal of Management Information Systems*, 34(2), 369-400. <https://doi.org/10.1080/07421222.2017.1334467>
- Lee, H., Park, H., & Kim, J. (2013). Why do people share their context information on Social Network Services? A qualitative study and an experimental study on users' behavior of balancing perceived benefit and risk. *International Journal of Human-Computer Studies*, 71(9), 862-877. <https://doi.org/10.1016/j.ijhcs.2013.01.005>
- Meng, X., & Liu, J. (2025). "Talk to me, I'm secure": Investigating information disclosure to AI chatbots in the context of privacy calculus. *Online Information Review*, 49(5), 944-954. <https://doi.org/10.1108/OIR-06-2024-0375>
- Nguyen, K. V. (2025). The use of generative AI tools in higher education: Ethical and pedagogical principles. *Journal of Academic Ethics*, 23, 1435-1455. <https://doi.org/10.1007/s10805-025-09607-1>
- Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, 41(1), 100-126. <https://doi.org/10.1111/j.1745-6606.2006.00070.x>
- Olatunde, S., & Mohamed, A. (2025). Exploring the privacy paradox in AI adoption: A data-driven analysis of user engagement. *Proceedings of the 6th International Conference on Artificial Intelligence, Robotics and Control, Savannah, GA, USA*, 424-429. <https://doi.org/10.1109/AIRC64931.2025.11077547>
- Pavlou, P. A. (2003). Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. *International Journal of Electronic Commerce*, 7(3), 101-134. <https://doi.org/10.1080/10864415.2003.11044275>
- Perkins, M., & Roe, J. (2025). Generative AI tools in academic research: Applications and implications for qualitative and quantitative research methodologies. In S. Popenici, J. Rudolph, F. Ismail, & S. Tan (Eds.), *Handbook of artificial intelligence in higher education*. Elgar Online. <https://doi.org/10.4337/9781035338764.00012>
- Punj, G. (2017). Consumer intentions to falsify personal information online: Unethical or justifiable? *Journal of Marketing Management*, 33(15-16), 1402-1412. <https://doi.org/10.1080/0267257X.2017.1348011>
- Rainie, L., Kiesler, S., Kang, R., & Madden, M. (2013). *Anonymity, privacy, and security online*. Pew Research Center's Internet & American Life Project. https://www.pewinternet.org/wp-content/uploads/sites/9/media/Files/Reports/2013/PIP_AnonymityOnline_090513.pdf
- Saadé, R., & Bahli, B. (2005). The impact of cognitive absorption on perceived usefulness and perceived ease of use in online learning: An extension of the technology acceptance model. *Information & Management*, 42(2), 317-327. <https://doi.org/10.1016/j.im.2003.12.013>
- Sheehan, K. B. (2002). Toward a typology of Internet users and online privacy concerns. *Information Society*, 18(1), 21-32. <https://doi.org/10.1080/01972240252818207>
- Sheng, H., Nah, F. F.-H., & Siau, K. (2008). An experimental study in ubiquitous commerce adoption: Impact of personalization and privacy concerns. *Journal of the Associations for Information Systems*, 9(6), Article 15. <https://doi.org/10.17705/1jais.00161>
- Silva, P. (2015). Davis' Technology Acceptance Model (TAM) (1989). In M. N. Al-Suqri & A. S. Al-Aufi (Eds.), *Information seeking behavior and technology adoption: Theories and trends* (pp. 205-219). IGI Global Scientific Publishing. <https://doi.org/10.4018/978-1-4666-8156-9.ch013>
- Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, 35(4), 989-1015. <https://doi.org/10.2307/41409970>

- Taddicken, M. (2014). The 'privacy paradox' in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. *Journal of Computer-Mediated Communication*, 19(2), 248-273. <https://doi.org/10.1111/jcc4.12052>
- Thelwall, M., & Vis, F. (2017). Gender and image sharing on Facebook, Twitter, Instagram, Snapchat and WhatsApp in the UK: Hobbying alone or filtering for friends? *Aslib Journal of Information Management*, 69(6), 702-720. <https://doi.org/10.1108/AJIM-04-2017-0098>
- Tomlinson, K., Jaffe, S., Wang, W., Counts, S., & Suri, S. (2025). *Working with AI: Measuring the occupational implications of generative AI*. PsyArXiv. <https://doi.org/10.48550/arXiv.2507.07935>
- Trepte, S., Teutsch, D., Masur, P. K., Eicher, C., Fischer, M., Hennhöfer, A., & Lind, F. (2015). Do people know about privacy and data protection strategies? Towards the "Online Privacy Literacy Scale" (OPLIS). In S. Gutwirth, R. Leenes & P. de Hert (Eds.), *Reforming European data protection law* (pp. 333-365). Springer. https://doi.org/10.1007/978-94-017-9385-8_14
- Upreti, D., Zhu, D., & West, H. J. (2023). ChatGPT – A promising generative AI tool and its implications for cancer care. *Cancer*, 129(15), 2284-2289. <https://doi.org/10.1002/cnccr.34827>
- Van den Broeck, E., Poels, K., & Walrave, M. (2015). Older and wiser? Facebook use, privacy concern, and privacy protection in the life stages of emerging, young, and middle adulthood. *Social Media + Society*, 1(2). <https://doi.org/10.1177/2056305115616149>
- Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, 27(3), 425-478. <https://doi.org/10.2307/30036540>
- Victor-Nyebuchi, M. (2025). *The impact of AI-driven personalization tools on privacy concerns and trust in social media marketing*. PsyArXiv. <https://doi.org/10.2139/ssrn.5385173>
- Wang, N., Li, Y., & Cong, F. (2025). University students' privacy concerns towards generative artificial intelligence. *Journal of Academic Ethics*, 23, 2401-2422. <https://doi.org/10.1007/s10805-025-09658-4>
- Weinberger, M., Bouhnik, D., & Zhitomirsky-Geffet, M. (2017). Factors affecting students' privacy paradox and privacy protection behavior. *Open Information Science*, 1(1), 3-20. <https://doi.org/10.1515/opis-2017-0002>
- Weinberger, M., & Bouhnik, M. (2018). Place determinants for the personalization-privacy tradeoff among students. *Issues in Informing Science and Information Technology*, 15, 79-95. <https://doi.org/10.28945/4019>
- Weinstein, N. D. (1989). Optimistic biases about personal risks. *Science*, 246(4935), 1232-1233. <https://doi.org/10.1126/science.2686031>
- Zeng, F., Ye, Q., Li, J., & Yang, Z. (2021). Does self-disclosure matter? A dynamic two-stage perspective for the personalization-privacy paradox. *Journal of Business Research*, 124, 667-675. <https://doi.org/10.1016/j.jbusres.2020.02.006>
- Zhou, T., & Wu, X. (2025). Examining generative AI user disclosure intention: A perceived affordance perspective. *Journal of Theoretical and Applied Electronic Commerce Research*, 20(2), 99. <https://doi.org/10.3390/jtaer20020099>

APPENDIX - USAGE HABITS IN GAI TOOLS QUESTIONNAIRE

Part A – Demographic Details

1. Sex: M/F
2. Year of birth
3. Country of birth
4. Department
 - a. Electrical Engineering
 - b. Industrial Engineering
 - c. Electro-Optics Engineering
 - d. Software Engineering

- e. Computer Science
 - f. Business Management
 - g. Accounting and Information Systems
 - h. Pharmaceuticals (Nursing)
 - i. Bioinformatics
 - j. Information Science
 - k. Management
 - l. Mathematics Teaching
5. How would you describe your level of Internet/computer proficiency?
- a. Not proficient at all
 - b. Low proficiency
 - c. Average proficiency
 - d. High proficiency
 - e. Very high proficiency

Part B – General Privacy Concern

6. How concerned are you about the protection of your personal information on the web?
- a. Not concerned at all
 - b. Slightly concerned
 - c. Moderately concerned
 - d. Highly concerned
 - e. Very highly concerned

Part C – GAI Usage

7. Are you using generative AI (GAI) tools, such as Claude, Gemini, ChatGPT, etc.?
- a. Yes
 - b. No

Part D – GAI Usage Habits

8. In case you replied “**Yes**,” how frequently do you use generative AI (GAI) tools, such as Claude, Gemini, ChatGPT, etc.?
- a. Rarely
 - b. Occasionally
 - c. Sometimes
 - d. Frequently
 - e. Usually
9. Do you have a paid account on one of the GAI tools that you use?
- a. Yes
 - b. No

Part E – GAI Privacy Concern

10. Have you ever revealed personal details to the GAI chatbot?
- a. Yes
 - b. No
11. To what extent do you trust the operators of the GAI tools you are using?
- a. Very low level
 - b. Low level
 - c. Medium level
 - d. High level
 - e. Very high level

12. How concerned are you about the protection of your personal information while using GAI tools?
 - a. Not concerned at all
 - b. Slightly concerned
 - c. Moderately concerned
 - d. Highly concerned
 - e. Very highly concerned
13. How concerned are you that the information you reveal to the chatbot will be disseminated to external parties?
 - a. Not concerned at all
 - b. Slightly concerned
 - c. Moderately concerned
 - d. Highly concerned
 - e. Very highly concerned
14. How concerned are you that the information you reveal to the chatbot will be used to profile your online user account?
 - a. Not concerned at all
 - b. Slightly concerned
 - c. Moderately concerned
 - d. Highly concerned
 - e. Very highly concerned

AUTHORS



Dr. Maor Weinberger has a PhD in Information Science from Bar-Ilan University (BIU), Israel. His professional interests include online privacy and anonymity, and information security.



Prof. Dan Bouhnik is the rector of the Jerusalem College of Technology (JCT) and a former lecturer in the Information Science department at Bar-Ilan University (BIU) in Israel. He taught Computer Science and Logic in High Schools both in Israel and the United States. In addition, he is the author of a number of books used for teaching Advanced Computer Sciences in High Schools and his professional interests include virtual learning and its effect on the thinking process.