International Journal of Advanced Mass Communication and Journalism

E-ISSN: 2708-4469
P-ISSN: 2708-4450
IJAMCJ 2025; 6(2): 26-29
© 2025 IJAMCJ
www.masscomjournal.com
Received: 09-05-2025
Accepted: 12-06-2025

Rachel Anthony
Student, High School-2025 Batch, Bhatnagar International School, Vasant Kunj, New Delhi, Delhi, India

Mishelle Anthony
Senior Executive, Digital Marketing Team, Utkarsh Surgical Center, Gurugram, Haryana, India

Corresponding Author:
Rachel Anthony
Student, High School-2025 Batch, Bhatnagar International School, Vasant Kunj, New Delhi, Delhi, India

AI privacy and the right to be forgotten: A survey-based analysis of user perceptions

Rachel Anthony and Mishelle Anthony

DOI: https://www.doi.org/10.22271/27084450.2025.v6.i2a.117

Abstract
This paper presents an analysis of user perceptions regarding data privacy in Artificial Intelligence (AI) systems, with a specific focus on the "right to be forgotten". Drawing from a survey of 30 participants, the study reveals an overwhelming demand for enhanced user control over personal data within AI, particularly the ability to view and delete data history. Key findings indicate that "loss of privacy" and "misuse of personal information" are primary concerns, significantly influencing user trust. Despite high awareness of AI data practices, engagement with privacy policies remains low, highlighting an "awareness-action gap". Furthermore, while there is strong support for mandatory "right to be forgotten" features, opinions are divided on their technical feasibility. These insights underscore the critical need for transparent data governance, user-centric privacy design, and robust technical solutions to foster trust and ensure ethical AI development.

Keywords: AI development, Artificial Intelligence, loss of privacy, misuse of personal information

1. Introduction

The pervasive integration of Artificial Intelligence (AI) into daily life has brought forth unprecedented technological advancements, yet it simultaneously presents complex challenges to established notions of digital privacy. AI's inherent reliance on vast datasets for training and continuous learning necessitates a re-evaluation of traditional data retention practices and privacy frameworks. Globally, the discourse surrounding individual data rights, epitomized by regulations such as the General Data Protection Regulation (GDPR) [2], has intensified, with AI's unique data demands adding novel dimensions to these critical discussions. This research aims to explore public perceptions, awareness, concerns, and preferences concerning AI data retention and the evolving concept of "digital forgetting". Specifically, it investigates user perspectives on how AI systems should manage and retain personal data, emphasizing the desire for control and the implications of persistent memory. The insights derived from this study are intended to inform AI developers, policymakers, and privacy advocates, guiding the development and deployment of AI technologies towards more ethical and user-centric principles.

The subsequent sections detail the methodology employed, present the key findings from the survey, discuss their implications for AI privacy and trust, and conclude with strategic recommendations for fostering a more trustworthy AI ecosystem.

2. Methodology

This study employed a quantitative and qualitative survey approach to gather insights into user perceptions of AI data privacy. An online questionnaire was administered, comprising a mix of multiple-choice questions for quantitative data collection and open-ended prompts to capture qualitative feedback.

2.1 Participants

A total of 30 unique responses were collected. The respondent pool exhibited a strong representation from younger demographics, with approximately 56.7% (17 out of 30) falling within the 18-25 age group.

Other age brackets included 25-34 (3 respondents), 35-44 (4 respondents), under 18 (4 respondents), and 45-54 (2 respondents). Participants represented diverse fields of study and work, including Economics, Healthcare, Business, Computer Science, Engineering, and Design.

2.2 Data Collection

The survey questions focused on several key areas:

- **Demographics and AI Engagement:** Age, field of study/work, familiarity with AI, AI usage frequency, and common AI use cases.
- **Awareness of AI Data Practices:** Knowledge regarding AI data storage for training and third-party access to AI data.
- **Engagement with Privacy Policies:** Frequency of reading privacy policies for AI tools and third-party data usage.
- **"Right to be forgotten":** Belief in the right to request data deletion, support for mandatory implementation, and perceived technical feasibility.
- **Concerns Regarding AI Data Retention:** Identification of top concerns (e.g., loss of privacy, data breaches).
- **Data Prioritization:** Types of information prioritized for deletion and comfort levels with providing specific data types.
- **Trust in AI Systems:** Impact of transparent data control on user trust.

Data was collected anonymously, and responses were analyzed to identify trends, patterns, and key themes.

3. Results

3.1 Respondent Demographics and AI Engagement

The survey participants were predominantly young, digitally native individuals (56.7% aged 18-25). A significant majority reported high familiarity with AI, with 53.3% being "Very familiar" and 33.3% "Somewhat familiar." AI usage frequency was also high, with 40% using AI "More than once a day" and 20% "Once a day." Top use cases included "Educational purposes" (60%), "Daily life (Planning, advice, ideas)" (53.3%), and "Research purposes" (50%). Despite high familiarity and frequent use, reliance on AI was more varied, with "Average" being the most common response (12 respondents).

Table 1: Respondent Demographics and AI usage overview

Characteristic	Category	Count	Percentage
Age Group	18-25	17	56.7%
	25-34	3	10.0%
	35-44	4	13.3%
	Under 18	4	13.3%
	45-54	2	6.7%
AI Familiarity	Very familiar	16	53.3%
	Somewhat familiar	10	33.3%
	Expert user	1	3.3%
	Slightly familiar	3	10%
AI Usage Frequency	More than once a day	12	40.0%
	Once a day	6	20%
	More than once a week	7	23.3%
	Lesser than once a week	3	10.0%
	Once a week	2	6.7%
Top AI Use Cases (Multiple Answers allowed)	Educational purposes	18	60%
	Daily life (Planning, advice, ideas)	16	53.3%
	Research purposes	15	50%
	Professional purposes	9	30%
	Entertainment purposes	7	23.3%

3.2 Awareness and Engagement with AI Data Practices

A significant majority of respondents (26 out of 30) were aware that AI platforms store user data for model training. Awareness regarding third-party access to AI data was also substantial (17 out of 30 respondents). However, engagement with privacy policies was notably low: only 3 respondents claimed to "read every line" of AI tool privacy policies, and 12 "never" read policies for third parties using AI data.

3.3 The "Right to be forgotten"

An overwhelming 26 out of 30 respondents believed that AI systems "should be able to 'forget' personal user data on request". Reasons cited included confidentiality, trust, personal privacy, and user control. Furthermore, 22 out of 30 respondents believed that "technical 'right to be forgotten' features should be mandatory in AI systems worldwide". Despite this strong demand, opinions were split on the technical feasibility of AI systems truly forgetting data once used for training: 13 believed it was feasible, 14 were "Not sure", and 3 believed it was not feasible.

3.4 Key Concerns Regarding AI Data Retention

"Loss of privacy" and "Misuse of personal information" were the top concerns, each cited by 25 respondents. "Data breaches" followed with 16 mentions. The general comfort level with AI systems retaining data indefinitely for training was low, with 18 out of 30 respondents being "Somewhat uncomfortable". Open-ended responses reinforced these themes, with "Privacy breach/Loss of privacy/Invasion of privacy" and "Misuse of personal information/data" being the most common ethical challenges identified. This was a question where multiple responses could be selected.

Table 2: Top Concerns Regarding AI Data Retention

Concern	Count	Percentage
Loss of privacy	22	73.3%
Misuse of personal information	25	83.3%
Data breaches	12	40%
Surveillance	7	23.3%
Bias due to outdated data	5	16.7%
None of the above	2	6.7%

3.5 Data prioritization for deletion and comfort levels

"Personally identifiable information (PII)" was overwhelmingly prioritized for deletion by 18 respondents, followed by "Location data" (14 respondents), "User behavioral data" (8 respondents). Conversely, 25 respondents were only comfortable providing "General preferences and opinions (not identifiable)," with very few comfortable providing PII (2 respondents) or user behavioral data (7 respondents). This was a question where multiple responses could be selected.

Table 3: Preferred data types for deletion and provision

Data Type	Prioritized for Deletion (Count)	Comfortable Providing (Count)
Personally identifiable information (PII)	18	2
User behavioral data	8	7
Location data	14	0
All of the above for deletion	19	1
General preferences and opinions (not identifiable)	N/A	25
None of the above for provision	0	5

3.6 Ethical Challenges and Trust in AI Systems

Beyond direct harms, some respondents identified more subtle ethical challenges, such as AI's potential to "steer behavior subtly" or perpetuate "bias due to outdated data." A critical finding was the near-unanimous agreement (21 out of 30 respondents) that transparent data control (e.g., view/delete history, opt out of training) would increase their trust in an AI service. Additional comments highlighted the need for "easy to go through set of privacy policies" and stronger "Data privacy laws".

4. Discussion

The findings of this survey illuminate a significant tension between the operational demands of AI systems and evolving user expectations for data privacy and control. The demographic profile of respondents-predominantly young, highly familiar with, and frequent users of AI suggests that their articulated concerns are indicative of future societal expectations for AI.

The "awareness-action gap" is a critical observation. While users are largely aware that AI collects and utilizes their data, their low engagement with privacy policies indicates that current mechanisms for informed consent are ineffective. This suggests that the burden of understanding data practices falls disproportionately on the user, leading to a de facto acceptance of terms without genuine comprehension. This gap necessitates innovative approaches to privacy communication, moving beyond lengthy legal documents to more accessible, interactive, and transparent formats that genuinely empower users [3].

The overwhelming support for the "right to be forgotten" and its mandatory implementation underscores its perceived status as a fundamental digital right. Users view the ability to erase their data as essential for maintaining confidentiality, boosting trust, and ensuring personal autonomy. This strong demand implies that for AI developers, implementing robust data deletion mechanisms is not merely a regulatory obligation but a strategic imperative for fostering user adoption and loyalty. Without this perceived control, users may limit their engagement with AI, particularly for sensitive interactions, thereby restricting AI's potential to deliver personalized and valuable services. However, the significant division regarding the technical feasibility of "forgetting" data once it has been used for AI training presents a considerable challenge. This disparity highlights a conundrum for both policymakers and technologists: The public's ethical expectation for data deletion appears to outpace the current understanding or capabilities of AI systems to genuinely "unlearn" or erase data from complex models without compromising integrity. This gap necessitates substantial research into machine unlearning techniques [4] and calls for a pragmatic approach to policy that carefully balances user rights with technical realities, potentially through clear definitions of what "forgetting" truly entails in the context of advanced AI.

The consistent prominence of "loss of privacy", "misuse of personal information", and "data breaches" as top concerns indicates that users perceive these as interconnected elements of a causal chain. Addressing these anxieties requires a holistic approach that encompasses robust data security, strict internal policies on data access and use, and clear user rights regarding data control. Furthermore, the emerging awareness of more subtle ethical challenges, such as AI's potential to "steer behavior subtly" or perpetuate "bias due to outdated data", suggests that future ethical discussions and regulations will need to evolve beyond traditional data protection to encompass the psychological and societal impacts of AI's pervasive memory.

Finally, the near-unanimous agreement that transparent data control builds trust is a powerful endorsement of user-centric design principles. This extends beyond simple data deletion to encompass broader features like the ability to view data history and opt out of training. For AI companies, investing in user-friendly data dashboards, clear opt-in/opt-out mechanisms, and accessible data deletion tools is paramount. This represents a significant competitive advantage, as companies prioritizing user agency and transparency are likely to gain a substantial trust dividend, leading to greater adoption and sustained engagement.

5. Conclusion

This survey provides compelling evidence of a strong public desire for greater control over personal data within AI systems, centered on the "right to be forgotten". The findings highlight critical gaps in current privacy practices, particularly the disconnect between user awareness and engagement with privacy policies, and the tension between ethical demands for data erasure and perceived technical feasibility.

To foster a trustworthy and ethically sound AI ecosystem, the following recommendations are crucial:

- **Implement user-centric privacy by design:** AI developers must integrate clear, intuitive data control features, including explicit options to view, delete, and opt out of data processing, as core functionalities [5].
- **Innovate privacy policy communication:** Transition from complex legal documents to more digestible, interactive, and transparent formats that genuinely inform users about data practices.
- **Invest in machine unlearning research:** Prioritize research and development into robust and verifiable machine unlearning techniques to bridge the gap between user expectations and technical capabilities for data erasure.
- **Strengthen data governance and regulation:** Policymakers should consider the global implementation of mandatory "right to be forgotten" features, particularly focusing on Personally Identifiable Information (PII), and reinforce regulatory frameworks to address third-party data access and use. Reinforcing existing data privacy laws and establishing new ones where gaps exist is essential.
- **Anticipate evolving ethical challenges:** Acknowledge that the ethical landscape of AI extends beyond personal data privacy to include intellectual property, algorithmic bias, and broader societal impacts, requiring continuous dialogue and adaptive policy.

The future success and societal acceptance of AI hinge on its ability to earn and maintain public trust. This study unequivocally demonstrates that trust is deeply intertwined with transparency and user control over personal data. A collaborative approach involving developers, policymakers, and users is imperative to build an AI future that is not only technologically advanced but also ethically sound and respectful of individual digital rights.

References

1. AI Privacy Survey. Responses; 2025.
2. European Parliament and Council of the European Union. Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Off J Eur Union. 2016;L119:1-88.
3. Acquisti A, Brandimarte L, Loewenstein G. Privacy and human behavior in the age of information. Science. 2015;347(6221):509-514.
4. Bourtoule L, Chandrasekaran V, Choquette-Choo CA, Jia H, Li L, Naresh BR, et al. Machine unlearning. In: 2021 IEEE Symposium on Security and Privacy (SP). Los Alamitos (CA): IEEE; 2021, p. 502-519.
5. Cavoukian A. Privacy by design: The 7 foundational principles. Toronto: Information and Privacy Commissioner of Ontario; 2012.