From Awareness to Practice: A Survey of U.S. Users' Privacy Perceptions in LLM Chatbots

Ece Gumusel
University of Illinois Urbana-Champaign
eceg@illinois.edu

Yueru Yan
Indiana University Bloomington
yueryan@iu.edu

Ege Otenen
Indiana University Bloomington
eotenen@iu.edu

***Abstract*—Interacting with Large Language Model (LLM) chatbots exposes users to new security and privacy challenges, yet little is known about how people perceive and manage these risks. While prior research has largely examined technical vulnerabilities, users' perceptions of privacy—particularly in the United States, where regulatory protections are limited—remain underexplored. In this study, we surveyed 267 U.S.-based LLM users to understand their privacy perceptions, practices, and data-sharing preferences, and how demographics and prior LLM experience shape these behaviors. Results show low awareness of privacy policies, moderate concern over data handling, and reluctance to share sensitive information like social security or credit card numbers. Usage frequency and prior experience strongly influence comfort and control behaviors, while demographic factors shape disclosure patterns of certain personal data. These findings reveal privacy behaviors that diverge from traditional online practices and uncover nuanced trade-offs that could introduce security risks in LLM interactions. Building on these lessons, we provide actionable guidance for reducing user-related vulnerabilities and shaping effective policy and governance.**

I. Introduction

In recent years, both individuals and organizations have increasingly adopted large language model (LLM) chatbots to routine practices. These chatbots interact through multiple modalities with the ability of modeling the user needs. Text interactions, in particular, have grown substantially with the development of LLM chatbots [1], [2]. By consistently aligning with the user's perspective, users build trust over LLM chatbots. However, this increases not only the frequency of personal data disclosure [3], [4], [5], [6] but also the reliance on these chatbots for decision-making across diverse aspects of their lives [7], [8].

Prior research has extensively examined LLM technical vulnerabilities, including data leakage [9], [10], [11], [12], [13], memorization [14], [15], [16], and malicious attacks [17], [18], [19], [20], [21]. In contrast, relatively few studies have addressed user-centered privacy concerns in LLM chatbot interactions and mostly are related to OpenAI's ChatGPT [22], [23], [24], [25]. However, these studies may not reflect the broader population and regional practices and expectations. Recent work has begun to investigate UK-based LLM conversational agent users' privacy behaviors, self-disclosure boundaries, and awareness of LLM-specific privacy issues [26].

Furthermore, as LLM chatbots cause complexities in obtaining users' informed consent at every stage of data collection and storage processes [27], transparency issues in model training further hinder users' ability to evaluate potential benefits and risks [28]. These issues are compounded by a complex and evolving regulatory landscape. In the European Union (EU), the General Data Protection Regulation (GDPR) [29] mandates lawful, fair, and transparent processing of personal data[1], requiring explicit consent and robust user rights, while the EU Artificial Intelligence (AI) Act [30] imposes additional obligations on high-risk in these AI systems, including risk assessments, transparency, and human oversight. In contrast, in the United States (U.S.), AI and data privacy are governed by a fragmented mix of federal and state regulations, and at the federal level, there is no comprehensive AI or data privacy law. President Trump's January 23, 2025 Executive Order 14179 on "Removing Barriers to American Leadership in Artificial Intelligence"[31] further shape federal priorities and procurement requirements, but also create compliance uncertainties for private-sector developers. State-level initiatives add further layers, creating unequal protections where some citizens are safeguarded while others are left vulnerable. Several states have introduced laws and frameworks addressing AI transparency, accountability, bias mitigation, high-risk systems, and consumer data privacy [32].

While these measures represent significant progress, the fragmented, rapidly evolving, and sometimes inconsistent regulatory landscape complicates compliance, enforcement, and cross-jurisdictional application. Most importantly, this regulatory gap leaves U.S.-based users more vulnerable to unfair or unethical practices in AI, including privacy violations in LLM chatbots and there is limited understanding of privacy sensitivities across different user groups in the U.S., where fragmented and inconsistent regulatory frameworks leave pop-

[1] The CCPA, as amended by the CPRA, defines personal data as "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." In this paper, we adopt this definition when referring to *personal data*.

Symposium on Usable Security and Privacy (USEC) 2026
27 February 2026, San Diego, CA, USA
ISBN 978-1-970672-07-7
https://dx.doi.org/10.14722/usec.2026.23005
www.ndss-symposium.org, https://www.usablesecurity.net/USEC/

ulations more vulnerable to privacy risks and harms. As a result, there is no comprehensive understanding of U.S. populations and perspectives, which poses challenges for developing privacy-aware, user-centered LLM chatbot systems. Thus, this study investigates U.S.-based chatbot users to better understand these dynamics, with a particular focus on their privacy awareness, comfort, and decisions to disclose personal data [33], [34], [35].

To investigate U.S. LLM chatbot users, this empirical study organizes the research questions:

- **RQ1.** To what extent do U.S. LLM chatbot users read privacy policies, and how transparent do they find them?
- **RQ2.** How do LLM chatbot privacy practices influence U.S. LLM chatbot users' perceived privacy concerns and potential risks?
- **RQ3.** How likely are U.S. LLM chatbot users to exercise control over their privacy preferences based on their perceived privacy concerns and comfort levels?
- **RQ4.** How comfortable are U.S. LLM chatbot users to disclose personal data when interacting with LLM chatbots?
- **RQ5.** What types of personal data do U.S. LLM chatbot users consider sensitive when interacting with LLM chatbots?

We conducted a large-scale survey of 267 U.S.-based LLM chatbot users to examine privacy awareness, perceptions, and data-sharing behaviors. Our findings reveal that users generally have low awareness of privacy policies and read them sparingly. Notably, males, frequent chatbot users, and those with moderate technical experience exhibited slightly higher awareness. Participants reported moderate perceived privacy risks but expressed skepticism about chatbots' responsible data handling. Younger, heterosexual, less experienced, and frequent users tended to perceive higher risks. Engagement with privacy settings varied: some users proactively adjusted settings, while others were indifferent or hesitant. Frequent chatbot users were more likely to manage settings, whereas demographics, technical experience, and confidence had minimal impact. Comfort with sharing personal data was generally low and influenced primarily by prior chatbot experience rather than demographic factors. Users were highly cautious with sensitive information, such as credit card numbers, social security numbers, and phone numbers, but more willing to share less sensitive preference- or relationship-based data. Data disclosure patterns varied: LGBTQ+[2] users were more likely to share certain sensitive information, while frequent or experienced users tended to share only less sensitive data, reflecting selective and cautious behavior.

In this work, we make the following contributions:

- We present the first empirical U.S.-based study on user-perceived privacy sensitivity, including measurements of various types of personal data sensitivity among U.S. LLM chatbot users, with a focus on the role of prior chatbot experience.
- We show that among U.S. LLM chatbot users, privacy awareness often exists without actionable understanding, leaving users uncertain about how to protect themselves.
- We reveal that consistent privacy concerns observed in traditional online users also apply to LLM chatbot interactions, highlighting increased user vulnerability.
- We provide actionable recommendations for privacy-enhancing technologies, as well as policy and governance guidelines.

II. Background and Related Work

A. LLM Architecture Challenges

Recent literature has addressed security and privacy risks in LLMs [36], [37], especially in model architectures [38], [39], [40], [41], [39], [42]. For example, Staab et al. [9] demonstrated that pretrained LLMs could infer personal data, such as geographic location, income levels, and gender, by leveraging publicly available data combined with user prompts. Tong et al. [10] showed that model outputs could inadvertently expose user-related details. The method of model adaptation also affects privacy vulnerability. Mireshghallah et al. [15] found that full model fine-tuning, particularly targeting the model head, makes LLMs more susceptible to inference attacks than parameter-efficient techniques like adapter-based tuning. Building on this, Lukas et al. [11] introduced more effective extraction strategies, significantly increasing the amount of personal data that can be recovered. Carlini et al. [14] highlighted that models such as GPT-2 could regenerate specific training examples in response to carefully designed prompts, potentially leaking sensitive content to unintended parties. Huang et al. [16] focused specifically on email addresses, showing that LLMs might reproduce them when context cues, such as names, are present in the input. Zanella-Béguelin et al. [12] examined the impact of model updates on privacy leakage, proposing metrics to measure how prior training data continues to influence model outputs over time. Additionally, Jagannatha et al. [13] explored susceptibility across architectures like BERT and GPT-2, highlighting consistent risks of information leakage.

B. Malicious Usage of LLMs

LLMs can be misused for malicious purposes. Falade [43] discussed scenarios where attackers exploit LLMs for impersonation and psychological manipulation. Other studies [44], [45], [46] noted that content filters based on censorship policies may unintentionally introduce biases in retrieval and code-generation tasks. Yin et al. [18] and Monje et al. [19] demonstrated that GPT models could be misused to create malware, including ransomware, keyloggers, and other malicious tools. Wan et al. [47] showed that even a small number of poisoned examples can significantly disrupt model performance, while Yao et al. [48] proposed a backdoor attack combining triggers with prompt tuning. Meisenbacher et al. [49] also showed that LLMs can reliably assess how private

[2] LGBTQ+ indicates standardization to uppercase, treating the term as an acronym for lesbian, gay, bisexual, transgender, queer/questioning identities, with "+" encompassing other related identities.

or sensitive text is, even though humans often disagree on what counts as private.

Addressing these challenges, recent work has begun exploring privacy-preserving techniques. For instance, Wang et al. [50] proposed the RewardDS framework, which aims to minimize the memorization of sensitive personal data during model fine-tuning, offering a promising direction for safer LLM deployment. Wu et al. [51] emphasized the importance of auditing and adversarial testing to ensure fairness, and Hui et al. [52] introduced PLeak, a framework for optimizing adversarial prompt attacks. Su et al. [53] developed a user-centric approach using the PA-BERT-BiLSTM-CRF model to automatically detect privacy leaks in LLM user inputs, demonstrating superior performance on real-world and custom privacy datasets. Despite these efforts, there are still few approaches that consider users' privacy needs and adapt LLMs accordingly.

C. Factors Affecting User Privacy Behaviors in LLMs

Chatbots that incorporate LLMs and advanced user interface features introduce novel risks regarding user privacy. Gumusel et al. [23] conducted semi-structured interviews with 13 participants to perceive harms and risks in LLM chatbots. Ali et al. [25] investigated user behavior on Reddit, focusing on their privacy awareness with engaging with ChatGPT, and provided insights into how users publicly discuss and reflect on their interactions with the model.

Studies show that user privacy shape user privacy decisions in chatbot interactions including willingness to initiate and sustain conversations and to share personal information. Sannon et al. [54] surveyed 385 users and found that users' perceptions of privacy-related behaviors during these interactions could influence their willingness to disclose personal data, thereby exposing potential privacy risks. Agnihotri and Bhattacharya [55] conducted a qualitative study 18 users and found that anthropomorphic chatbot increase user trust and encourage the sharing of more information. Bouhia et al. [56] emphasized that feelings of creepiness and perceptions of risk play a key role in influencing users' privacy concerns, especially when handling sensitive information. Pizzi et al. [57] indicated that users' warmth and competence perceptions of chatbots can influence users' decisions about disclosing personal information. Zhang et al. [22] thematically analyzed user-ChatGPT interaction logs to examine patterns of personal data disclosure and revealed limited user understanding of privacy implications in such interactions. Ischen et al. [4] compared users' comfort in sharing personal information with human-like chatbots, machine-like chatbots, and websites, employing an experimental design to analyze the relationships between privacy concerns, attitudes, and comfort levels. Belen-Saglam et al. [58] found that users have different sensitivity over sharing some personal data types if the context is irrelevant, particularly for sensitive domains such as healthcare and finance. Kwesi et al. [59] also investigated the mental health context, finding that U.S. users often misunderstand the privacy and security of LLM chatbots, conflating human-like empathy with accountability and exposing an "intangible vulnerability" in the protection of emotional disclosures.

Recent work have shown that user privacy in LLM chatbots can vary based on demographic background and prior experience. For example, research on Chinese users' privacy awareness and expectations regarding LLM-based healthcare chatbots [60], UK-based LLM chatbot users [26], [61], and Black older adults' perceptions of U.S.-based text chatbots [62] indicates that certain groups may be particularly vulnerable. Yet, no study has directly examined the privacy attitudes of general U.S. users or how these relate to prior chatbot experience. This work addresses that gap by exploring how U.S. users' characteristics influence their privacy attitudes in LLM chatbots.

III. Methodology

A. Survey Instrument

We conducted a within-subject survey using Qualtrics[3]. The survey was developed by researchers from diverse disciplines and backgrounds in the U.S., including security and privacy, human-computer interaction, cognitive science, information science, law and policy, and statistics. The online survey was developed using insights from prior work [35], [60], [26] and included both participant-reported and participant-perceived questionnaire items. Followed by obtaining consent and confirming participants' prior experience with LLM chatbots—defined using Stanford's AI teaching guide[4]—the survey consisted of seven parts. Part I collected participants' demographic information. Part II assessed participants' prior experience with LLM chatbots. Part III measured participants' perceived informativeness and their experiences reading privacy policies (RQ1). Part IV included five items evaluating perceived privacy concerns and potential risks associated with LLM chatbots (RQ2). Part V examined participants' ability to exercise privacy-control behaviors, such as adjusting privacy settings in LLM chatbots (RQ3). Part VI measured participants' comfort with disclosing personal data (RQ4). Part VII asked about participants' preferences for sharing different types of personal data with LLM chatbots, distinguishing between sensitive information and preference-based information (RQ5), following distinctions used in traditional online privacy studies from the dot-com era [63], [64].

Parts III–VI were assessed with questions participants rated their answers in a five-point Likert-scale, whereas Part VII was a multiple choice items allowing participants to indicate their personal data–sharing preferences among given situations. Table I summarizes the privacy measures items in the questionnaire. The complete set of survey questions can be found in Appendix A-B.

[3] https://www.qualtrics.com/

[4] We adopted Stanford's AI teaching guide: https://teachingcommons.stanford.edu/teaching-guides/artificial-intelligence-teaching-guide/defining-ai-and-chatbots. The term "chatbot" explicitly includes LLMs, defined as: "A computer program that uses an LLM to simulate a conversation with human users, typically through typed text in a software application."

1) Part I: Demographics: The first part of the survey is provided to collect the basic demographic information, including age, gender, sexual orientation, and education level. These variables were later used as predictors in the quantitative analyses to examine potential differences in privacy perceptions and behaviors across demographic groups.

2) Part II: Prior LLM Chatbot Experience: Participants are asked about their prior experience with LLM chatbots, including length of use, confidence in using LLMs, and frequency of daily interactions. These measures are included to assess how familiarity and experience with LLM chatbots relate to privacy attitudes and behaviors. Importantly, we here focus on participants' self-reported experience and confidence, rather than data from third-party application usage (e.g., ChatGPT, Character AI, etc.).

3) Part III: Reading Privacy Policies: Participants report the extent to which they engage with privacy policies and terms of service for LLM chatbots. Items include:

- "I review the privacy policy or terms of service provided by LLM chatbots."
- "I feel well-informed about privacy measures and data handling practices of LLM chatbots before starting to use it."

Responses are recorded on a five-point Likert scale (1 = Strongly Disagree, 5 = Strongly Agree). Higher scores indicate greater engagement with privacy policies. These items are primarily included to address **RQ1**, examining the extent to which users read privacy policies and perceive transparency. However, these items were measured separately to assess users' review behaviors and their perceived informativeness of privacy policies.

4) Part IV: Perceived Privacy Concerns and Potential Risks: Participants rate their concerns and perceptions of privacy risks related to LLM chatbots using a five-point Likert scale (1 = Strongly Disagree, 5 = Strongly Agree). Items include:

- "I am concerned about the potential privacy risks associated with interacting with LLM chatbots."
- "I am confident that my personal data is handled securely and responsibly by LLM chatbots after our interaction."
- "LLM chatbots always explain how they use and store the information I provide during the conversation."
- "LLM chatbots respect my privacy by not asking for unnecessary personal information during the interaction."
- "LLM chatbots demonstrate a commitment to safeguarding my privacy after the interaction has ended."
- "LLM chatbots successfully balance user experience with privacy considerations throughout the entire interaction process."

These items were guided throught the prior studies [26], [35], [65] to address **RQ2** and assess how users' perceptions of LLM chatbot privacy practices influence their perceived risks and trust. These items were assessed using Cronbach's alpha, which yielded a reliability coefficient of $\alpha = 0.77$ for the Perceived Privacy Risks subscale (95% CI [0.71, 0.80]).

5) Part V: Exercise Control over Privacy Preferences: Participants indicate how likely they would be to review or adjust their privacy settings after interacting with an LLM chatbot (1 = Very Likely, 5 = Very Unlikely). This measure captures perceived control over personal information and are included to address **RQ3**, examining the relationship between perceived privacy concerns, comfort, and proactive privacy behavior.

6) Part VI: Comfort of Disclosing Personal Data: Participants reported their comfort with sharing personal information on a Likert scale (1 = Very Uncomfortable, 5 = Very Comfortable). Higher scores indicate greater willingness to disclose information. This measure are included to address **RQ4**, focusing on user comfort during LLM interactions.

7) Part VII: Disclosing Personal Data Type Preferences: The final part of the survey asks participants which types of personal information they are most hesitant to share via two "select all that apply" questions. The first question included sensitive information (e.g., social security number, credit card number, medical data), and the second included preference-based information (e.g., favorite snack, favorite TV show). These data types were adopted directly from prior studies [63], [64]. These items address **RQ5**, identifying which types of personal data users consider sensitive when interacting with LLM chatbots.

B. Data Collection

1) Pilot Study and Reliability Check: Before distributing the survey, we conducted a pilot study to evaluate the research procedures, estimate the average survey completion time, and assess the reliability and consistency of the survey questions. 12 active U.S.-based LLM chatbot users (7 women, 4 men, and 1 non-binary) whose ages ranging from 18 to 55+ participated in the pilot study. They provided detailed feedback on question comprehension, interpretation, and response processes. Based on their input, we refined the wording of questions, scale descriptions, and instructions to ensure clarity and consistency, and shortened the questionnaire. We then performed preliminary statistical analyses, including internal consistency checks and item-level correlations.

Following these refinements, we conducted a second pilot with 7 active U.S.-based LLM chatbot users. We assessed their understanding and ability to complete the survey, which took approximately 10 minutes. The results indicated that the majority of participants could successfully comprehend and complete the survey, after which we proceeded with full distribution to the target population.

2) Recruitment: The survey was conducted over four months. Using convenience sampling approach, the researchers first posted recruitment information and the online survey link (Appendix A-A) on various popular social media platforms, including LinkedIn, X, and Reddit, and later asked friends and colleagues to further share the survey through their social networks. This approach allowed us to collect data beyond the researchers' immediate social circles and capture responses from a diverse range of U.S.-based LLM chatbot

TABLE I: Summary of Survey Privacy Measure Items

Survey Privacy Measures and Items
Part III: Reading privacy policies [29], [66]
I feel well-informed about privacy measures and data handling practices of LLM chatbots before starting to use it.
I review the privacy policy or terms of service provided by LLM chatbots.
Part IV: Perceived privacy concerns and potential risks (e.g., data handling practices, breaches, transparency) [26], [35], [65]
Cronbach's alpha for the Perceived Privacy Risks subscale = 0.77 (95% CI [0.71, 0.80])
I am concerned about the potential privacy risks associated with interacting with LLM chatbots.
I am confident that my personal data is handled securely and responsibly by LLM chatbots after our interaction.
LLM chatbots always explain how they use and store the information I provide during the conversation.
LLM chatbots demonstrate a commitment to safeguarding my privacy after the interaction has ended.
LLM chatbots successfully balance user experience with privacy considerations throughout the interaction process.
Part V: Exercise control over privacy preferences [26], [35], [65]
"How likely are you to review or adjust your privacy settings related to a LLM chatbot after concluding the conversation?"
Part VI: Comfort of disclosing personal data [63], [64], [35], [65]
"How comfortable are you with sharing personal information with LLM chatbots?"
Part VII: Disclosing personal data type preferences from prior studies [63], [64]
Sensitive information: Social security number, credit card number, phone number, income, medical information, postal address, full name, computer information (e.g., device ID, IP address, password), email address, gender, sexual orientation, education, political affiliation, religion, race, social media profiles
Preference-based information: Favorite snack, favorite TV show, favorite movie, favorite pet, favorite sport, favorite brand, favorite restaurant, favorite city, favorite artist, favorite friend, favorite family member, favorite teacher

users. During recruitment, we deliberately avoided mentioning that the study focused on privacy and security to reduce potential sample bias. Participants were required to meet the following criteria: (1) 18 years or older, (2) residing in the U.S., (3) proficient in English, and (4) having prior experience with text-based LLM chatbots. All participants were volunteers and provided informed consent prior to participation.

3) Sample Size: Of the total of 311 survey respondents, 12 respondents did not provide consent, 3 had never used text-based LLM chatbots, 2 did not reside in the U.S., and 29 exited the survey before completion. After excluding these invalid responses, 267 participants successfully completed the survey. Our sample represented a diversity in terms of age, gender, sexual orientation and prior LLM chatbot experience. The demographic distribution also aligned with prior research on Internet privacy attitudes [35], [67], [64] and supported meaningful insights into the current U.S. LLM chatbot user population. The average survey completion time, including the consent form, was 8.14 minutes.

With 267 valid responses, the study was adequately powered to detect medium-sized effects. Although smaller subgroups (e.g., participants aged 55+, $n = 18$) might be underpowered for small effects, the overall sample is sufficient for meaningful analyses of LLM chatbot experience, user confidence, and privacy attitudes. In other words, we excluded only education level from the demographics due to limited statistical power.

4) Participants' Background: A total of 267 participants completed the study, providing a diverse sample of LLM chatbot users in the United States. Table II summarizes participant demographics alongside 2020 U.S. Census comparisons, as well as prior experience with LLM chatbots. The sample skews younger than the general U.S. population, with 60.7% of participants aged 18–34 compared to 23.1% nationally. Older adults (45+) are underrepresented. Gender distribution is roughly balanced, with slightly more females (47.2%) than males (42.5%), and 10.1% identifying as LGBTQ+. In terms of sexual orientation, 65.5% identified as heterosexual and 34.5% as LGBTQ+. Education level is higher than the national average. Nearly three-quarters of participants hold at least a bachelor's degree, reflecting the tendency of early adopters of emerging technologies to have higher education levels.

In addition to the demographics, participants reported varied prior experience with LLM chatbots. Most had used these systems for less than one year (56.9%), though a substantial portion (30.0%) reported one to three years of experience. Confidence in using LLMs was generally high, with 46.1% indicating they felt "very" or "extremely" confident. Daily interaction frequency varied, with 29.2% using LLMs rarely and 13.9% interacting multiple times per day.

C. Data Analysis

1) Quantitative Analysis: Our independent variables were the participants demographics (age, gender, sexual orientation) and prior LLM chatbot experience (length of use, confidence, and daily interaction frequency), while our dependent variables were privacy measures (Table I). We first descriptively analyzed means, standard deviations, and distributions for each privacy-related item in Parts III to VII of the survey (Table I). Then, we examined the influence of demographic factors (age, gender, sexual orientation) and prior LLM chatbot experience (length of use, confidence, and daily interaction frequency) on privacy perceptions by using generalized linear models (GLMs). Because the privacy items in Part III–VI were assessed using a five-point Likert scale, we treated these items as continuous dependent variables. Personal data types in Part VII were treated as categorical variables for the subsequent

TABLE II: Participants’ Background: Demographics, Census Comparison, and LLM Chatbot Experience

Characteristic	**Participant (%Sample)**	**U.S. Census**
Age		
18–24	54 (20.2%)	9.5%
25–34	108 (40.4%)	13.6%
35–44	59 (22.1%)	12.5%
45–54	28 (10.5%)	12.6%
55+	18 (6.7%)	14.5%
Gender		
Female	126 (47.2%)	50.8%
Male	114 (42.5%)	49.2%
LGBTQ+	27 (10.1%)	–
Sexual Orientation		
Heterosexual or straight	175 (65.5%)	–
LGBTQ+	92 (34.5%)	–
Education Level		
Less than high school	1 (0.4%)	10%
High school or equivalent	8 (3.0%)	28%
Some college/Associate’s	33 (12.4%)	30%
Bachelor’s degree	102 (38.2%)	36%
Master’s degree	91 (34.1%)	14%
Professional/Doctoral degree (Master & Higher)	32% (12.0%)	
LLM Chatbot Experience: Length of Use		
Less than 6 months	66 (24.7%)	–
6 months–1 year	86 (32.2%)	–
1–3 years	80 (30.0%)	–
More than 3 years	35 (13.1%)	–
LLM Chatbot Experience: Confidence		
Extremely Confident	33 (12.4%)	–
Very Confident	90 (33.7%)	–
Moderately Confident	81 (30.3%)	–
Slightly Confident	47 (17.6%)	–
Not Confident	16 (6.0%)	–
LLM Chatbot Experience: Daily Interaction Frequency		
Rarely	78 (29.2%)	–
Few times a month	64 (24.0%)	–
Few times a week	68 (25.5%)	–
Once a day	20 (7.5%)	–
Multiple times a day	37 (13.9%)	–

GLMs. These items and the other categorical predictors (demographic factors and prior LLM chatbot experience) were dummy-coded. Predictor significance was evaluated using Wald χ^2 tests, with 95% confidence intervals computed for all coefficients. Interaction terms between demographics and prior chatbot experience were also explored to assess whether the effect of LLM use on privacy attitudes varied across subgroups. This approach allowed us to quantify both the independent and interactive effects of demographics and prior chatbot experience on multiple dimensions of privacy behavior and perceptions.

2) Qualitative Analysis: Free-text responses (e.g., ”Other: please specify”) were reviewed and inductively coded using thematic analysis [68] to capture users’ perceptions and insights beyond the provided questionnaire options. A primary researcher initially read all responses and iteratively developed a codebook. A second researcher then independently coded the responses according to this codebook. Inter-coder reliability was assessed using Cohen’s Kappa (κ), yielding $\kappa > 0.91$ across the open-ended questions, indicating excellent agreement. The researchers subsequently identified the overarching themes corresponding to the final codes.

D. Ethical Considerations

This study was approved by our institute’s Institutional Review Board (IRB) and posed minimal risks to the study participants. Prior to the survey, we ensured that participants were informed about the purpose of the study and the consent process. They were acknowledged that the survey was entirely voluntary. They had the right to opt-out and leave the survey at any time. Additionally, participants could skip any questions they did not feel comfortable answering. Participants were also informed that the data would be used solely for research purposes and deleted in accordance with the data retention guidelines described in the Informed Consent Statement (Appendix A-B). All personally identifiable information (PII) collected during the survey was removed to protect participants’ confidentiality and comply with ethical guidelines for research involving human subjects. No participants raised concerns regarding compensation or participation risks in their final free-text responses, nor did they contact the research team or the IRB for feedback.

IV. Results

In this section, we present the survey findings in relation to our research questions, providing a comprehensive understanding of the factors that shape U.S.-based LLM chatbot users' privacy perceptions.

A. RQ1: Perceived Privacy Policy Awareness

Summary: U.S. LLM chatbot users generally had low awareness of privacy policies and reported limited reading of them. Males, frequent chatbot users, and those with moderate technical experience have higher awareness level.

The findings showed that LLM chatbot users had low awareness of policies, with perceived informativeness ($M = 2.30$ ($SD = 0.99$; $95\% CI$ $[2.18, 2.42]$)) and self-reported reading ($M = 2.38$ ($SD = 1.15$; $95\% CI$ $[2.24, 2.52]$)) (see Figure 1). Descriptive statistics for participants' engagement with privacy policies indicate generally low awareness and reading behavior. For the item assessing how well-informed participants felt about privacy measures, the mean score was 2.30 (SD = 0.99), suggesting that, on average, users felt slightly below neutral in being informed. Similarly, self-reported review of privacy policies had a mean of 2.38 (SD = 1.15), indicating limited engagement with policy content. Overall, these results suggest that U.S. LLM chatbot users demonstrate modest attention to privacy policies and perceive them as only moderately informative.

We further investigated the influence of demographics (gender, sexual orientation, and age) and prior chatbot experience on the perceived privacy policy awareness. Gender significantly predicted perceived informativeness of privacy policies, with males reporting higher scores than females ($\beta = 0.37$, $p = 0.007$). Sexual orientation and age were not significant predictors. For self-reported reading, while sexual orientation (LGBTQ+) showed a marginal trend ($\beta = 0.36$, $p = 0.050$) that did not reach statistical significance, neither gender nor age showed significant effects. In addition, perceived informativeness was higher in participants who used chatbots multiple times per day ($\beta = 0.81$, $p = 0.010$) and those with 1–3 years of technical experience ($\beta = 0.80$, $p = 0.006$), while other experience levels and lower engagement had weaker effects. Self-reported reading was also positively related to frequent engagement, with multiple-times-per-day users showing a marginal increase but not significant ($\beta = 0.85$, $p = 0.053$) and 6–12 months of prior experience showing a positive non-significant trend ($\beta = 0.33$, $p = 0.072$).

B. RQ2: Perceived Privacy Risks

Summary: U.S. LLM chatbot users perceived moderate privacy protection but doubted responsible data handling, with higher risk perceived by younger, heterosexual, less experienced, and frequent users.

After assessing participants' perceived privacy concerns across five survey items, we found moderate perceptions of privacy protection, including how chatbots explain data use, safeguard privacy after interactions, and balance user experience with privacy considerations (M = 2.27–3.08, SD = 0.87–1.08, 95% CIs [2.14, 3.20]) (see Figure 2). Participants yet generally disagreed that LLM chatbots handle data responsibly (M = 1.98, SD = 0.91, 95% CI [1.87, 2.09]).

The further demographic and prior experienced showed interesting findings. Sexual orientation significantly predicted perceived privacy risk. LGBTQ+ participants reported lower risk perceptions than heterosexual participants ($\beta = -0.33$, $p = 0.001$). Age effects were also observed: participants aged 35–44 ($\beta = -0.47$, $p < 0.001$) and 55+ ($\beta = -0.41$, $p = 0.023$) reported lower risk than those aged 18–24. Gender did not significantly predict perceived risk. Participants with less than six months of technical experience reported higher risk than those with 1–3 years ($\beta = 0.26$, $p = 0.025$). Confidence level was not a significant predictor. Frequency of chatbot use predicted risk: multiple daily uses ($\beta = 0.57$, $p = 0.006$) and once-per-day use ($\beta = 0.53$, $p = 0.039$) were associated with elevated risk, while users indicated rarely using LLMs showed marginally lower risk, but this effect did not reach statistical significance ($p = 0.070$).

C. RQ3: Privacy Control Practices

Summary: U.S. LLM chatbot users have mixed/uncertain engagement with privacy settings, ranging from proactive adjustments to indifference or hesitation. Users who interact with LLM chatbots more frequently tend to be more likely to adjust their privacy settings, while demographics and technical experience and confidence have little apparent influence.

Participants were asked how likely they were to review or adjust their privacy settings after interacting with an LLM chatbot. Responses were generally neutral ($M = 3.19$, $SD = 1.40$), indicating uncertainty about making changes. Among 267 respondents, 30.3% were neutral, 26.6% were likely, and 14.2% were very likely to review their settings, while 22.1% were unlikely and 6.74% very unlikely. Overall, 41% of respondents indicated some likelihood of reviewing or adjusting their privacy settings.

None of the demographic variables significantly predicted participants' likelihood to adjust privacy settings. Although LGBTQ+ participants and older age groups tended to report slightly lower likelihoods, these differences were not statistically significant (all $p > 0.1$). However, among the participants who used chatbots multiple times per day reported higher likelihoods of adjusting privacy settings ($\beta = 0.62$, SE = 0.24, 95% CI [0.15, 1.09], $p = 0.010$), and those who used chatbots once per day also showed elevated likelihoods ($\beta = 0.92$, SE = 0.29, 95% CI [0.36, 1.49], $p = 0.001$). Participants who used chatbots rarely tended to report slightly lower likelihoods ($\beta = -0.38$, SE = 0.21, 95% CI [-0.79,

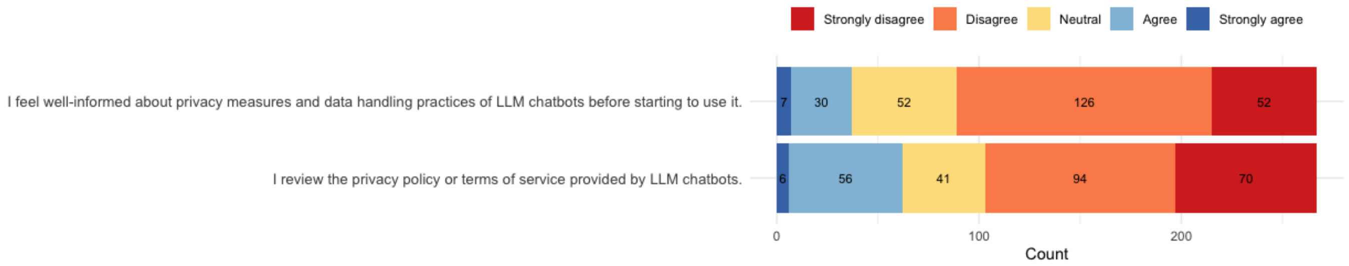

Fig. 1: Distribution of user responses for five-point Likert scale questions for perceived privacy policy awareness items.

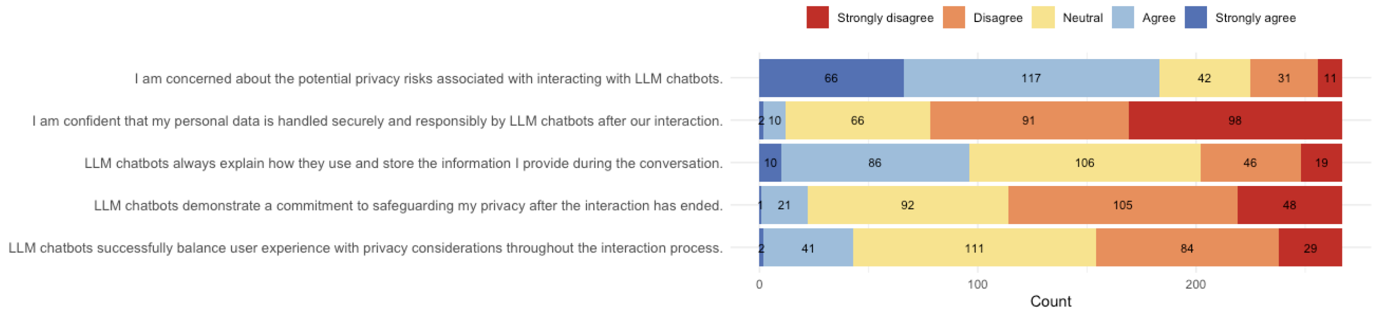

Fig. 2: Distribution of user responses for five-point Likert scale questions for perceived privacy risk items.

0.02], $p = 0.065$). Technical experience and confidence were not significant predictors (all $p > 0.1$).

D. RQ4: Comfort of Sharing Personal Data

Summary: U.S. LLM chatbot users are generally uncomfortable sharing personal data. Comfort levels are influenced more by prior experience with chatbots than by demographic factors.

To understand the respondents' comfort level with sharing personal data with LLM chatbots, the survey included a question measured on a 5-point Likert scale (1 = Very uncomfortable to 5 = Very comfortable). The results indicated an overall discomfort with mean score of 2.18 ($M = 2.18$, $median = 2$, $SD = 1.23$). 39.85% of respondents felt very uncomfortable 21.08% were uncomfortable, 15.47% were neutral 17.21% were comfortable, and only 2.51% felt very comfortable. Respondents were moderately uncomfortable sharing personal data with LLM chatbots ($M = 2.18$, $median = 2$, $SD = 1.23$).

The results further indicated that comfort levels did not differ meaningfully by user demographics (gender, sexual orientation, or age) ($p > 0.05$ for all comparisons). Several aspects of prior experience were significantly associated with comfort levels. Specifically, respondents with accounts for more than three years reported lower comfort ($\hat{\beta} = -0.537$, 95% CI = $[-1.057, -0.016]$, $p = 0.043$). Prior experience explained more variance in comfort levels than demographic characteristics (Adjusted $R^2 = 0.056$, $F(24, 242) = 1.654, p = 0.032$). Frequency of daily interactions was positively associated with comfort: respondents who interacted with data a few times a month ($\hat{\beta} = 1.309$, 95% CI = $[0.574, 2.044]$, $p < 0.001$), a few times a week ($\hat{\beta} = 1.361$, 95% CI = $[0.590, 2.131]$, $p < 0.001$), multiple times a day ($\hat{\beta} = 1.356$, 95% CI = $[0.427, 2.284]$, $p = 0.004$), and rarely ($\hat{\beta} = 1.366$, 95% CI = $[0.665, 2.067]$, $p < 0.001$) all reported higher comfort. Confidence measures were not statistically significant.

E. RQ5: Personal Data Sensitivity

Summary: U.S. LLM chatbot users were cautious with sensitive data, especially credit cards, social security numbers, and phone numbers, but more willing to share preferences and relationship-based information. Users who identified themselves as LGBTQ+ were more likely to share social security numbers, income, computer information, and postal addresses, male participants were more likely to share credit cards, phone numbers, postal addresses, and religion, certain age groups shared specific items like gender or sexual orientation, and frequent or experienced users generally shared less.

1) High Sensitive: As shown in Figures 3, most of the participants reported high discomfort sharing sensitive data with LLM chatbots, particularly credit card numbers (94.8%), social security numbers (91.4%), and phone numbers (82.8%). Moderate discomfort was reported for computer information (e.g., password) (80.9%), postal addresses (80.5%), and medical information (70.0%). Participants were more comfortable sharing less sensitive data such as income (28.8%), political affiliation (28.5%), sexual orientation (18.7%), religion (18.7%), age (14.6%), race (12.4%), gender (11.2%), and education (10.9%). Some participants also provided responses in the

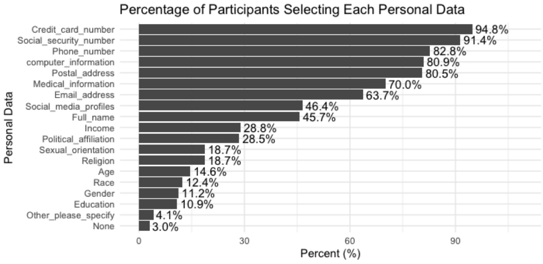

Fig. 3: Participant discomfort levels for sharing sensitive personal data with LLM chatbots.

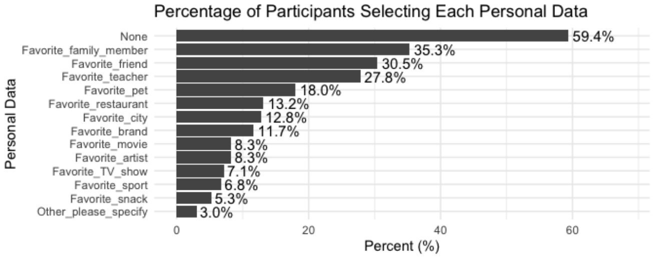

Fig. 4: Participant discomfort levels for sharing preference-based personal data with LLM chatbots.

”Other” category, including statements such as *“I wouldn’t share anything with this”*, *“without my consent there won’t be any data I can share with”*, and *“Maybe only data related to intellectual property”*. These quotes reflect participants’ cautious and conditional approach to sharing personal information with LLM chatbots.

Further, we conducted multiple regression analyses to explore the relationship between respondent characteristics and the likelihood of sharing sensitive personal data. Participants identifying as LGBTQ+ were more likely to disclose their social security number ($\hat{\beta} = 6.80, p = 0.037$), income ($\hat{\beta} = 2.39, p = 0.022$), computer information (e.g., password) ($\hat{\beta} = 0.19, p = 0.011$), and postal address ($\hat{\beta} = 0.40, p = 0.037$). Male participants were more likely to disclose credit card numbers ($\hat{\beta} = 0.062, p = 0.029$), phone numbers ($\hat{\beta} = 0.36, p = 0.019$), postal addresses ($\hat{\beta} = 0.39, p = 0.022$), and religion ($\hat{\beta} = 2.31, p = 0.039$). Age predicted disclosure of specific information: participants 55+ disclosed more income ($\hat{\beta} = 4.28, p = 0.029$), gender ($\hat{\beta} = 15.08, p = 0.004$), and race ($\hat{\beta} = 5.75, p = 0.047$), while those 35–44 disclosed more sexual orientation ($\hat{\beta} = 3.88, p = 0.027$). Education data type was associated with higher disclosure across most age groups, including 25–34 ($\hat{\beta} = 11.16, p = 0.029$), 35–44 ($\hat{\beta} = 15.01, p = 0.021$), 45–54 ($\hat{\beta} = 18.51, p = 0.026$), 55+ ($\hat{\beta} = 53.95, p = 0.002$), and LGBTQ+ individuals ($\hat{\beta} = 3.17, p = 0.040$).

For postal addresses, participants who had the information available were more likely to share it ($\hat{\beta} = 7.05$, $p = 0.041$), while frequent daily sharers were less likely to disclose it ($\hat{\beta} = 0.059$, $p = 0.024$). Those with less than six months of experience sharing their full name were more likely to do so ($\hat{\beta} = 2.33$, $p = 0.038$), while frequent full-name sharers showed reduced disclosure ($\hat{\beta} = 0.209$, $p = 0.036$). Prior experience consistently decreased sharing of computer information across frequencies, including a few times per week ($\hat{\beta} = 0.070$, $p = 0.025$), multiple times per day ($\hat{\beta} = 0.089$, $p = 0.042$), once per day ($\hat{\beta} = 0.024$, $p = 0.006$), and rarely ($\hat{\beta} = 0.069$, $p = 0.017$). Sharing email a few times per week ($\hat{\beta} = 0.210$, $p = 0.049$) and gender information ($\hat{\beta} = 0.086$, $p = 0.034$) was also less likely. Finally, prior experience in the “Other” category reduced disclosure ($\hat{\beta} = 0.011$, $p = 0.043$).

2) Less Sensitive: For less privacy-sensitive preferences, respondents were generally willing to share relationship-based data such as favorite family member (35.3%), friend (30.5%), and teacher (27.8%). In contrast, consumer or entertainment preferences—like pet (18.0%), restaurant (13.2%), city (12.8%), brand (11.7%), movie (8.3%), artist (8.3%), TV show (7.1%), sport (6.8%), and snack (5.3%)—were less commonly shared. Additionally, 3.0% selected ”Other” specifying that they would not be comfortable sharing *any data* with LLM chatbots at all. In general, 68.0% of the respondents were comfortable sharing some personal preferences, while a substantial portion (59.4%) indicated that they would not hesitate to share *any* of the less sensitive data provided (see Figure 4).

In contrast to high sensitive personal data, here, demographic variables and prior experience did not significantly predict disclosure of less sensitive information. Slightly lower sharing by LGBTQ+ participants and older adults was not statistically significant ($p > 0.1$). Although some frequent users showed marginally higher odds of sharing certain personal data items, these effects were generally nonsignificant. Technical experience and confidence levels also did not significantly influence sharing behavior ($p > 0.1$).

V. Discussion

In this section, we discuss the key insights from our study, highlight its originality, provide recommendations, and outline its limitations to guide future research.

A. Perceived Risks vs Protective Actions

Users need to understand the privacy risks of LLM chatbots and manage their privacy, either by being informed of current risks (e.g., notices, policies) or by setting their own preferences [69], [70]. Yet, as in traditional online privacy [71], [65], a gap often exists between users’ privacy intentions and their actual behavior—a phenomenon widely discussed as the privacy paradox, where individuals express concern about privacy but fail to enact corresponding protective actions due to limited awareness, perceived complexity, or trade-offs with convenience and utility [72], [73].

First, the survey showed that many U.S. LLM chatbot users are not fully well-informed by privacy policies. This limited understanding affects users’ ability to make informed privacy choices and manage their data effectively [74]. The combination of limited knowledge, uncertainty, and reliance on complex policies underscores the need for more accessible, actionable privacy guidance to empower users in safely navigating interactions with LLM chatbots. Extensive research across both AI and non-AI contexts—such as online behavioral advertising, the Internet of Things, and smart home technologies—similarly finds that complex or abstract policy disclosures may increase general privacy awareness without enabling concrete protective actions, thereby reinforcing the gap between expressed concern and actual behavior. The combination of limited knowledge, uncertainty, and reliance on complex policies underscores the need for more accessible, actionable privacy guidance to empower users in safely navigating interactions with LLM chatbots. Second, although participants expressed discomfort interacting with LLM chatbots and showed privacy sensitivity, many were uncertain how to manage their privacy effectively and lacked clear knowledge of protective measures. Consequently, U.S. users showed uncertainty about adjusting privacy settings or controlling their data, even when aware of potential risks. Here, privacy loss may also be implicitly perceived as an acceptable trade-off for the utility and convenience of LLM chatbots.

We contribute to the literature by showing that, for U.S. LLM chatbot users, this uncertainty reveals a critical gap between privacy awareness and actionable understanding: users may recognize risks but remain unsure—or unaware of how—to protect themselves effectively. These findings call special attention for LLM chatbot ecosystems that pair privacy awareness with clear, usable controls that support informed and actionable privacy management.

B. Extending Legally Defined PII

Users' selective approach to sharing personal data with LLM chatbots reflects a sophisticated, context-dependent negotiation of privacy rather than a simple binary of willing or unwilling disclosure. Even data that is conventionally considered "less sensitive", such as favorite family members, friends, or teachers, can reveal patterns that inadvertently expose users' identities or correlate with sensitive information, creating subtle vulnerabilities. U.S. LLM chatbot users in this study were more willing to share these preference-based items than regulatory-defined personal data types like social security numbers or credit cards, reflecting a gap between lived privacy practices and formal PII definitions. Regulatory frameworks often focus on a narrow set of identifiers, overlooking the ways seemingly innocuous information can be aggregated or cross-referenced to infer identity, preferences, or behaviors. In the context of LLM chatbots, which can process and connect diverse data types in ways traditional web services cannot, this creates heightened exposure risk. We emphasize that it is important not to rely solely on legally defined PII. Privacy safeguards should also consider what users perceive as low-risk, extending protection to all forms of personal data, since even seemingly innocuous information can be used for profiling, identity inference, or other unintended purposes.

C. Consistent Privacy Concerns but High User Vulnerability

Consistent with prior research on traditional online privacy [75], [76], this study found that users aged 35–44 and 55+ reported lower perceived risk compared to younger users aged 18–24 when interacting with LLM chatbots. This age group may be slower to adopt new technologies [77], [78] and often has limited knowledge about technological risks [79], which can make them more vulnerable and less equipped to protect themselves from potential threats [80]. Despite this limited awareness, they still express privacy concerns regarding LLM chatbots, often framing these concerns in terms of traditional online privacy rather than recognizing the unique risks and harms posed by this emerging technology [61], [22], [23].

In addition, the study showed that LGBTQ+ users perceive lower risks than heterosexual users when interacting with LLM chatbots. Historically, LGBTQ+ individuals face unique vulnerabilities both online and offline, and are often driven to seek more privacy [81] due to societal stigmatization, discrimination, and identity-related risks [82], [83], [84], [85]. From a legal perspective, the overturning of Roe *v.* Wade [86] not only represents a regression in reproductive rights but also signals potential weakening of privacy protections related to personal identity and autonomy under the Fourteenth Amendment—protections that have historically supported landmark LGBTQ+ rulings such as Obergefell *v.* Hodges (same-sex marriage) [87] and Lawrence *v.* Texas (decriminalization of homosexuality) [88]. Although these legal developments might suggest heightened privacy risk for marginalized communities, our study found that LGBTQ+ participants reported lower perceived risk when using LLM chatbots. This apparent discrepancy may reflect increased familiarity with privacy practices, proactive privacy behaviors, or trust in technology-mediated interactions, highlighting the need to consider both structural legal context and individual user experiences when interpreting perceived privacy risk.

D. Usage Frequency and Confidence as Privacy Risk

This study is the first to demonstrate how these user attributes affect privacy perceptions and practices, highlighting the need for LLM chatbots to address diverse user vulnerabilities and informing future research on these critical issues. The quantitative findings indicate that U.S. LLM chatbot user privacy is strongly influenced by users' chatbot literacy, experience, and confidence. Lower familiarity or self-efficacy can reduce sensitivity to privacy risks, whereas frequent interaction and greater confidence enhance awareness and management of these concerns. Users with over three years of experience generally show stronger privacy awareness, and daily use is linked to greater comfort in handling the system.

E. Recommendations

Based on our findings, we offer actionable recommendations (1) to guide privacy-enhancing technologies for LLM chatbots and (2) to inform related policy and governance frameworks.

1) Privacy Tech in LLM Chatbots: As our study underscored, ensuring user privacy in LLM-based chatbots requires a multi-layered approach that goes beyond traditional online privacy practices. Interaction-level privacy measures should incorporate context-aware and dynamic decision-making, allowing the system to adapt responses based on user behavior, session history, or the sensitivity of disclosed information.

We therefore recommend that privacy technology practitioners: (1) develop mechanisms that account for varying levels of user understanding and provide clear, actionable options for informed consent, recognizing that users may be uncertain, misinformed, or influenced by manipulative cues at any point before, during, and after LLM interactions, as risks can arise continuously; (2) implement privacy-sensitive, reward-based language models that can provide adaptive disclosure warnings or proactive redaction suggestions, reinforcing privacy-preserving behaviors by giving positive feedback or incentives when users share information safely; and (3) develop differentiated privacy-preserving technologies for LLMs—tailored to user culture-sensitive behavior and interaction context [89], [60]—that provide nuanced protection, such as dynamic masking, context-sensitive data retention, and time-sensitive intervention to mitigate leakage risks at all stages of user-LLM interactions, accounting for the continuous and evolving nature of potential threats.

2) Policy Governance Implications: Ensuring privacy in LLM chatbots requires adherence to a complex web of legal frameworks, including U.S. federal and state laws and international regulations such as the EU's GDPR and AI Act. In the U.S., developers also need to navigate a patchwork of state statutes such as CCPA/CPRA each with differing definitions of personal or sensitive data, consent requirements, and enforcement mechanisms. Adding to this complexity, as mentioned in §I, executive actions under recent administrations, such as deregulatory orders promoting AI adoption [31], create further uncertainty by shifting federal priorities and enforcement stances.

In the context of uncertain regulatory governance and compliance, our study also revealed that many U.S. end users of LLM chatbots demonstrate limited privacy literacy and awareness. While most of the regulations such as GDPR and CCPA emphasize transparency, notice, and consent, they largely assume that users can understand disclosures and meaningfully exercise available rights. Our results suggest that, in practice, users may struggle to interpret privacy policies or translate regulatory protections into effective control over their data. This gap between formal compliance and practical usability indicates that current regulatory approaches may be insufficient for supporting informed, user-centered privacy management in conversational systems.

While regulatory frameworks vary across jurisdictions, developers can further mitigate uncertainty by adopting a standardized governance approach aligned with the strictest common requirements and consensus on best practices. Such measures help maintain long-term protection, allowing LLM systems to safeguard user privacy even amid shifting laws and executive priorities. Policies for LLM chatbots should specifically move beyond static regulation-forced consent and implement adaptive privacy measures that respond to evolving user input and interaction context. Also, cognitive biases, cultural norms, and fairness to prevent privacy discriminatory outcomes are needs to be acknowledged in the LLM policies.

Thus, we recommend that organizational policy and governance strategies for LLM chatbots ensure consistent, proactive management of user privacy by including: (1) mandating the deployment of technical safeguards (specifically, this can be done by governing automated personal-data detection and removal, role-based access controls, and robust identity and access management practices) and requiring that these safeguards be integrated with user-centric interface elements that clearly communicate ethical user data-management rights at every point of interaction; (2) implementing tiered disclosure controls, contextual privacy nudges, and non-manipulative and clear consent or non-consent options in the user interface; and (3) establishing adaptive, time- and manipulation-sensitive policy mechanisms that provide transparent feedback on data usage and the potential consequences of information sharing for both end-users and the organization.

F. Limitations and Future Work

While our study offers valuable insights into users' privacy sensitivity, awareness, and comfort with LLM chatbots, it has several limitations. We did not differentiate between text-based, voice-based, or multimodal systems, nor among different chatbot vendors, which may involve distinct privacy challenges and user experiences. In addition, the survey instrument relied on participants' own interpretation of the chatbot term which may have varied across respondents depending on their prior experience and familiarity with different systems. Such variation in interpretation could have influenced how participants understood and responded to survey items, thereby affecting the consistency of the measurements. Our sample was geographically limited, and self-reported measures may be affected by recall bias, social desirability, or misunderstandings. In particular, survey items related to privacy control may capture participants' self-perceived sense of control rather than their actual privacy-related behaviors. Although the survey was carefully designed and pre-tested, some constructs, such as perceived privacy risk, may require further validation. Real-world interactions with LLM chatbots might yield different results, so participants' reported attitudes may not fully reflect actual behavior. Despite these limitations, this study contributes to understanding privacy sensitivity in LLM chatbot use and lays the groundwork for more inclusive, privacy-conscious chatbot design.

Future work could consider conducting studies with larger, more diverse samples, especially targeting groups that may have unique privacy concerns, such as children, older adults, or marginalized communities. Longitudinal studies are also recommended to understand how users' privacy concerns evolve as they gain more experience with LLM chatbot systems. Additionally, qualitative studies (e.g., interviews or ethnographies) could complement vignette-based survey approaches by providing richer insights into users' nuanced experiences and perceptions.

VI. Conclusion

Surveying 267 U.S. LLM chatbot users, we found generally low awareness of privacy policies, with slight differences by gender, usage frequency, and technical experience (**RQ1**), and moderate concerns about data handling, particularly among younger, less experienced, and frequent users (**RQ2**). Engagement with privacy settings was mixed, with frequent users more likely to adjust settings while demographics and experience had little effect (**RQ3**). Comfort with sharing personal data was generally low and influenced primarily by prior chatbot experience (**RQ4**), with participants cautious about highly sensitive information such as credit card numbers and social security numbers, but more willing to share less sensitive preference- or relationship-based data (**RQ5**). Ultimately, our findings highlight how experience and perceived risk shape privacy behavior, provide actionable guidance for designing privacy-aware LLM chatbots, and establish a baseline for future U.S.-focused and cross-cultural research.

Acknowledgment

We thank the anonymous reviewers for their insightful comments. This work is based on data extracted from part of the first author's (E.G.) doctoral thesis [90]. We are grateful for the thoughtful and constructive feedback provided at earlier stages of this work by Professors Howard Rosenbaum, Ronqian Ma, Devan Ray Donaldson, Xiaojing Liao, Madelyn Rose Sanfilippo, and Faye E. Jones. We also gratefully acknowledge Indiana University's Statistical Consulting Center for their help. This work was not supported by any funding, and the views and conclusions expressed herein are solely those of the authors and do not reflect the views of the University of Illinois Urbana-Champaign or Indiana University.

AI Acknowledgment

The authors acknowledge the use of AI-based tools, specifically GPT-5, for grammar refinement, language editing, and improving the clarity and readability of the text in this manuscript. All intellectual contributions, content development, and research findings presented in this paper remain the sole responsibility of the authors.

References

[1] E. Gumusel, "A literature review of user privacy concerns in conversational chatbots: A social informatics approach: An annual review of information science and technology (arist) paper," *Journal of the Association for Information Science and Technology*, vol. 76, no. 1, pp. 121–154, 2025.

[2] A. Leschanowsky, S. Rech, B. Popp, and T. Bäckström, "Evaluating privacy, security, and trust perceptions in conversational ai: A systematic review," *Computers in Human Behavior*, p. 108344, 2024.

[3] P. Kucherbaev, A. Bozzon, and G.-J. Houben, "Human-aided bots," *IEEE Internet Computing*, vol. 22, no. 6, p. 36–43, Nov. 2018.

[4] C. Ischen, T. Araujo, H. Voorveld, G. van Noort, and E. Smit, "Privacy concerns in chatbot interactions," in *Chatbot Research and Design*, ser. Lecture Notes in Computer Science, A. Følstad, T. Araujo, S. Papadopoulos, E. L.-C. Law, O.-C. Granmo, E. Luger, and P. B. Brandtzaeg, Eds. Cham: Springer International Publishing, 2020, p. 34–48.

[5] S. T. Völkel, R. Haeuslschmid, A. Werner, H. Hussmann, and A. Butz, "How to trick ai: Users' strategies for protecting themselves from automatic personality assessment," in *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. Honolulu HI USA: ACM, Apr. 2020, p. 1–15. [Online]. Available: https://dl.acm.org/doi/10.1145/3313831.3376877

[6] A. C. Griffin, Z. Xing, S. P. Mikles, S. Bailey, S. Khairat, J. Arguello, Y. Wang, and A. E. Chung, "Information needs and perceptions of chatbots for hypertension medication self-management: a mixed methods study," *JAMIA Open*, vol. 4, no. 2, p. ooab021, Apr. 2021.

[7] A. Leschanowsky, B. Popp, and N. Peters, "Privacy strategies for conversational ai and their influence on users' perceptions and decision-making," in *Proceedings of the 2023 European Symposium on Usable Security*, 2023, pp. 296–311.

[8] S. Cao and C.-M. Huang, "Understanding user reliance on ai in assisted decision-making," *Proceedings of the ACM on Human-Computer Interaction*, vol. 6, no. CSCW2, pp. 1–23, 2022.

[9] R. Staab, M. Vero, M. Balunović, and M. Vechev, "Beyond memorization: Violating privacy via inference with large language models," no. arXiv:2310.07298, May 2024, arXiv:2310.07298 [cs]. [Online]. Available: http://arxiv.org/abs/2310.07298

[10] M. Tong, K. Chen, J. Zhang, Y. Qi, W. Zhang, N. Yu, T. Zhang, and Z. Zhang, "Inferdpt: Privacy-preserving inference for black-box large language models," *IEEE Transactions on Dependable and Secure Computing*, 2025.

[11] N. Lukas, A. Salem, R. Sim, S. Tople, L. Wutschitz, and S. Zanella-Béguelin, "Analyzing leakage of personally identifiable information in language models," 2023. [Online]. Available: https://arxiv.org/abs/2302.00539

[12] S. Zanella-Béguelin, L. Wutschitz, S. Tople, V. Rühle, A. Paverd, O. Ohrimenko, B. Köpf, and M. Brockschmidt, "Analyzing information leakage of updates to natural language models," in *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '20. New York, NY, USA: Association for Computing Machinery, 2020, p. 363–375.

[13] A. Jagannatha, B. P. S. Rawat, and H. Yu, "Membership inference attack susceptibility of clinical language models," 2021. [Online]. Available: https://arxiv.org/abs/2104.08305

[14] N. Carlini, F. Tramèr, E. Wallace, M. Jagielski, A. Herbert-Voss, K. Lee, A. Roberts, T. Brown, D. Song, Erlingsson, A. Oprea, and C. Raffel, "Extracting training data from large language models," 2021, p. 2633–2650. [Online]. Available: https://www.usenix.org/conference/usenixsecurity21/presentation/carlini-extracting

[15] F. Mireshghallah, K. Goyal, A. Uniyal, T. Berg-Kirkpatrick, and R. Shokri, "Quantifying privacy risks of masked language models using membership inference attacks," *arXiv preprint arXiv:2203.03929*, 2022.

[16] J. Huang, H. Shao, and K. C.-C. Chang, "Are large pre-trained language models leaking your personal information?" in *Findings of the Association for Computational Linguistics: EMNLP 2022*, Y. Goldberg, Z. Kozareva, and Y. Zhang, Eds. Abu Dhabi, United Arab Emirates: Association for Computational Linguistics, Dec. 2022, p. 2038–2047. [Online]. Available: https://aclanthology.org/2022.findings-emnlp.148/

[17] K. Nakka, A. Frikha, R. Mendes, X. Jiang, and X. Zhou, "Pii-compass: Guiding llm training data extraction prompts towards the target pii via grounding," in *Proceedings of the Fifth Workshop on Privacy in Natural Language Processing*, I. Habernal, S. Ghanavati, A. Ravichander, V. Jain, P. Thaine, T. Igamberdiev, N. Mireshghallah, and O. Feyisetan, Eds. Bangkok, Thailand: Association for Computational Linguistics, Aug. 2024, p. 63–73. [Online]. Available: https://aclanthology.org/2024.privatenlp-1.7/

[18] Y. M. Pa Pa, S. Tanizaki, T. Kou, M. Van Eeten, K. Yoshioka, and T. Matsumoto, "An attacker's dream? exploring the capabilities of chatgpt for developing malware," in *Proceedings of the 16th cyber security experimentation and test workshop*, 2023, pp. 10–18.

[19] A. Monje, A. Monje, R. A. Hallman, and G. Cybenko, "Being a bad influence on the kids: Malware generation in less than five minutes using chatgpt," *Publisher: Unpublished*, 2023.

[20] F. He, T. Zhu, D. Ye, B. Liu, W. Zhou, and P. S. Yu, "The emerged security and privacy of llm agent: A survey with case studies," no. arXiv:2407.19354, Jul. 2024, arXiv:2407.19354 [cs]. [Online]. Available: http://arxiv.org/abs/2407.19354

[21] J. Chen, X. Wang, R. Xu, S. Yuan, Y. Zhang, W. Shi, J. Xie, S. Li, R. Yang, T. Zhu, A. Chen, N. Li, L. Chen, C. Hu, S. Wu, S. Ren, Z. Fu, and Y. Xiao, "From persona to personalization: A survey on role-playing

language agents,” no. arXiv:2404.18231, Oct. 2024, arXiv:2404.18231 [cs]. [Online]. Available: http://arxiv.org/abs/2404.18231

[22] Z. Zhang, M. Jia, H.-P. Lee, B. Yao, S. Das, A. Lerner, D. Wang, and T. Li, ““it’s a fair game”, or is it? examining how users navigate disclosure risks and benefits when using llm-based conversational agents,” in *Proceedings of the CHI Conference on Human Factors in Computing Systems*, 2024, pp. 1–26.

[23] E. Gumusel, K. Z. Zhou, and M. R. Sanfilippo, “User privacy harms and risks in conversational ai: A proposed framework,” *arXiv preprint arXiv:2402.09716*, 2024.

[24] H.-P. H. Lee, Y.-J. Yang, T. S. Von Davier, J. Forlizzi, and S. Das, “Deepfakes, phrenology, surveillance, and more! a taxonomy of ai privacy risks,” in *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*, ser. CHI ’24. New York, NY, USA: Association for Computing Machinery, 2024. [Online]. Available: https://doi.org/10.1145/3613904.3642116

[25] M. Ali, A. Arunasalam, and H. Farrukh, “Understanding users’ security and privacy concerns and attitudes towards conversational ai platforms,” no. arXiv:2504.06552, Apr. 2025, arXiv:2504.06552 [cs]. [Online]. Available: http://arxiv.org/abs/2504.06552

[26] L. M. Malki, A. Polamarasetty, M. Hatamian, E. Costanza, and M. Warner, ““hoovered up as a data point”: Exploring privacy behaviours, awareness, and concerns among uk users of llm-based conversational agents,” in *Proceedings on Privacy Enhancing Technologies*. ACM, 2025.

[27] S. Tran, H. Lu, I. Slaughter, B. Herman, A. Dangol, Y. Fu, L. Chen, B. Gebreyohannes, B. Howe, A. Hiniker *et al.*, “Understanding privacy norms around llm-based chatbots: A contextual integrity perspective,” *arXiv preprint arXiv:2508.06760*, 2025.

[28] Y. Shanmugarasa, S. Pan, M. Ding, D. Zhao, and T. Rakotoarivelo, “Privacy meets explainability: Managing confidential data and transparency policies in llm-empowered science,” in *Proceedings of the Extended Abstracts of the CHI Conference on Human Factors in Computing Systems*, 2025, pp. 1–8.

[29] EU, “General Data Protection Regulation (EU) 2016/679,” *Official Journal of the European Union*, 2016.

[30] European Union, “Regulation (eu) 2024/1689 of the european parliament and of the council of 12 july 2024 on artificial intelligence,” 2024, accessed: 2025-08-31. [Online]. Available: https://data.europa.eu/eli/reg/2024/1689/oj

[31] T. W. House, “Executive order 14179: Removing barriers to american leadership in artificial intelligence,” 2025, accessed: 2025-08-31. [Online]. Available: https://www.whitehouse.gov/presidential-actions/2025/01/removing-barriers-to-american-leadership-in-artificial-intelligence/

[32] National Conference of State Legislatures, “Artificial intelligence 2025 legislation,” 2025, accessed: 2025-08-31. [Online]. Available: https://www.ncsl.org/technology-and-communication/artificial-intelligence-2025-legislation

[33] T. Zukowski and I. Brown, “Examining the influence of demographic factors on internet users’ information privacy concerns,” in *Proceedings of the 2007 annual research conference of the South African institute of computer scientists and information technologists on IT research in developing countries*, 2007, pp. 197–204.

[34] J. L. Dupree, R. Devries, D. M. Berry, and E. Lank, “Privacy personas: Clustering users via attitudes and behaviors toward security practices,” in *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, 2016, pp. 5228–5239.

[35] P. E. Naeini, S. Bhagavatula, H. Habib, M. Degeling, L. Bauer, L. F. Cranor, and N. Sadeh, “Privacy expectations and preferences in an {IoT} world,” in *Thirteenth symposium on usable privacy and security (SOUPS 2017)*, 2017, pp. 399–412.

[36] V. Rathod, S. Nabavirazavi, S. Zad, and S. S. Iyengar, “Privacy and security challenges in large language models,” in *2025 IEEE 15th Annual Computing and Communication Workshop and Conference (CCWC)*. IEEE, 2025, pp. 00 746–00 752.

[37] B. C. Das, M. H. Amini, and Y. Wu, “Security and privacy challenges of large language models: A survey,” *ACM Computing Surveys*, vol. 57, no. 6, pp. 1–39, 2025.

[38] V. Rathod, S. Nabavirazavi, S. Zad, and S. S. Iyengar, “Privacy and security challenges in large language models,” in *2025 IEEE 15th Annual Computing and Communication Workshop and Conference (CCWC)*, Jan. 2025, p. 00746–00752. [Online]. Available: https://ieeexplore.ieee.org/document/10903912/?arnumber=10903912

[39] M. Mozes, X. He, B. Kleinberg, and L. D. Griffin, “Use of llms for illicit purposes: Threats, prevention measures, and vulnerabilities,” no. arXiv:2308.12833, Aug. 2023, arXiv:2308.12833 [cs]. [Online]. Available: http://arxiv.org/abs/2308.12833

[40] A. Kumar, S. Singh, S. V. Murty, and S. Ragupathy, “The ethics of interaction: Mitigating security threats in llms,” no. arXiv:2401.12273, Jan. 2024, arXiv:2401.12273 [cs]. [Online]. Available: http://arxiv.org/abs/2401.12273

[41] Y. Yao, J. Duan, K. Xu, Y. Cai, Z. Sun, and Y. Zhang, “A survey on large language model (llm) security and privacy: The good, the bad, and the ugly,” *High-Confidence Computing*, vol. 4, no. 2, p. 100211, Jun. 2024.

[42] N. Carlini, F. Tramèr, E. Wallace, M. Jagielski, A. Herbert-Voss, K. Lee, A. Roberts, T. Brown, D. Song, Erlingsson, A. Oprea, and C. Raffel, “Extracting training data from large language models,” 2021, p. 2633–2650. [Online]. Available: https://www.usenix.org/conference/usenixsecurity21/presentation/carlini-extracting

[43] P. V. Falade, “Decoding the threat landscape: Chatgpt, fraudgpt, and wormgpt in social engineering attacks,” *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, p. 185–198, Oct. 2023. [Online]. Available: http://dx.doi.org/10.32628/CSEIT2390533

[44] A. Urman and M. Makhortykh, “The silence of the llms: Cross-lingual analysis of political bias and false information prevalence in chatgpt, google bard, and bing chat,” 2023.

[45] S. Dai, Y. Zhou, L. Pang, W. Liu, X. Hu, Y. Liu, X. Zhang, G. Wang, and J. Xu, “Neural retrievers are biased towards llm-generated content,” in *Proceedings of the 30th ACM SIGKDD Conference on Knowledge Discovery and Data Mining*, ser. KDD ’24. ACM, Aug. 2024, p. 526–537. [Online]. Available: http://dx.doi.org/10.1145/3637528.3671882

[46] D. Huang, J. M. Zhang, Q. Bu, X. Xie, J. Chen, and H. Cui, “Bias testing and mitigation in llm-based code generation,” 2025. [Online]. Available: https://arxiv.org/abs/2309.14345

[47] A. Wan, E. Wallace, S. Shen, and D. Klein, “Poisoning language models during instruction tuning,” 2023. [Online]. Available: https://arxiv.org/abs/2305.00944

[48] H. Yao, J. Lou, and Z. Qin, “Poisonprompt: Backdoor attack on prompt-based large language models,” 2023. [Online]. Available: https://arxiv.org/abs/2310.12439

[49] S. Meisenbacher, A. Klymenko, and F. Matthes, “Llm-as-a-judge for privacy evaluation? exploring the alignment of human and llm perceptions of privacy in textual data,” in *Proceedings of the 2025 Workshop on Human-Centered AI Privacy and Security*, 2025, pp. 126–138.

[50] J. Wang, J. Yang, H. Li, H. Zhuang, C. Chen, and Z. Zeng, “Rewardds: Privacy-preserving fine-tuning for large language models via reward driven data synthesis,” 2025. [Online]. Available: https://arxiv.org/abs/2502.18517

[51] F. Wu, N. Zhang, S. Jha, P. McDaniel, and C. Xiao, “A new era in llm security: Exploring security concerns in real-world llm-based systems,” no. arXiv:2402.18649, Feb. 2024, arXiv:2402.18649 [cs]. [Online]. Available: http://arxiv.org/abs/2402.18649

[52] B. Hui, H. Yuan, N. Gong, P. Burlina, and Y. Cao, “Pleak: Prompt leaking attacks against large language model applications,” in *Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security*. Salt Lake City UT USA: ACM, Dec. 2024, p. 3600–3614. [Online]. Available: https://dl.acm.org/doi/10.1145/3658644.3670370

[53] T. Su, B. Zhang, C. Zhang, and L. Wei, “Privacy leak detection in llm interactions with a user-centric approach,” in *2024 IEEE 23rd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*. IEEE, 2024, pp. 1647–1652.

[54] S. Sannon, B. Stoll, D. DiFranzo, M. F. Jung, and N. N. Bazarova, ““i just shared your responses”: Extending communication privacy management theory to interactions with conversational agents,” *Proceedings of the ACM on Human-Computer Interaction*, vol. 4, no. GROUP, p. 1–18, Jan. 2020.

[55] A. Agnihotri and S. Bhattacharya, “Chatbots’ effectiveness in service recovery,” *International Journal of Information Management*, p. 102679, Jul. 2023.

[56] M. Bouhia, L. Rajaobelina, S. PromTep, M. Arcand, and L. Ricard, “Drivers of privacy concerns when interacting with a chatbot in a customer service encounter,” *International Journal of Bank Marketing*, vol. 40, no. 6, pp. 1159–1181, Jan. 2022, publisher:

Emerald Publishing Limited. [Online]. Available: https://doi.org/10.1108/IJBM-09-2021-0442

[57] G. Pizzi, V. Vannucci, V. Mazzoli, and R. Donvito, "I, chatbot! the impact of anthropomorphism and gaze direction on willingness to disclose personal information and behavioral intentions," *Psychology Marketing*, vol. 40, no. 7, p. 1372–1387, 2023.

[58] R. Belen-Saglam, J. R. C. Nurse, and D. Hodges, "An investigation into the sensitivity of personal information and implications for disclosure: A uk perspective," *Frontiers in Computer Science*, vol. 4, Jun. 2022. [Online]. Available: https://www.frontiersin.org/articles/10.3389/fcomp.2022.908245

[59] J. Kwesi, J. Cao, R. Manchanda, and P. Emami-Naeini, "Exploring user security and privacy attitudes and concerns toward the use of {General-Purpose}{LLM} chatbots for mental health," in *34th USENIX Security Symposium (USENIX Security 25)*, 2025, pp. 6007–6024.

[60] Z. Liu, L. Hu, T. Zhou, Y. Tang, and Z. Cai, "Prevalence overshadows concerns? understanding chinese users' privacy awareness and expectations towards llm-based healthcare consultation," in *2025 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2025, pp. 2716–2734.

[61] X. Zhan, J. C. Carrillo, W. Seymour, and J. Such, "Malicious llm-based conversational ai makes users reveal personal information," *arXiv preprint arXiv:2506.11680*, 2025.

[62] C. N. Harrington and L. Egede, "Trust, comfort and relatability: Understanding black older adults' perceptions of chatbot design for health information seeking," in *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, 2023, pp. 1–18.

[63] A. M. McDonald and L. F. Cranor, "The Cost of Reading Privacy Policies," *A Journal of Law and Policy for the Information Society*, vol. 4, p. 543, 2008. [Online]. Available: https://kb.osu.edu/handle/1811/72839

[64] A. Westin and H. L. . Associates, "Harris-equifax consumer privacy survey," Equifax Inc., Tech. Rep., 1991, conducted for Equifax Inc. 1,255 adults of the U.S. public.

[65] J. Colnago, L. Cranor, and A. Acquisti, "Is there a reverse privacy paradox? an exploratory analysis of gaps between privacy perspectives and privacy-seeking behaviors," *Proceedings on Privacy Enhancing Technologies*, vol. 2023, no. 1, p. 455–476, Jan. 2023.

[66] C. S. Assembly, "California Consumer Privacy Act (CCPA)," 2018.

[67] A. M. McDonald and L. F. Cranor, "Americans' attitudes about internet behavioral advertising practices," in *Proceedings of the 9th annual ACM workshop on Privacy in the electronic society*, 2010, pp. 63–72.

[68] V. Braun and V. Clarke, *Thematic analysis*, ser. APA handbooks in psychology®. Washington, DC, US: American Psychological Association, 2012, p. 57–71.

[69] S. Pötzsch, "Privacy awareness: A means to solve the privacy paradox?" in *The Future of Identity in the Information Society*, ser. IFIP Advances in Information and Communication Technology, V. Matyáš, S. Fischer-Hübner, D. Cvrček, and P. Švenda, Eds. Berlin, Heidelberg: Springer, 2009, p. 226–236.

[70] D. F. Spake, R. Zachary Finney, and M. Joseph, "Experience, comfort, and privacy concerns: antecedents of online spending," *Journal of Research in Interactive Marketing*, vol. 5, no. 1, p. 5–28, Jan. 2011.

[71] S. Kokolakis, "Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon," *Comput. Secur.*, 2017.

[72] A. Acquisti and J. Grossklags, "Privacy and rationality in individual decision making," *IEEE security & privacy*, vol. 3, no. 1, pp. 26–33, 2005.

[73] S. Barth and M. D. De Jong, "The privacy paradox–investigating discrepancies between expressed privacy concerns and actual online behavior–a systematic literature review," *Telematics and informatics*, vol. 34, no. 7, pp. 1038–1058, 2017.

[74] A. Acquisti, C. Taylor, and L. Wagman, "The economics of privacy," *Journal of Economic Literature*, vol. 54, no. 2, p. 442–492, Jun. 2016.

[75] D. Hornung, C. Müller, I. Shklovski, T. Jakobi, and V. Wulf, "Navigating relationships and boundaries: Concerns around ict-uptake for elderly people," in *Proceedings of the 2017 CHI conference on human factors in computing systems*, 2017, pp. 7057–7069.

[76] A. Frik, L. Nurgalieva, J. Bernd, J. Lee, F. Schaub, and S. Egelman, "Privacy and security threat models and mitigation strategies of older adults," in *Fifteenth symposium on usable privacy and security (SOUPS 2019)*, 2019, pp. 21–40.

[77] L. Gitlow, "Technology use by older adults and barriers to using technology," *Physical & Occupational Therapy in Geriatrics*, vol. 32, no. 3, pp. 271–280, 2014.

[78] K. G. Vroman, S. Arthanat, and C. Lysack, ""who over 65 is online?" older adults' dispositions toward information communication technology," *Computers in Human Behavior*, vol. 43, pp. 156–166, 2015.

[79] N. Charness and W. R. Boot, "Aging and information technology use: Potential and barriers," *Current directions in psychological science*, vol. 18, no. 5, pp. 253–258, 2009.

[80] H. Tamut and I. K. Dutta, "Understanding and mitigating social engineering attacks to elderly people: A comprehensive survey of methods, impacts, and future solutions," in *2024 IEEE 15th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*. IEEE, 2024, pp. 0461–0470.

[81] C. Geeng, M. Harris, E. Redmiles, and F. Roesner, ""like lesbians walking the perimeter": Experiences of U.S. LGBTQ+ folks with online security, safety, and privacy advice," 2022, p. 305–322. [Online]. Available: https://www.usenix.org/conference/usenixsecurity22/presentation/geeng

[82] H. R. Bregman, N. M. Malik, M. J. L. Page, E. Makynen, and K. M. Lindahl, "Identity profiles in lesbian, gay, and bisexual youth: The role of family influences," *Journal of Youth and Adolescence*, vol. 42, no. 3, p. 417–430, Mar. 2013.

[83] B. Mehra and D. Braquet, "A "queer" manifesto of interventions for libraries to "come out" of the closet! a study of "queer" youth experiences during the coming out process," 2006, accepted: 2021-09-06T02:04:07Z. [Online]. Available: https://dr.ntu.edu.sg/handle/10356/152619

[84] E. M. Saewyc, "Research on adolescent sexual orientation: Development, health disparities, stigma, and resilience," *Journal of Research on Adolescence*, vol. 21, no. 1, p. 256–272, 2011.

[85] D. G. Campbell and S. R. Cowan, "The paradox of privacy: Revisiting a core library value in an age of big data and linked data," *Library Trends*, vol. 64, no. 3, p. 492–511, 2016.

[86] "Roe v. Wade," 410 U.S. 113, 1973.

[87] "Obergefell v. Hodges," 576 U.S. 644, 2015.

[88] "Lawrence v. Texas," 539 U.S. 558, 2003.

[89] H. Nissenbaum, "Privacy in context: Technology, policy, and the integrity of social life," in *Privacy in context*. Stanford University Press, 2009.

[90] E. Gumusel, "User privacy dynamics in conversational text-based ai chatbots: Understanding harms, risks, and strategies for mitigation," Ph.D. dissertation, Indiana University, proQuest Dissertations & Theses, Order No. 31938996. [Online]. Available: https://www.proquest.com/docview/31938996

A. Appendix

A. Recruitment Letter

Dear all,

We are writing to invite you to participate in our survey. You are eligible to participate in our study if you are

- 18 years of age or older,
- currently reside in the United States, and
- have prior experience with an LLM chatbot.

Your contribution is critical to our research. Completing the survey will take approximately 10 minutes, and you can access it via the following link: [Survey Link]

Compensation: There will be no compensation.

Participating in research is voluntary. This research has been approved by Indiana University Bloomington IRB: #22235.

Contact Information: For questions about this study, contact Indiana University Bloomington.

Thank you so much for your support and cooperation.

B. Survey Questionnaire

Informed Consent Statement. Thank you so much for your interest in participating in this study. In this survey, you are being asked to participate in a research study. This survey is voluntary and confidential, and you may withdraw your participation at any time by exiting the survey. You are being asked to participate in a research study focused on user privacy concerns in LLM chatbot systems. These systems are computer programs designed to engage in natural language conversations with users through written or typed messages. Their primary objective is to establish conversations with users, prioritizing engagement over specialized task assistance. There will be no connection to you personally in the analysis of survey data or future publications based on this research. Your participation in this research study involves completing a short questionnaire regarding your prior experience and interactions with these systems. More details are provided in the next section. You may participate in this study if you are aged 18 or older, live in the United States, are proficient in English, and have prior experience with a LLM chatbot system. If you decide to participate in this study, a reasonably foreseeable risk or discomfort involves the potential breach of confidentiality and privacy. Upon successful completion, you will be directed to a page where you can choose whether to take part in the subsequent study. There, you can enter your email address and indicate your interest in participating in the next phase of the study.

DETAILED INFORMATION ABOUT THIS RESEARCH STUDY: In addition to the above information, the following paragraphs offer more detailed information about this study.

PURPOSE OF THE STUDY: The purpose of this study is to explore the privacy issues and challenges that users face when interacting with LLM chatbot systems. The study also evaluates how personas of LLM chatbot influence users' perceptions and decision-making regarding privacy and security.

TIME COMMITMENT: Participation in this study is expected to last approximately 15 minutes, depending on the depth of your responses.

STUDY PROCEDURES: The survey will consist of questions about your prior experience with LLM chatbot systems. The survey will also ask you to report your gender, sexual orientation, education level, age, race, income level, and political affiliation, as well as potentially other similar demographic information.

POSSIBLE BENEFITS: While there are no direct benefits to the participants in this study, results may help practitioners and researchers better understand user privacy harms and risks in LLM chatbot and develop mitigation strategies.

POSSIBLE RISKS/DISCOMFORTS: Participation in this online survey involves risks to confidentiality similar to a person's everyday use of the internet, including potential breaches of confidentiality. Study data will be physically and electronically secured by the research team. Despite safeguards, the use of electronic data storage entails some risk of data security breach. You have the right to withdraw from any study procedures at any time without penalty. If you experience excessive discomfort, you may stop participating at any time without penalty. While the researchers will try to prevent any problems, unforeseeable risks may exist.

COMPENSATION: There will be no compensation.

CONFIDENTIALITY: Efforts will be made to keep your personal information private. All electronic data collected will be stored on secure platforms protected by two-factor authentication and accessible only by the researchers. Data will be stored for at least three (3) years after the study. Results may be published or presented without identifying you. Data may be used for future research not described here. Absolute confidentiality cannot be guaranteed, but every effort will be made to protect your information as permitted by law. Your personal information may be shared outside this study if required by law or for quality assurance, including with institutional review boards or state/federal agencies as allowed. This research uses Qualtrics software, subject to Qualtrics' privacy policies: https://www.qualtrics.com/privacy-statement/.

CONTACT INFORMATION FOR QUESTIONS ABOUT THE STUDY: For questions about the study, contact co-PI Indiana University Bloomington. Questions about your rights or complaints may be directed to Indiana University Bloomington Institutional Review Boards at Indiana University Bloomington.

Please select your choice below. Clicking on the "Agree" button indicates that you:

- have read the above information,
- voluntarily agree to participate, and
- are 18 years of age or older.

Agree Do Not Agree

Skip to End of Survey if answer is Do Not Agree.

LLM chatbots[5] *are computer programs designed to engage in natural language conversations with users through written or typed messages. Their primary objective is to establish conversations with users, prioritizing engagement over specialized task assistance.*

According to the above definition, have you had an experience interacting with a LLM chatbot?

□ Yes

□ No

Skip to End of Survey if answer is No.

How well can you speak and understand English?

□ I am a native speaker of English

□ I am proficient in spoken and written English in an academic context or at work

□ I am comfortable with everyday conversations in English

□ I can speak and manage simple conversations in English

□ Not well

Skip to End of Survey if answer is "I can speak and manage simple conversations in English" or "Not well".

Do you live in the United States?

[5] In the survey, this term was presented to participants as "conversational text-based AI chatbots" to assess their perceived understanding throughout the survey.

☐ Yes
☐ No
Skip to End of Survey if answer is No.

What gender do you identify as?
☐ Female
☐ Male
☐ Transgender Female
☐ Transgender Male
☐ Non-binary
☐ Agender
☐ Gender-fluid
☐ Other (please specify):

How do you describe your sexual orientation?
☐ Heterosexual or straight
☐ Gay, lesbian, or homosexual
☐ Bisexual
☐ Pansexual
☐ Demisexual
☐ Asexual
☐ Queer
☐ Other (please specify):

What is the highest degree or level of school you have completed?
☐ Less than a high school diploma
☐ High school or equivalent
☐ Some college
☐ Associate's degree
☐ Bachelor's degree
☐ Master's degree
☐ Professional degree or doctoral degree
☐ Other (please specify):

What is your age?
☐ 18–24
☐ 25–34
☐ 35–44
☐ 45–54
☐ 55–64
☐ 65+

How long have you been using LLM chatbot?
☐ Less than 6 months
☐ 6 months to 1 year
☐ 1 to 3 years
☐ More than 3 years
☐ Never used
Skip to End of Survey if answer is Never used.

To what extent do you feel confident in your technical skill-set when interacting with LLM chatbot?
☐ Not confident at all
☐ Slightly confident
☐ Moderately confident
☐ Very confident
☐ Extremely confident

How frequently do you interact with LLM chatbot?
☐ Multiple times a day
☐ Once a day
☐ A few times a week
☐ A few times a month
☐ Rarely
☐ Never

To what extent do you agree or disagree with the following statements?
(1) Strongly disagree, (2) Disagree, (3) Neutral, (4) Agree, (5) Strongly agree

I feel well-informed about privacy measures and data handling practices of LLM chatbots before starting to use it.
☐ ☐ ☐ ☐ ☐

I review the privacy policy or terms of service provided by LLM chatbots.
☐ ☐ ☐ ☐ ☐

I am concerned about the potential privacy risks associated with interacting with LLM chatbots.
☐ ☐ ☐ ☐ ☐

I am confident that my personal data is handled securely and responsibly by LLM chatbots after our interaction.
☐ ☐ ☐ ☐ ☐

LLM chatbots always explain how they use and store the information I provide during the conversation.
☐ ☐ ☐ ☐ ☐

LLM chatbots respect my privacy by not asking for unnecessary personal information during the interaction.
☐ ☐ ☐ ☐ ☐

LLM chatbots demonstrate a commitment to safeguarding my privacy after the interaction has ended.
☐ ☐ ☐ ☐ ☐

LLM chatbots successfully balance user experience with privacy considerations throughout the entire interaction process.
☐ ☐ ☐ ☐ ☐

How likely are you to review or adjust your privacy settings related to a LLM chatbot after concluding the conversation?
☐ Very likely
☐ Likely
☐ Neutral
☐ Unlikely
☐ Very unlikely

How comfortable are you with sharing personal information with LLM chatbot?
☐ Very uncomfortable
☐ Somewhat uncomfortable
☐ Neutral
☐ Somewhat comfortable
☐ Very comfortable

Which of the following types of personal information are you most hesitant to share with LLM chatbots? (Select all that apply)

☐ Social security number
☐ Credit card number
☐ Phone number
☐ Income
☐ Medical information
☐ Postal address
☐ Full name
☐ Computer information (e.g., device ID, IP address, password)
☐ Age
☐ Email address
☐ Gender
☐ Sexual orientation
☐ Education
☐ Political affiliation
☐ Religion
☐ Race
☐ Social media profiles
☐ None of them
☐ Other (please specify):

Which of the following types of personal information are you most hesitant to share with LLM chatbots? (Select all that apply)

☐ Favorite snack
☐ Favorite TV show
☐ Favorite movie
☐ Favorite pet
☐ Favorite sport
☐ Favorite brand
☐ Favorite restaurant
☐ Favorite city
☐ Favorite artist
☐ Favorite friend
☐ Favorite family member
☐ Favorite teacher
☐ None of them
☐ Other (please specify):

Thank you for your participation!