From Concern to Trust: How Privacy Shapes Public Adoption of Western Versus Non-Western Online GenAI Services

Amir Schreiber * and Ilan Schreiber

Department of Computer Science, The Ashkelon Academic College (AAC), Ashkelon, Israel
Email: amirsh@edu.aac.ac.il (A.S.); ilans@edu.aac.ac.il (I.S.)
*Corresponding author

***Abstract*—This study investigates how privacy concerns influence public trust and adoption of online Generative AI (GenAI) services, specifically comparing western (e.g., ChatGPT) and non-western (e.g., DeepSeek) services. A national cross-sectional survey was conducted across diverse demographics, exploring privacy risks related to both online purchasing and Online GenAI Services usage. This research fills a knowledge gap by specifically examining public perception of privacy protection across western versus non-western Online GenAI Services. To accomplish that we introduce a new index named Adoption-to-Concern Ratio (ACR). Findings indicate that public privacy concern for western Online GenAI Services is moderate, yielding relatively high adoption willingness. Concern intensifies significantly for non-western services, including foreign government exploitation and unintended data use. This translates to significantly reduced willingness to adopt non-western services. While price reduction modestly promotes adoption, superior quality/accuracy is a more effective driver for non-western Online GenAI Services. Non-western developers must build trust through transparency and demonstrate superior quality, not just lower cost. Western providers need more active measures beyond legal compliance to maintain trust. Growing concerns with AI privacy affect public trust and adoption and they manifest in geopolitical tensions around data sovereignty and ethical dilemmas about IP.**

***Keywords*—online services, privacy, Generative Artificial Intelligence (GenAI), AI risks**

I. Introduction

In the age of technological world, there has been rising concern for privacy and data security issues among individuals, organizations, and governments. Although the digital services revolution unlocks vast potential, it also creates a complex interrelationship between technology and data protection regulations. In this perspective, the Internet is a considerable revolutionary opportunity in terms of consumption and behavior change, in particular online shopping, while the current generation provides access to services to not only find information but now also generate it.

The field of Generative Artificial Intelligence (GenAI) has achieved significant progress through its developments in chatbot technology. Despite its significant promise for customer service, education, and mental health industries, security and privacy concerns, together with ethical issues, have been brought up. ChatGPT and models such as DeepSeek from developing nations demonstrate serious challenges related to sensitive information leaks.

National regulations such as the General Data Protection Regulation (GDPR), serve as a governmental response to these problems, yet public trust remains essential for the successful adoption of new technologies. Alongside research comparing western and non-western Artificial Intelligence (AI) and mapping security risks, there is a need to thoroughly examine users' perceptions regarding privacy protection. As usage increases, concerns about data leakage and the entry of sensitive information into models grow, and precisely understanding consumers' attitudes may help in developing safer tools and technologies.

Paper Outline: This paper examines existing literature on online privacy, internet and e-commerce services, the rise and public accessibility of GenAI, and associated privacy risks, including differences between western and non-western online GenAI services. Building on identified gaps in public perception, the study then outlines its methodological approach based on the Fairness, Accountability, and Transparency (FAT) framework and the Adoption-to-Concern Ratio (ACR), followed by the presentation and analysis of results both statistically and visually addressing the research questions.

Core Contribution: This study has three main contributions. First, this is among the first privacy and trust literature that systematically compares public privacy perceptions and adoption behavior between western and non-western online GenAI services, addressing a growing gap in the geo-politicized AI ecosystem. Second, it introduces the ACR as a novel, interpretable, individual-level metric for quantifying the privacy–adoption trade-off—a methodological value beyond traditional difference or regression-based

Manuscript received January 8 2026; accepted February 26 2026; published April 16, 2026.

approaches. Third, it situates the findings within the FAT framework to inform actionable implications for policymakers and service providers regarding privacy governance, transparency, and perceived accountability in shaping public trust and the adoption of AI-enabled services.

II. Literature Review

A. Aspects of Online Privacy Protection

The digital transformation creates complex ties between technological advancements and the changing data privacy laws landscape, e.g. GDPR, HIPAA (Health Insurance Portability & Accountability Act), EU AI ACT (Kalodanis *et al.,* 2024). The Internet of Things (IOT) and AI create novel security threats and privacy concerns, as they rely on extensive data processing across interconnected networks (Farayola *et al.,* 2024).

Leading industry companies are driving innovation, while providing online services that lead to better efficiency as the digital economy grows. However, the swift advancements in technology raise major concerns about consumer data protection, requiring careful management between innovation and regulatory compliance (Oyewole *et al.,* 2024).

On media sites, disclosing personal information can bring with it benefits such as personalized experiences and targeted advertisements, but can also raise concerns such as privacy violations of surfers. This and other poor data management has motivated governments to establish privacy laws. Users evaluate the potential risks to their privacy against the benefits they might gain. The key objective remains finding equilibrium between personal privacy risks and personalized marketing benefits. Privacy Management has become a sophisticated web which mirrors the multi-dimensional modern digital age (Malik, 2024; Elciyar, 2025).

B. The Internet and Online Shopping

Online shopping perfectly illustrates the current state of this tug of war between convenience and privacy concerns. As our modern lives become more hectic, online shopping is the easiest way for most to make a purchase. Online shopping saves time for the on-the-go consumer who has neither the time nor the inclination for extended shopping sprees.

Due to the extensive impact of the internet on people's behavior, many users of the internet rely on the use of online shops to buy clothes and other accessories. They also use the Internet to gather information on online shopping from various sites, especially from social media. Moreover, most of them are not confident with the security measures of online payment systems, and their level of satisfaction with online shopping is average (Honnakatti, 2025).

Online retailers, trying to lure customers away from brick-and-mortar shops, will need to provide excellent customer service and a simple, user-friendly interface for their customers. It has also been found that the level of consumers' satisfaction plays a significant role in determining whether they choose to make purchases online (Kumari, 2024). With the rapid development of information technology, online shopping is on the rise—a trend that has led to growing and ongoing concerns about privacy in e-commerce marketing (Yao & Tarofder, 2024).

C. The Rise of GenAI

AI is a rapidly growing point of interest for many industries, including the generation of creative and realistic artifacts. A subcategory of this is GenAI, which has seen tremendous growth in late 2022. Tools like ChatGPT, DALL-E, and Midjourney give users access to Large Language Models (LLMs) on-demand and create content that looks like human-written content (Peñalvo, 2023).

GenAI is a branch of AI and a subfield of deep learning that imitates the human brain. It allows intelligent systems to create new content such as text, images, and audio. Utilizing advanced algorithms and deep learning methods, GenAI models can absorb data and produce realistic and creative results resembling human creativity (Mallikarjuna, 2024).

The availability, simplicity of use, and convenience of chatbots has made its use ubiquitous and it is actively being applied in various fields. OpenAI research laboratory released ChatGPT, which represents one of the latest advancements in artificial intelligence in 2022. ChatGPT lets it study specific parts of the text and produce a more human-like and natural output. At last, the pre-training method allows it to generate more relevant and accurate text for a specific task (Albadarin, 2024).

D. Accessibility of Online GenAI Services to the General Public

Recently, systems based on GenAI have gained momentum and are increasingly being used by the general public. Traditionally, people have used Google and other search platforms to research products before making a purchase. However, the integration of ChatGPT into the Bing search engine and Google's announcement of the development of its BARD model may significantly influence how customers search for and discover products (Gude, 2023).

Besides, with the arrival of online GenAI services such as ChatGPT, the technology of using natural language processing to communicate has invaded the business world. ChatGPT, has been adopted in various sectors, including customer service, healthcare, education, automotive industry, and finance (Singh & Singh, 2023). Individuals of any age and origin can utilize ChatGPT for natural, multilingual communication, without having any knowledge of programming (Gouvi *et al.,* 2023).

As it can process the context, intent, emotions, and other components of human speech, a system like ChatGPT allows users to communicate efficiently (Rahman and Husain, 2022). Many domains can significantly benefit from this technology (George & George, 2023; Molla *et al.,* 2023). However, most studies emphasize the importance of having proper guidance,

support, and clear instructions to prevent some pitfalls in output (Albadarin *et al.,* 2024).

E. Public Privacy Protection Risks Specific to Online GenAI Services

There is a need to investigate the privacy and security of the tool that we work with. In OpenAI's privacy policy, the company warns users that personal information, such as the user's account details, user content, social media data, log data, and usage data, are automatically collected once a user creates an account and logs in. Moreover, device information, cookies, and web analytics, are also collected automatically, and personal information can be shared with third parties, such as cloud service providers, web analytics vendors, government authorities, and partners (Wu *et al.,* 2024).

GDPR mandates that a user's information cannot be obtained or processed without a person's prior knowledge and permission (Wolford, 2025). Although OpenAI claims to adhere to the GDPR in its privacy policy, these measures do not alleviate the concerns of the public—Despite its flagship feature allows users to turn off the chat history the company can still access the log for 30 days (Shanklin, 2023).

It is evident that ChatGPT does not adequately address the protection of personal data, as required by the GDPR. For instance, the ChatGPT system may share user data with third-party vendors without the user's consent. The major privacy issue is the risk of privacy breaches via the exploitation of personal input by the model. Privacy issues over OpenAI's data handling led to ChatGPT's temporary ban in Italy and ongoing investigations elsewhere and in several other countries (Lomas, 2023; Mauran, 2023).

Even though OpenAI implements technical measures to secure data centers and physical machines, there are frequent cases of cybersecurity events, leading to a high risk of private information leaking out (Smish, 2024; Kovvuru, 2025).

F. Global Power Struggles for AI Technological Leadership

AI stands out as one of the most important technological innovations in today's age. Amongst many countries trying to become leaders in this technological field, China is now recognized as one of the two strongest AI developers in the world (Zhang & Khanal, 2024). It is rapidly building the environment that would help the AI systems to be easily incorporated into the people's everyday lives (Cheng & Zeng, 2023).

These days, when living in the United States, one of the most interesting and most often mentioned in media things is the fact that China won the AI race against the US. America is considered a rival, and it serves as a reference point for China to measure its own progress and competitiveness. The U.S. success in AI is one of the main concerns of the strategic community of China, which is making the Chinese leaders reflect, and fueling China's AI ambitions (Zeng, 2025).

G. Online GenAI Services Originating from Developing Countries

In January 2025, DeepSeek-R1, a new AI model, was introduced and rapidly adopted, dominating the user market and becoming the number one AI application in downloads (Conroy & Mallapaty, 2025; Gibney, 2025). DeepSeek is known for being open-source under the MIT license, offering optimal cost-effectiveness and impressive reasoning capabilities. Furthermore, it outperforms GPT-4o and OpenAI o1 across various benchmarks and excels in tasks such as mathematics and coding (Hugging Face, 2025; Gibney, 2025). While ChatGPT is better suited for engagement and adaptability, DeepSeek excels in task accuracy when it comes to executing complex operations.

Since the launch of DeepSeek's LLMs and its free applications, the industry, investors, and the media have reacted with alarm—surprised that a Chinese startup, operating with a limited budget and restricted access to dedicated AI hardware, managed to outperform the latest ChatGPT models. This situation has sparked geopolitical concerns about threats to U.S. technological dominance, and the effectiveness of U.S.-imposed sanctions on China regarding AI chip technologies. Investor confidence in leading U.S. tech companies focused on AI, AI hardware, and AI/cloud hosting has been shaken, contributing to a significant market decline in January 2025 (Maes, 2025).

H. Advantages and Disadvantages of Chinese Online GenAI Services

DeepSeek was designed with consideration of the deployment into resource-constrained systems such as edge computing devices or resource-limited systems. These models maintain scalability and low costs, enabling further expansion of DeepSeek to make advanced AI even more accessible across a wide range of applications (Poo, 2025). This allows the company to offer its online services to the public at significantly lower prices—even free of charge for certain models—where competitors typically charge for similar services.

Several commentators have expressed concerns about DeepSeek's Chinese origin, citing issues such as privacy, user data storage, intellectual property protection, potential unethical practices, censorship, governmental influence, and related risks (Yang, 2025; Smith, 2025; Lyons, 2025; AP, 2025; Italiano & Musumeci, 2025). Many have already questioned how the company's LLM was built, suggesting the possibility that it may have relied on OpenAI or other models as a foundation for fine-tuning—potentially violating the terms of service of those models (Thompson, 2025; Reuters, 2025). It also appears that large volumes of data are being transmitted to servers in China under questionable conditions, raising concerns around security, privacy, and regulatory compliance (Smith, 2025).

I. Gaps in Public Perception and Research Questions

Over the years, an extensive body of literature has evolved, discussing the technological requirements of AI systems in terms of FAT or FAT plus Ethics (FAT-E)

(e.g.: Zhdanov *et al.,* 2022; Memarian & Doleck, 2023; New America, 2025). Concrete requirements have even been formulated for systems designed to protect privacy, known as PETs (Privacy-Enhancing Technologies) (OECD 2023). Subsequently, researchers have also examined the level of general trust users placed in ChatGPT service (e.g.: Choudhury & Shamszare, 2023).

However, current studies do not aim to observe how privacy concerns influence public trust and adoption of online GenAI services. Nor does it examine the uniqueness of this phenomenon in comparison to standard online shopping services. In addition, it is not yet possible to assess the variation in privacy perceptions within the geopolitical context—between western and non-western service providers—where unique factors such as foreign government interests, price and product quality may influence risk perception and willingness to use the service.

While the promotion and technological adoption of innovative services are partially governed by privacy protection laws, they also largely depend on the public's perception of these services—particularly in terms of the confidentiality of their personal information and the safeguarding of data input into models, which may potentially leak into foreign or even malicious hands.

This study will address these questions, which call for an expansion of the current academic literature and have been largely absent from previous research:

- (RQ1) To what extent does the public express concern over privacy when using online GenAI services?
- (RQ2) Does this concern intensify when it comes to online GenAI services from non-western countries, such as the recently introduced DeepSeek?
- (RQ3) Does this concern translate into a reduced willingness to use these services?
- (RQ4) Are there factors—such as lower cost or superior output quality/accuracy—that could promote adoption of online GenAI services from developing countries despite privacy concerns?
- (RQ5) How does this concern compare to privacy concerns during standard online product purchases?

III. Materials and Methods

A. Approach and Workflow

To investigate public perception regarding online GenAI services, specifically in terms of privacy protection, we designed a structured survey comprising four key sections (See Fig. 1, and the following bullet points).

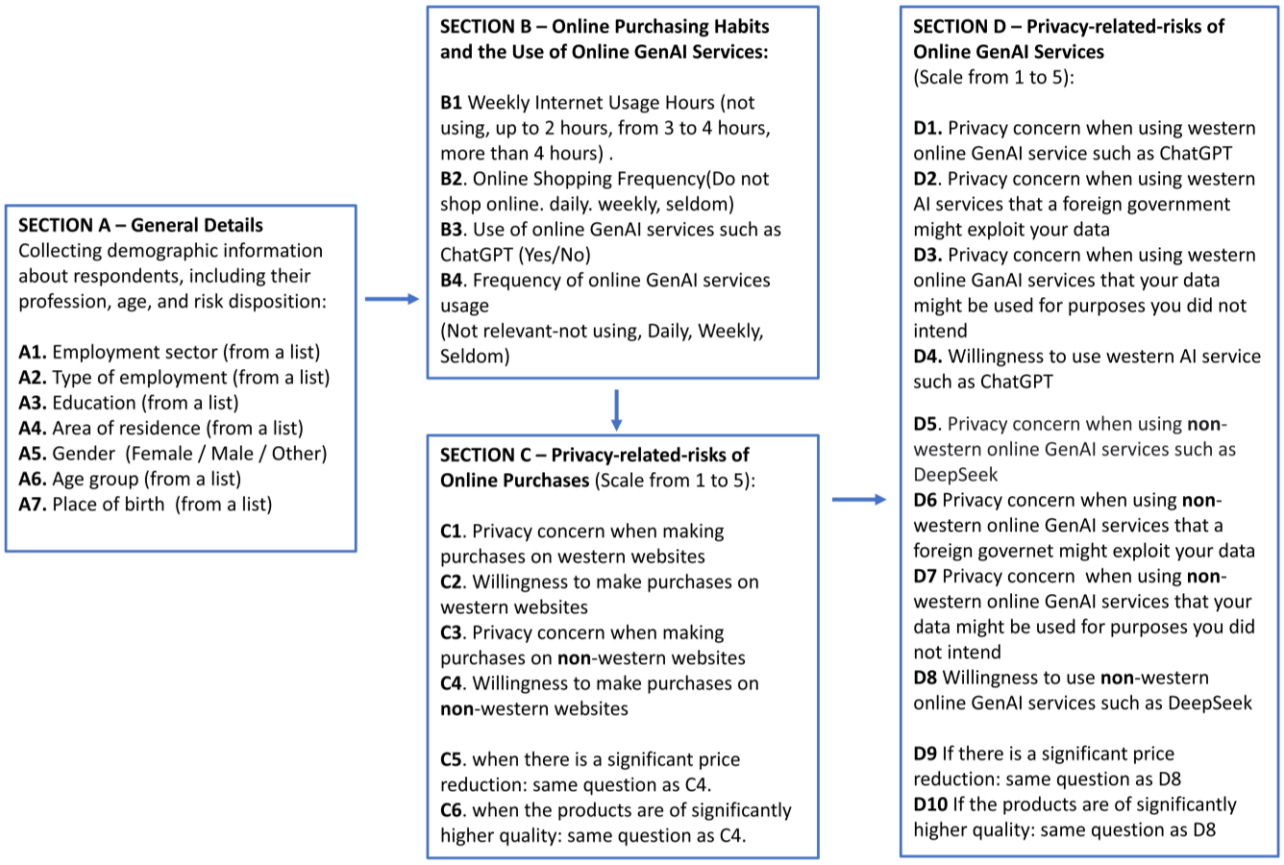

Fig. 1. Workflow process.

The first two sections provide us with general details and consumption habits. The following two sections are aligned with the vast literature on FAT (discussed in Section II.I) with a spot on privacy concern and willingness to use.

- General Details (A): Collecting demographic information about respondents, including their profession, age group, gender and living area.
- Online purchasing habits and the use of online GenAI services (B): Exploring the extent to which respondents engage with both online consumption and GenAI chatbots in their daily lives.
- Privacy-related risks of online purchasing (C): as a reference point for comparison
- Privacy-related risks of online GenAI services (D): as the main domain to be investigated.

B. Detailed Design

At the outset of the survey, participants were provided with an informed notice stating that participation was anonymous and that the data collected would be used exclusively for academic and research purposes.

- Section A: Survey General Details

Collecting demographic and general information about respondents, including (see Table I):

TABLE I. SECTION A DETAILED QUESTIONS

No	Questions
A1	Employment sector: Choosing from a list based on the main employment domains set by the Federal Bureau of Statistics: information and communication, hi-tech and technology, real estate and construction, industry and factory, academic and scientific activity, education, entertainment arts, public administration, health services, financial services and insurance, wholesale trade and retail chains, security, other services.
A2	A2: Type of employment: self-employed, employee, student, pensioner, between jobs
A3	Education: sciences/engineering academic degree or student, social sciences & humanities academic degree or student, law academic degree or student, up to 12 years of education, other (free input).
A4	Area of Living: Primary city, Capital city, Port city, Northern rural area, Central rural area, Southern rural area.
A5	Gender: Female, Male or Other.
A6	Age group: 15–24, 25–34, 35–44, 45–54, 55–64, 65+.
A7	Place of birth: Middle East, West Europe, East Europe, America, Africa, Asia, Australia/New Zealand

- Section B: Online Purchasing Habits and the use of online GenAI services

Exploring respondents' online purchasing habits and the extent to which they encounter GenAI technologies in their daily use (see Table II):

TABLE II. SECTION B DETAILED QUESTIONS

No	Questions	Choices
B1	How many hours per week do you spend browsing the internet?	Not at all, up to 2 hours, approximately 3 to 4 hours, more than 4 hours.
B2	How often do you make purchases online?	I do not shop online, Daily, Weekly, Seldom.
B3	Have you ever used any Artificial Intelligence services such as ChatGPT?	Yes, No.
B4	What is your usage frequency (please choose the option that best reflects your actual use)?	Not relevant-not using, Daily, Weekly, Seldom.

- Section C: Privacy-related risks of online purchasing (see Table V for FAT reference)

Exploring respondents' perception regarding privacy-related risks of online purchasing Scale from 1 (slightly) to 5 (very much) (see Table III):

TABLE III. SECTION C DETAILED QUESTION

No	Questions
C1	How concerned are you about your privacy when making online purchases on western websites?
C2	Given this, how likely are you to make a purchase on a western website such as Amazon or eBay?
C3	How concerned are you about your privacy when making online purchases on non-western websites such as Shein or Temu?
C4	Given this, how likely are you to make a purchase on a non-western website such as Shein or Temu?
C5	However, when there is a significant price reduction (compared to western websites), to what extent would you be willing to make purchases on a non-western website such as Shein or Temu?
C6	Additionally, when it comes to significantly higher-quality products (compared to western websites), to what extent would you be willing to make purchases on a non-western website such as Shein or Temu?

- Section D: Privacy-related risks of online GenAI services (see Table VI for FAT reference)

Privacy-related risks of online GenAI services

Exploring respondents' perception regarding privacy-related risks of online GenAI services Scale from 1 (slightly) to 5 (very much) (see Table IV):

TABLE IV. SECTION D DETAILED QUESTION

No	Questions
D1	How concerned are you about your privacy when using western online GenAI services such as ChatGPT?
D2	How concerned are you that, when using a western website such as ChatGPT, a foreign government might exploit access to the data you entered in the conversation for malicious purposes you did not intend?
D3	How concerned are you that, when using a western website such as ChatGPT, business data (IP) entered in the conversation might be used for unintended purposes, such as model training and inference improvement, or might leak into conversations with other users?
D4	Given this, to what extent would you be willing to use a western AI service such as ChatGPT?
D5	How concerned are you about your privacy when using a non-western AI service such as the Chinese DeepSeek?
D6	How concerned are you that, when using a non-western website such as the Chinese DeepSeek, a foreign government might exploit access to the data you entered in the conversation for malicious purposes you did not intend?
D7	How concerned are you that, when using a non-western website such as the Chinese DeepSeek, business data (IP) entered in the conversation might be used for unintended purposes, such as model training and inference improvement, or might leak into conversations with other users?
D8	Given the possibility that the data you entered might be misused, how likely are you to use a non-western AI service such as the Chinese DeepSeek?
D9	However, when there is a significant reduction in service cost (compared to the western service), to what extent would you be willing to use a non-western AI service such as the Chinese DeepSeek?
D10	Additionally, if there is a possibility of higher-quality and more accurate results (compared to the western tool), to what extent would you be willing to use a non-western AI service such as the Chinese DeepSeek?

To examine respondents' privacy-related risk perceptions in both e-commerce and GenAI contexts, this study adopts the FAT framework as a reference point. FAT has been widely applied to structure ethical, governance, and trust dimensions of data-driven systems, particularly where personal or sensitive data are involved.

The FAT framework was used to guide the selection and formulation of survey questions, ensuring key aspects of privacy-related concerns were adequately represented. Each survey item was mapped to the FAT component it most directly reflects:

- Transparency conveys the respondents' perception of data visibility, clarity of data use and understanding of how personal or business information is processed.
- Accountability signifies perceived responsibility, enforceability and institutional safeguards including regulation, oversight and liability in the event of misuse.
- Fairness symbolizes the value-based trade-off by the respondents, that is, between economic incentives or performance benefits and the associated privacy risks.

Some items intentionally span multiple FAT dimensions, reflecting the interdependent nature of privacy risk perception in real-world decision-making.

TABLE V. FAT REFERENCE FOR ONLINE SHOPPING

Question	FAT Reference	Rationale for This Research
C1	Transparency (T)	Privacy concern during online shopping reflects user's understanding of transparency regarding how personal data are collected, processed, and shared by the platform.
C2	Accountability (A)	Willingness to purchase despite risks reflects perceived provider responsibility, user confidence in mitigation controls and the availability of recourse mechanisms in case of misuse.
C3	Transparency (T)	Heightened concern toward non-western platforms is primarily associated with uncertainty regarding data handling practices and disclosure standards.
C4	Accountability (A)	Reduced willingness to purchase reflects perceived weaknesses in legal, regulatory, and organizational accountability structures.
C5	Fairness (F) + Accountability (A)	Willingness to trade privacy for lower prices reflects perceived fairness of the value exchange and expectations regarding the platform's responsibility to mitigate risks.
C6	Fairness (F)	Preference for higher-quality products despite privacy concerns reflects a utilitarian fairness judgment balancing benefit against perceived risk.

TABLE VI. FAT REFERENCE FOR ONLINE GENAI SERVICES

Question	FAT Reference	Rationale for This Research
D1	Transparency (T)	Privacy concern when using western online GenAI services reflects users' understanding of data usage, retention, and model training practices.
D2	Accountability (A)	Concern over governmental exploitation reflects perceived responsibility of the provider to prevent unauthorized state-level access.
D3	Transparency (T)+ Accountability (A)	Risks related to IP misuse and data leakage combine opacity regarding data reuse with responsibility for preventing unintended dissemination.
D4	Accountability (A)	Willingness to use western online GenAI services is grounded in trust in the provider's governance, compliance, and enforcement mechanisms.
D5	Transparency (T)	Elevated concern regarding non-western online GenAI services reflects limited visibility into data governance and processing practices.
D6	Accountability (A)	Fear of state exploitation underscores perceived absence of enforceable accountability mechanisms across jurisdictions.
D7	Transparency (T)+ Accountability (A)	Potential misuse of business data reflects both unclear data policies and insufficient safeguards and liability structures.
D8	Accountability (A)	Willingness to use the service despite risks reflects perceived provider responsibility and user confidence in mitigation controls.
D9	Fairness (F) + Accountability (A)	Acceptance of lower-cost services reflects a fairness-based cost–risk trade-off, moderated by perceived accountability of the provider.
D10	Fairness (F)	Preference for higher accuracy despite privacy risks reflects a fairness assessment prioritizing outcome quality over potential harm.

IV. RESULTS AND ANALYSIS

A. Cultural and Geopolitical Context

The setting of this study was Israel where people generally are tech savvy, exposed to cybersecurity threats, and where awareness regarding data privacy and protection concerns is high. Furthermore, geopolitical aspects such as sensitivity to foreign intervention may affect users' attitudes towards technology not developed in the western world. On the other hand, one could argue that these sensitivities exist in western populations as well (people are wary of foreign technologies for reasons such as control over their data, trust in regulations, etc.). Therefore, in this regard, Israeli users may stand as proxies for western users of non-domestically developed online GenAI services.

B. Deployment and Statistics of Survey

Data statistics (period of activity, return rate, completion rate): The survey was open for a period of three months. The response rate was 97% of the total distribution. In fact, 2% of the recipients from the total distribution did not respond due to either too many inquiries or a general lack of interest in responding to surveys, and 1% of the forms were partially filled out and disqualified in the completeness check (filling required fields).

Deployment method & selection of participants: The survey is Cross-sectional survey research aimed at collecting information from various sectors over a period of three months, to produce a descriptive analysis of the public perception on the extent and impact of AI privacy risk in using online AI applications. The information collected is intended to spot patterns between variables, preparing for future statistical analysis. This type of research focuses on the most critical aspects of the phenomenon as it exists and, more broadly, on the context of real-world practice in which a research study is to be interpreted.

Measurement type and results visualization: Finding the central tendency and the average response is crucial in descriptive analysis. To summarize the findings, we used various charts and plots to visualize and categorize the data: scatter plots, bar charts or stacked bar charts, pie charts and a spider chart.

C. Methodological detailed information

Sampling Method/Recruitment: Our study employed nonprobability convenience sampling, striving for a broad spectrum of participants across demographic categories (age, gender, education, job type, and region). Samples were recruited online via networks of professional contacts, mailing lists and public forums on social media platforms over a recruitment period of three months. The survey was designed to be completed on a voluntary basis, with no monetary rewards.

The current study has a more modest objective aiming to identify patterns rather than draw conclusions about the general population. Despite noting that the study is "national" in scope, samples were not drawn using a probability sampling frame and thus are not statistically representative at the population level. The term "national" is employed to capture the broad geographic distribution of the participants, with respondents representing central, peripheral, and rural areas, according to their demographic details (see Fig. 2).

Response rate: The 97% response rate quoted here is only amongst participants who clicked on the survey link. It does not account for all of those exposed to the invitation to participate. As this was an opt-in study, completion rate can only be measured amongst those who accessed the survey link. In other words, we can measure how many people finished the survey successfully, but calculating a typical response rate isn't possible, as we didn't use a specific sample. Participants were excluded if their response was incomplete (around 1%) due to technical or issues errors. We used a completeness criteria to identify incomplete responses.

Sample Size Considerations: The sample size falls into the range of exploratory cross-sectional studies (Bhattacherjee, 2012) which usually aim to uncover tendencies and associations, rather than draw conclusions about a population as a whole. Furthermore, given that there are no strict rules/ceilings/floors for sample size (Ahmed, 2024) and the goal of the study was to look at differences in privacy perception and adoption behavior between conditions (western vs. non-western services), the sample size should suffice to detect medium-to-large effects, which was demonstrated by the presented Cohen's d statistics.

*Common academic scale for Cohen's d[z] by Cabridge: 0.2 = small, 0.5 = medium, 0.8 = large.

However, as the authors, we acknowledge that due to sample size, the study in a way is limited in statistical power to draw conclusions about smaller subgroups and has lower generalizability—especially when looking at demographic breakdowns. Given that this is a first (pioneering) study into this research domain, this is stated in the limitations of the study and serves as an interesting avenue for future work.

Scope of Inference: The findings should be interpreted as indicative of patterns observed within the sampled population rather than as fully generalizable to the national population. Accordingly, references to "public perception" in this study reflect aggregated respondent perceptions within the sample.

Data Handling and Data Quality Controls: There were several built-in features in the survey instrument to reduce the amount of missing data. The first was that questions, for the most part, were close-ended (i.e. Likert scale questions, questions with predefined categories) to reduce ambiguity. The second was to make all questions required. The survey design prevented users from jumping ahead without providing an answer to each prompt.

In addition, participants received one overall validation check before being allowed to submit the questionnaire which confirmed that all questions had been answered. The final dataset submitted for analysis contained only complete questionnaires. Incomplete questionnaires were discarded during the data cleaning phase (~1%); this was defined using built in variables that indicated completeness.

Prevention of Bias: Structured surveys such as these help eliminate measurement error or alternate responses (especially true with regards to the perception oriented Likert-scale questions).

Imputation: Imputation was not necessary because we built in measures to structurally prevent missingness. We do not run the risk of biased imputation here. This allows for better internal consistency/reliability because we have ensured that every participant responded to every question. Therefore, missing data was minimal and did not require imputation.

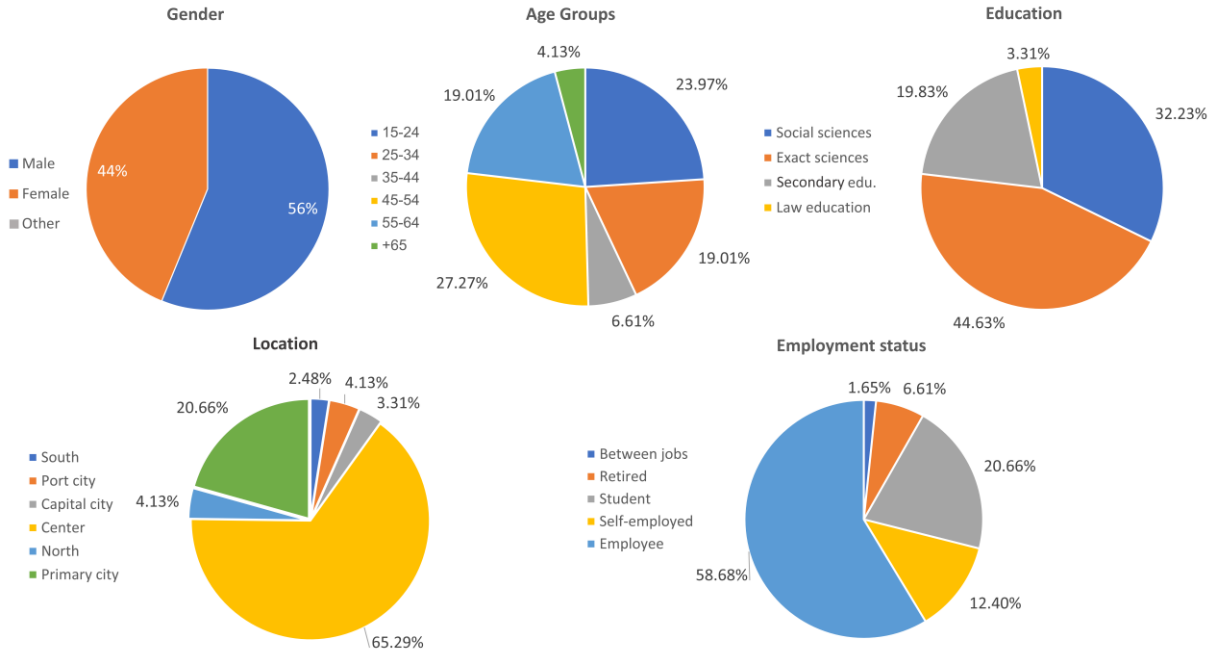

Fig. 2. Distribution over population.

D. Settings and Distribution

The survey garnered responses (N = 121) from a diverse demographic background. As depicted in Fig. 2, there's a balanced distribution between male and female participants (Males 56%; Females 44%). The age groups represented span a broad spectrum that fits both traditional workplaces as well as technology-oriented workplaces. Roughly 51% of the respondents are aged 45 and above—a demographic mixture often seen in traditional workplaces. Conversely, about 49% are below this age, typically representative of technology-oriented environments.

The educational backgrounds of the survey participants displayed a balanced distribution: around 44% held

academic degrees in Exact Sciences and another 32% in Social Sciences. The remaining 24% were a mix of individuals with degrees in various other academic fields and those with secondary education.

Geographically, the respondents represented all regions of the country, with a predominant 65% from the central and 20% from the primary city, which mirrors the population distribution in the country, where most businesses and universities are concentrated in the central area. The other 15% of respondents were from diverse regions across the country. Employment status among the participants varied: a substantial 58% were in employment, 12.4% self-employed, 6.6% retired, 1.6% students and 20.6% between jobs.

E. Main Results

The public expresses moderate privacy concern regarding western online GenAI services, such as ChatGPT. The average privacy concern when using western online GenAI services is 2.55 out of 5. When asked separately, the average concern that a foreign government could use their data when using western online GenAI services is 2.58. While both *p*-values are significant with a small* difference (*p*-value < 0.01, Cohen's $d^z = 0.03$) the concern specific to data being used for unintended purposes when using western online GenAI services is 2.90 and not statistically significant (*p*-value>0.1). This suggests that while there is an overall privacy concern and a specific concern about foreign government exploitation with western online GenAI services, the worry about data misuse for unintended purposes is not as pronounced or statistically robust. This explains why there is a relatively 4.1 strong willingness to use western online GenAI services (RQ1) (see Fig. 3—Western services colored in blue).

Privacy concern intensifies significantly when it pertains to online GenAI services from non-western countries such as DeepSeek. Privacy concern is higher on average (3.88 vs. 2.55), when using online GenAI services developed by non-western countries, and this difference in the overall privacy concern score is significant and large (*p*-values < 0.01, Cohen's $d^z = 0.83$). Concern about foreign government exploitation of data also increases significantly and largely (mean of 3.87 vs. 2.58, *p*-values < 0.01, Cohen's $d^z = 0.88$), and so does the concern about data being used for unintended purposes (3.90, *p*-value: <0.01 vs. 2.90, *p*-values > 0.1, Cohen's $d^z = 0.71$). The consistently higher average scores and their strong statistical significance and large Cohen's d^zs across all three measures of concern clearly demonstrate a pronounced intensification of privacy concerns when engaging with non-western online GenAI services (RQ2) (see Fig. 3—first three rows for non-western services are colored in orange vs. western services colored in blue).

The heightened privacy concerns directly translate into a significantly reduced willingness to use non-western GenAI services. The willingness to use western online GenAI services such as ChatGPT averages a high of 4.10. In stark contrast, the willingness to use non-western online GenAI services like DeepSeek drops to 2.10. This substantial decrease is statistically significant and large (*p*-values < 0.01, Cohen's $d^z = -1.30$). This indicates a strong inverse relationship between heightened privacy concerns for non-western AI and the public's readiness to adopt these services (RQ3) (see Fig. 3—last three rows for willingness to use non-western services colored in orange vs western services colored in blue).

Despite the significant privacy concerns, certain factors can modestly promote the adoption of non-western online GenAI services. The baseline willingness to use non-western online GenAI services is 2.10. When the scenario includes a significant price reduction, the willingness to use these services increases to 2.30. This improvement in willingness is statistically significant but with small difference (*p*-values < 0.01, Cohen's $d^z = 0.2$). Even more impactful is the prospect of significantly higher quality or accuracy. This factor boosts the willingness to use non-western online GenAI services to 2.70 from the baseline of 2.10. This increase due to higher quality is also statistically significant with medium effect (*p*-values < 0.01, Cohen's $d^z = 0.52$). Between these two, superior output quality appears to be a more effective driver of adoption than merely a price reduction (RQ4) (see Fig. 3—last two rows—for willingness to use non-western services when conditions change colored in orange).

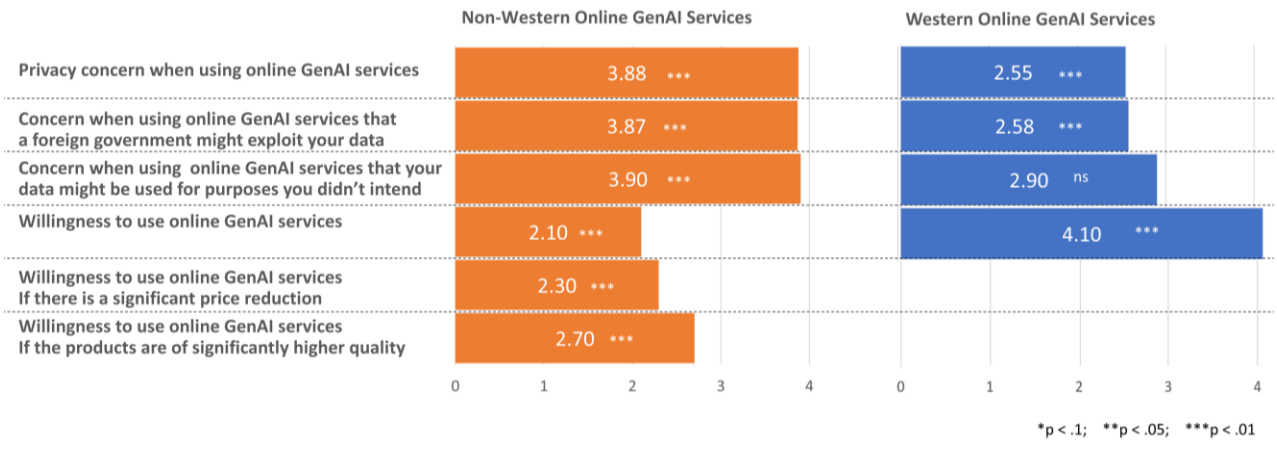

Fig. 3. Privacy concern—non-western GenAI services Vs. western GenAI services.

The level of privacy concern for western online GenAI services (average 2.55) is marginally higher than the concern for making standard online purchases on western websites (average 2.23). Both these concerns are statistically significant and large (p-values < 0.01, Cohen's d^z = 1.01). However, a more pronounced difference emerges when comparing western online GenAI services to online purchases from non-western websites. Privacy concern when using western online GenAI services (average 2.55) is significantly lower than the concern associated with making purchases on non-western websites (average 3.80). The higher concern for non-western purchases is statistically significant but with a small difference from using of western online GenAI services (p-value < 0.01, Cohen's d^z = 0.05). This comparative analysis suggests that geographical origin (western vs. non-western) may slightly increase privacy concern regardless of the specific type of online activity (see Fig. 4—Online GenAI Services usage vs. online product purchase) (RQ5).

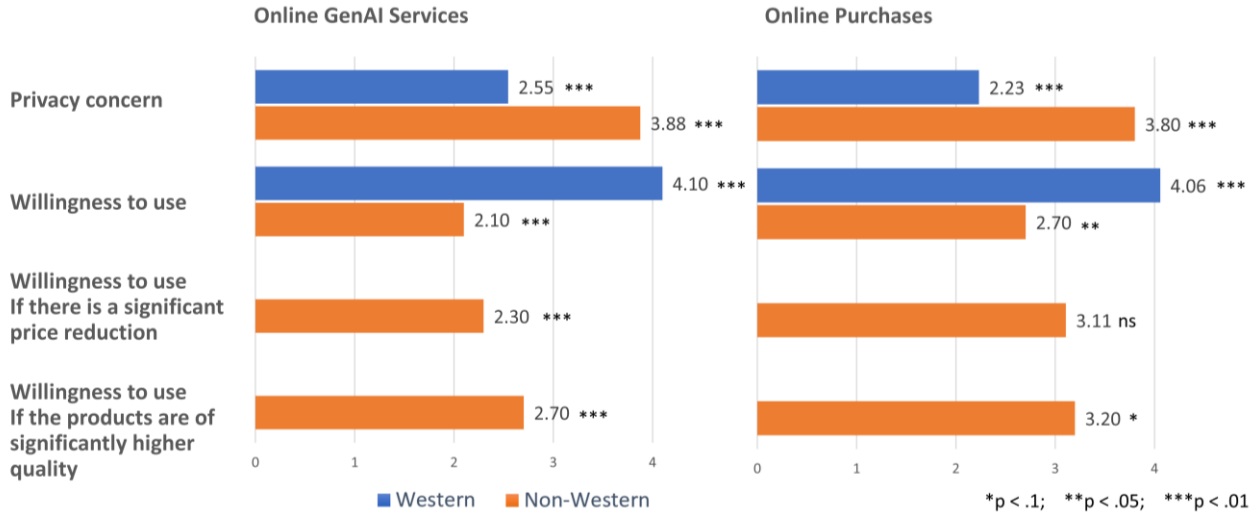

Fig. 4. Privacy concern—online GenAI services Vs online purchases.

F. Introduction of ACR Metric

To gain a deeper understanding of the phenomenon, we focused on discovering the characteristics of the adoption and privacy concern relationship to provide further differentiated answers for RQ3 via various analyses regarding Industry specific insights, Socio-Demographic insights, and Education and Experience insights.

Utilizing ACR, we introduce a meaningful quantitative framework for understanding the balance between willingness to adopt technology and privacy concerns among users. This approach aligns with recent literature emphasizing the importance of examining this tension between willingness to use and apprehension regarding AI technology adaptation (such as Cubio, 2025; Brandimarte *et al.,* 2025). Higher ACR values indicate greater openness to adoption relative to concern, enabling identification of areas with substantial market or technological potential, as well as domains that may require increased trust-building or enhanced privacy policies. This kind of ratio-based analysis is encouraged by current research trends that call for multidimensional assessments of the determinants and inhibitors of AI adoption, as well as cross-sectoral comparative studies (Khanfar *et al.,* 2024).

Compared to simple difference, the ratio-based ACR enables more meaningful comparisons across respondents as it captures the relative balance between perceived risk and behavioral willingness, emphasizing proportional differences rather than absolute score gaps; By expressing the gap relative to the observed position on the bounded scale, ACR reduces interpretive bias that arises when identical units may reflect unequal substantive change. This formulation is particularly suitable in perceptual Likert-type measures, where equal point differences do not necessarily correspond to equal substantive change. Moreover, unlike regression models designed to assess association or predictive relationships, the ACR ratio-based measure directly operationalizes a per-observation gap as a single derived metric, enabling straightforward comparison across individuals, services, and groups in different categories/attributes without imposing additional modeling assumption.

This perspective is intended to complement rather than replace the primary statistical analyses in the main results section by adding interpretive clarity to the reported results. Presenting results using a ratio-based measure provides an intuitive and interpretable representation of effect size by expressing differences in relative rather than absolute terms.

G. ACR Metric Technical Description

1) Formal definition

Let Wi and Ci represent willingness-to-use score and privacy concern score or participant, respectively, both on a bounded Likert scale, e.g. 1–5. The Adoption-to-Concern Ratio is computed as follows:

$$ACR_i = W_i / C_i$$

At the aggregate level, ACR can be computed as:

$$ACR = mean(W)/mean(C)$$

2) Interpretation and limits

Since W and C are bounded, we also have that:

$$0.2 \leq ACR \leq 5$$

ACR > 1 can be interpreted as Adoption is greater than Concern and suggests adoption is comparatively favorable. ACR < 1 conversely suggests disinclination to adoption. Near 1, scores should suggest balanced risk/reward perceptions.

3) Methodological contribution

Difference metrics (e.g., W–C) fail to capture the proportional relationship between adoption and privacy concern. For example, although the differences are equal ($5 - 3 = 4 - 2$), the ratios are not ($5/3 \neq 4/2$). Thus, differences collapse distinct situations into identical values, whereas ratios preserve the relative relationship between variables. With Likert scales, equal numerical distances don't necessarily reflect equal perceived differences. By recasting the relationship as a ratio, ACR allows for easy between-group comparisons and highlights differential sensitivity to privacy concerns across user groups, service types, etc.

4) Relation to standard metrics

We examined whether ACR provided directional agreement with some traditional, descriptive statistics (means, significant, and effect size; specifically, Cohen's d). As can be observed from the main results based on descriptive statistics and the In-depth supplemental view (next section), ACR agrees with these metrics in terms of identifying key patterns while providing easily interpretable supplement layer.

As such, ACR is not intended to replace standard practices, but to complement them by providing an intuitive, scalable means of comparison.

5) Contextualizing the ACR metric

ACR is intended to be used as one supplemental lens through which statistics can be interpreted. It is not designed to supplant current statistical practices, but to provide insights into user behavior, enhancing the scalability of those analyses.

Accordingly, ACR should be viewed as an interpretive and comparative indicator rather than a standalone inferential measure.

H. In-Depth Analysis Using ACR

1) Industry-specific finding

Fig. 5 presents the ACR for online GenAI services across different occupational sectors, comparing western online GenAI services (blue line) and non-western online GenAI services (orange line). The ACR is calculated as the average willingness to use online GenAI services divided by the average level of privacy concern when using them (on a 1–5 scale). Higher values indicate greater openness to adoption relative to concern.

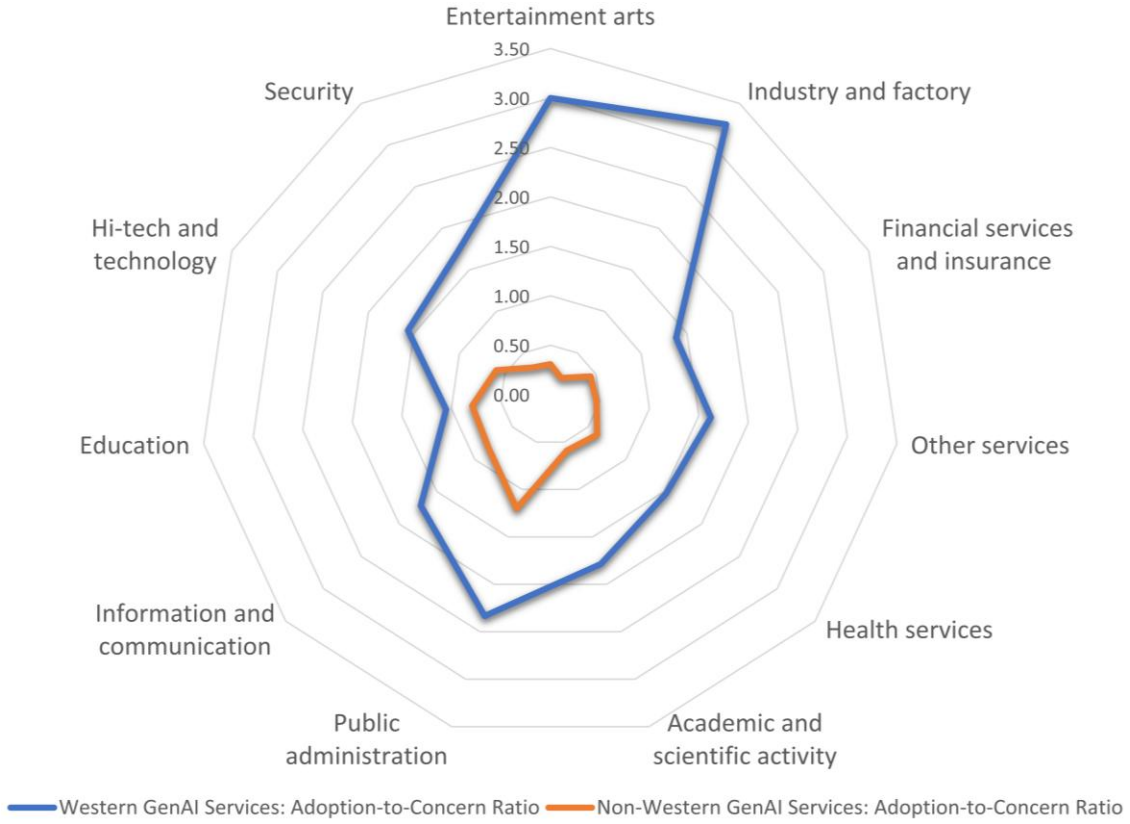

Fig. 5. ACR of online GenAI services by industry sectors.

As shown, the ACR for western online GenAI services is consistently higher across all sectors, particularly in Entertainment arts, Industry and factory, where the ratio exceeds 3.0, suggesting high adoption willingness despite privacy concerns. In contrast, non-western online GenAI services display much lower ACR values across nearly all sectors, below 1.0—indicating that privacy concerns may be a stronger deterrent in those cases. Notably, fields such as Financial Services, Insurance and Education show especially low ratios for both tool manufacturers, possibly reflecting higher institutional sensitivity to privacy risks.

2) Socio-demographic insights

Fig. 6 displays the ACR by western vs. non-western online GenAI services segmented by socio-demographic variables (age group, Gender, and Region of residence). Western online GenAI services (blue bars) have consistently higher ACR values than non-western services (orange bars) in all divisions, which overall suggests a higher willingness to adopt western online GenAI services despite the privacy concerns.

In the Age Groups the highest ACR value for western online GenAI services is among 65+ (2.11), followed by 25–34 (1.96) and 15–24 (1.74). A gradual decrease is noted for middle-aged and older respondents, with the lowest ACR for the 55–64 group (1.34). For non-western services, ACRs are consistently low across all age groups, ranging from 0.45 to 0.63, with little variation.

Regarding Gender, males report a slightly higher ACR for western online GenAI services (1.77) compared to females (1.44), suggesting greater relative openness to adoption among male respondents. For non-western online GenAI services, ACR values are almost similar for both males (0.52) and females (0.57), remaining well below 1.0 in both groups.

In the Region of Residence segment, respondents from Capital city report the highest ACR for western services (2.71), followed by Primary city (2.08) and the Southern rural area (1.86). Moderate values are observed in the Central rural area (1.51) and Port city (1.46), while the Northern rural area shows the lowest western ACR (1.00). In contrast, ACR values for non-western services are substantially lower across all regions, ranging from 0.29 (South) to 0.75 (Jerusalem).

These findings highlight the influence of age, gender, and residence location on the balance between willingness to adopt online GenAI services and privacy concerns—clearly differentiating between perceptions of western and non-western platforms.

Fig. 6. ACR of online GenAI services by socio-demographic.

3) Insights education and experience insights

Fig. 7 presents the Adoption-to-Privacy Concern Ratio (ACR) for western online GenAI services (blue bars) and non-western online GenAI services (orange bars), segmented by four variables: education field, employment status, AI usage experience, and frequency of AI tool use. In all groups, ACR values for western online GenAI services are consistently higher than those for non-western services, suggesting a stronger relative willingness to adopt western online GenAI services despite privacy concerns.

In the Education category, respondents with a background in law education report the highest ACR for western services (3.80), followed by those with secondary education (1.75), exact sciences (1.54), and social sciences (1.52). For non-western online GenAI services, ACRs remain lower and fairly uniform, ranging from 0.49 to 1.00.

Under Employment Status, the highest ACR for the western services is reported for the self-employed (2.14), followed by students (1.70), between jobs (1.60), pensioners (1.55), and employees (1.51). As before, the ACRs for non-western services remain below 0.70 across all groups.

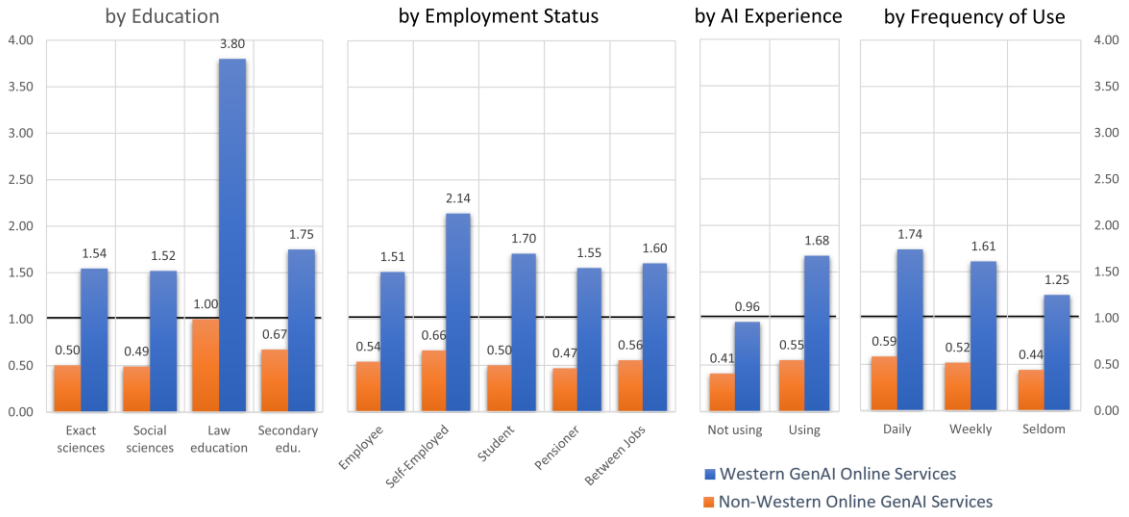

Fig. 7. ACR of online GenAI services by education, employment status, AI usage experience, and frequency of using AI services.

Under AI Usage Experience, currently using online GenAI services report a significantly higher ACR (1.68) compared to those who are not using (0.96). This may be an indication that the more experience with the services, the higher the adoption willingness.

Finally, under Frequency of Use, daily users of online GenAI services report the highest ACR for western services (1.74), followed by weekly users (1.61) and those who seldom use online GenAI services (1.25). Non-western online GenAI services exhibit lower ACR values across all usage frequencies (ranging from 0.44 to 0.59).

These findings suggest that education level, employment status, and especially actual exposure to online GenAI services play an important role in shaping the balance between adoption willingness and privacy concern—particularly in favor of western-developed platforms.

V. Discussion and Conclusion

The results of the study have several implications that are relevant for both developers and users of GenAI tools and services. The key insight in this regard is that there is a stark contrast in public concern over privacy between western-origin GenAI and its non-western counterparts. In particular, the much stronger negative public response to non-western-origin online GenAI services in general and DeepSeek in particular, in the form of privacy concerns and lack of willingness to adopt, presents a considerable challenge for AI companies and governments.

A. Practical Implications

For non-western GenAI developers, building trust—through clear communication and robust privacy controls—is key. Although DeepSeek presents itself as a technically capable AI with demonstrated outputs and cost advantages relative to western competition, it suffers greatly from low user trust due to its foreign origin. Heightened privacy concerns, reflected in low ACR values, often extend beyond general aversion to Chinese technology to fears of government access and data misuse. Given the difficulty of entering established markets, lower pricing alone may not drive adoption; the findings suggest that quality and accuracy influence user decisions more strongly. Thus, achieving superior product quality and clearly communicated privacy practices—beyond legal requirements and required transparency—remains critical.

For established western GenAI providers, public willingness to adopt services like ChatGPT is high, yet privacy concerns remain—particularly regarding government monitoring and data exploitation. Although OpenAI has taken measures, such as providing options to disable chat history, these do not meet public expectations. Data sharing without user permission and potential government data access indicates the necessity for stronger trust measures. As cybersecurity incidents often cause information leakage from cloud or third-party servers, meeting legal standards alone is insufficient; providers must clearly communicate how user data is used, stored, and shared.

Finally, the socio-demographic data collected in this study can inform the design of GenAI solutions across industries and services. The low ACR for non-western GenAI in almost all characteristics reflects a more generalized level of concern, whereas the higher ACR among western AI in law-educated and self-employed respondents suggests greater willingness to adopt such tools—possibly due to better legal understanding or perceived benefits. Tailored educational and privacy guidelines, emphasizing compliance and safe use, should target user groups with low ACR such as non-technical employees, adults aged 55+, peripheral populations, and infrequent AI users.

B. Social Implications

Growing privacy concerns around online GenAI services have broad social implications, impacting public trust in technology, geopolitics, and digital ethics. Fundamentally, privacy concerns about user data in online GenAI services reflect the tension between public's perception of rapidly evolving technologies and the slower-moving data protection laws. This

"cat-and-mouse" dynamic often erodes trust in emerging GenAI technologies, potentially hindering their adoption despite their vast potential across sectors such as customer service, education, and mental health.

The cultural and legal framework of online GenAI services strongly affects global power dynamics and the race for technological leadership in the development of online GenAI services. This is evident in the surprise over DeepSeek's performance and China's ambition to challenge the U.S.-centric "techno-hegemony" through GenAI and related technologies. Such geopolitical rivalry may create a new "Digital Iron Curtain," where access to advanced tools becomes restricted based on trust and national alignment rather than user merit or benefit.

At the same time, concerns about the potential leakage of sensitive private information and Intellectual Property (IP) data, along with GenAI learning from user input—which may itself be sensitive—raise significant ethical issues, including data misuse and corporate espionage. This has, in part, been addressed by government regulation (e.g.: GDPR) but will need ongoing attention to ensure that regulation and scientific progress remain aligned. The consistently low ACRs in high risk sectors such as financial services and education suggest a need for sector specific ethical guidelines and data handling rules to prevent sensitive information disclosure.

C. Limitations and Future Research

As an initial study of user perspectives on privacy concerns in online GenAI services, this study has several limitations that suggest starting points for future work. First, given the rapid evolution of technologies, regulation, and public attitudes, the cross-sectional survey design captures public perception at only a single point in time. A longitudinal follow-up study—as online GenAI services progress, new privacy laws, regulations, or major data breaches emerge—would be highly informative.

A potential limitation of the present study is its cross-cultural nature, even though a diverse cross-section of the population of Israel responded to the survey. While the sample here is informative about the attitudes of GenAI users toward privacy issues, a more geopolitically and culturally widespread study is a subject for future work to better determine global trends and national differences in privacy concerns and willingness to adopt online GenAI services.

Generalizability and the Context: Another issue relates to generalizability and Interpretation Caveats. Results should be understood in the Israeli cultural context. Users in other countries may have different perceptions of privacy, trust and willingness to use online GenAI services depending on local regulations, technology-readiness or geopolitical concerns. For example, the heightened caution toward non-western online GenAI services found in this study may be partly attributed to local concerns regarding geopolitics/risk. Thus, findings should be interpreted as grounded in the current setting but can still provide strong indicative perception patterns.

Replications of this work should be conducted in different countries to examine generalizability and potential cross-national differences.

An additional limitation relates to the sampling method and sample size. The use of a non-probability sample and a relatively small number of respondents limit the external validity of the findings.

Future research should employ larger, stratified, or probabilistic samples to validate and extend the results across broader populations and geopolitical contexts.

Moreover, the factors driving privacy concerns could be further explored. Future research may investigate whether trust in the AI service providers increases with additional third-party certifications or publicly verified data encryption standards.

CONFLICT OF INTEREST

The authors declare no conflict of interest.

AUTHOR CONTRIBUTIONS

AS had led the research with the conceptual framework, conducted the research, analyzed the data and wrote the paper; IS provided research guidelines and supervisory role; all authors had approved the final version.

REFERENCES

AP. Did DeepSeek copy ChatGPT to make new AI chatbot? Trump adviser thinks so. ***AP Press***. Available: https://www.newsbreak.com/the-associated-press-510077/3782434624981-did%20deepseek-copy-chatgpt-trump-adviser-thinks-so

Ahmed, S. K. 2024. How to choose a sampling technique and determine sample size for research: A simplified guide for researchers. ***Oral Oncology Reports***, 12: 100662. https://doi.org/10.1016/j.oor.2024.100662

Albadarin, Y., Saqr, M., Pope, N., & Tukiainen, M. 2024. A systematic literature review of empirical research on ChatGPT in education. ***Discover Education***, 3(1): 60. https://doi.org/10.1007/s44217-024-00138-2

Brandimarte, L., Gutmann, J., Muehlheusser, G., & Weber, F. 2025. Privacy concerns and willingness to adopt AI products: A cross-country randomized survey experiment. ***CESifo*** Working Paper. no. 11774. Available: https://hdl.handle.net/10419/3168881

Bhattacherjee, A. 2012. Social science research: Principles, methods, and practices. ***Textbooks Collection:*** 3. http://scholarcommons.usf.edu/oa_textbooks/3

Choudhury, A., & Shamszare, H. 2023. Investigating the impact of user trust on the adoption and use of ChatGPT: Survey analysis. ***Journal of Medical Internet Research***, 25: e47184.

Carroll, D. R. 2021. Cambridge analytica. In ***Research handbook on political propaganda***: 41–50. Edward Elgar Publishing. https://doi.org/10.4337/9781789906424.00010

Cubio, J. V. 2025. The influence of privacy, bias, and surveillance concerns on teacher's willingness to use artificial intelligence in education. ***International Journal of Research and Innovation in Social Science***, *9*(3s): 3192–3208. https://dx.doi.org/10.47772/IJRISS.2025.903SEDU0240

Elciyar, K. 2025. Users' privacy behaviors in response to WhatsApp policy changes. ***Information & Computer Security***. https://doi.org/10.1108/ICS-04-2024-0096

Farayola, O. A., Olorunfemi, O. L., & Shoetan, P. O. 2024. Data privacy and security in it: a review of techniques and challenges. ***Computer Science & IT Research Journal***, 5(3): 606–615. https://doi.org/10.51594/csitrj.v5i3.909

George, A. S., & George, A. H. 2023. A review of ChatGPT AI's impact on several business sectors. ***Partners Universal International Innovation Journal (PUIIJ)***. https://doi.org/10.5281/zenodo.7644359

Cheng, J., & Zeng, J. 2023. Shaping AI's future? China in global AI governance. ***Journal of Contemporary China***, 32(143): 794–810. https://doi.org/10.1080/10670564.2022.2107391

Gibney, E. 2025. China's cheap, open AI model DeepSeek thrills scientists. ***Nature***, 638(8049): 13–14. https://doi.org/10.1038/d41586-025-00229-6

Conroy, G., & Mallapaty, S. 2025. How China created AI model DeepSeek and shocked the world. ***Nature***, 638(8050): 300–301. https://doi.org/10.25082/AMLER.2023.02.009

Gouvi, S. A. P. M. M., Lavidas, K., & Komis, V. 2023. The use of ChatGPT as a learning tool to improve foreign language writing in a multilingual and multicultural classroom. ***Advances in Mobile Learning Educational Research***, 3(2): 818–824. http://doi.org/10.25082/AMLER.2023.02.009

Gude, V. 2023. Factors influencing ChatGPT adoption for product research and information retrieval. ***Journal of Computer Information Systems***, 65(2): 222–231. https://doi.org/10.1080/08874417.2023.2280918

Honnakatti, D. V. 2025. An analytical study on online shopping customers. ***SSRN:*** 5095623. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5095623

Hugging Face. 2025. DeepSeek-R1. ***Hugging Face***. Available: https://huggingface.co/deepseek-ai/DeepSeek-R1

Italiano, L. & Musumeci, N. 2025. OpenAI has little legal recourse against DeepSeek, tech law experts say. ***Business Insider***. Available: https://www.businessinsider.com/openai-little-legal-recourse-against-deepseek-tech-law-experts-2025-1

Kalodanis, K., Rizomiliotis, P., & Anagnostopoulos, D. 2024. European artificial intelligence act: an AI security approach. ***Information & Computer Security***, 32(3): 265–281. https://doi.org/10.1108/ICS-10-2022-0165

Khanfar, A. A., Kiani Mavi, R., Iranmanesh, M., & Gengatharen, D. 2024. Determinants of artificial intelligence adoption: research themes and future directions. ***Information Technology and Management***: 1–21. https://doi.org/10.1007/s10799-024-00435-0

Kovvuru, I., 2025. ChatGPT privacy leak 2025: Deep dive, real-world impact, and industry lessons. ***Medium***. Available: https://medium.com/@ismailkovvuru/chatgpt-privacy-leak-2025-deep-dive-real-world-impact-and-industry-lessons-421f4ad450c0

Kumari, A. 2024. The study on customer satisfaction towards online shopping. ***International Journal for Multidisciplinary Research (IJFMR)***. https://www.ijfmr.com/papers/2024/1/10774.pdf

Lyons, E. 2025. DeepSeek AI raises national security concerns, U.S. officials say. ***CBS News***, Available: https://www.cbsnews.com/news/deepseek-ai-raises-national-security-concerns-trump/

Lomas, N. 2023. ChatGPT-maker OpenAI accused of string of data protection breaches in GDPR complaint filed by privacy researcher. ***TechCrunch***. Available: https://techcrunch.com/2023/08/30/chatgpt-maker-openai-accused-of-string-of-data-protection-breaches-in-gdpr-complaint-filed-by-privacy-researcher/

Maes, S. H. 2025. The circle of life for LLMs. Was the reaction to DeepSeek Justified?. ***Research Gate Preprint***. https://doi.org/10.13140/RG.2.2.21459.49444

Malik, M. S. 2024. Analyzing the trade-offs of data sharing in social networks and privacy concerns. ***International Journal for Electronic Crime Investigation***: 8(4). https://doi.org/10.54692/ijeci.2024.0804213

Mallikarjuna, B., & Chittemsetty, P. 2024. Generative artificial intelligence: Fundamentals and evolution. In Raza, K., Ahmad, N., Singh, D. (Eds)., ***Generative AI: Current trends and applications***: 3–17. Singapore: Springer. https://doi.org/10.1007/978-981-97-8460-8_1

Mauran, C. 2023. OpenAI violated EU privacy and transparency law, complaint alleges. ***Mashable***. Available: https://mashable.com/article/openai-gdpr-complaint-europe-violating-data-protection-laws

Memarian, B., & Doleck, T. 2023. Fairness, Accountability, Transparency, and Ethics (FATE) in Artificial Intelligence (AI) and higher education: A systematic review. ***Computers and Education: Artificial Intelligence***, 5: 100152. https://doi.org/10.1016/j.caeai.2023.100152

Melo, A., Silva, I., & Lopes, J. 2024. Chatgpt: A pilot study on a promising tool for mental health support in psychiatric inpatient care. ***International Journal of Psychiatric Trainees***, 2(2). https://doi.org/10.55922/001c.92367

Molla, C., Mani, L., Bhuiyan, M. R. I., & Hossain, R. 2023. Examining the potential usages, features, and challenges of using ChatGPT technology: A PRISMA-based systematic. ***Migration Letters***, 20(S9): 927–945.

New America. accessed 2025. FAT approaches internet platforms and governments can implement. Available: https://www.newamerica.org/oti/reports/cracking-open-the-black-box/fat-approaches-internet-platforms-and-governments-can-implement/

OECD. 2023. Emerging privacy-enhancing technologies. Available: https://www.oecd.org/en/publications/emerging-privacy-enhancing-technologies_bf121be4-en.html

Oyewhole, A. T., Oguejiofor, B. B., Eneh, N. E., Akpuokwe, C. U., & Bakare, S. S. 2024. Data privacy laws and their impact on financial technology companies: A review. ***Computer Science & IT Research Journal***, 5(3): 628–650. https://doi.org/10.51594/csitrj.v5i3.911

Reuters. 2025. Microsoft probes if DeepSeek-linked group improperly obtained OpenAI data, Bloomberg News reports. Available: https://www.reuters.com/technology/microsoft-probing-if-deepseek-linked-group-improperly-obtained-openai-data-2025-01-29/

Shanklin, W. 2023. OpenAI improves ChatGPT privacy with new data controls. ***Engadget***. Available: https://www.engadget.com/openai-improves-chatgpt-privacy-with-new-data-controls-174851274.html

Smish, J. 2024. The data governance wake-up call from the OpenAI breach. ***Dataversity***. Available: https://www.dataversity.net/the-data-governance-wake-up-call-from-the-openai-breach/

Smith, C. 2025. DeepSeek AI collects tons of data about you and sends it all to China. ***BGR***. Available: https://bgr.com/tech/deepseek-ai-collects-tons-of-data-about-you-and-sends-it-all-to-china

Thompson, A. 2025. Why did DeepSeek tell me it's made by Microsoft? ***Applied AI***. Available: https://www.fastcompany.com/91267647/deepseek-told-me-made-by-microsoft-r1-openai-claude-anthropic-ai-model-copilot

Peñalvo, F. J. G., & Ingelmo, A. V. 2023. What do we mean by GenAI? A systematic mapping of the evolution, trends, and techniques involved in Generative AI. ***International Journal if Interactive Multimedia and Artificial Intelligence (IJIMAI)***, 8(4): 7–16. https://doi.org/10.9781/ijimai.2023.07.006

Poo, M. M. 2025. Reflections on DeepSeek's breakthrough. ***National Science Review***, 12(3): nwaf044. https://doi.org/10.1093/nsr/nwaf044

Ullah, I., Hassan, N., Gill, S. S., Suleiman, B., Ahanger, T. A., Shah, Z., Qadir J., & Kanhere, S. S. 2024. Privacy preserving large language

models: Chatgpt case study based vision and framework. ***IET Blockchain***, 4: 706–724. https://doi.org/10.1049/blc2.12091

Wolford, B. 2025. What is GDPR, the EU's new data protection law? ***GDPR.EU.*** Available: https://gdpr.eu/what-is-gdpr

Wu, X., Duan, R., & Ni, J. 2024. Unveiling security, privacy, and ethical concerns of ChatGPT. ***Journal of Information and Intelligence***, 2(2): 102–115. https://doi.org/10.1016/j.jiixd.2023.10.007

Yang, A. 2025. On DeepSeek, you can watch AI navigate censorship in real time. ***NBC News.*** Available: https://www.nbcnews.com/tech/innovation/deepseek-censorship china-rcna189594

Yao, H., & Tarofder, A. K. 2024. Privacy concerns in e-commerce marketing: A systematic literature review study. ***International Journal of Global Economics and Management***, 2(3): 64–75. https://doi.org/10.62051/IJGEM.v2n3.07

Zeng, J. 2025. The US factor in Chinese perceptions of militarized artificial intelligence. ***International Affairs***: iiae323. https://doi.org/10.1093/ia/iiae323

Zhang, H., & Khanal, S. 2024. To win the great AI race, China turns to Southeast Asia. ***Asia Policy***, 19(1): 21–34. https://doi.org/10.1353/asp.2024.a918871

Zhdanov, D., Bhattacharjee, S., & Bragin, M. A. 2022. Incorporating FAT and privacy aware AI modeling approaches into business decision making frameworks. ***Decision Support Systems***, 155: 113715. https://doi.org/10.1016/j.dss.2021.113715