International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor 2025: 7.089

AI Chatbot Companies Promise Privacy Control, But Lawsuits and Regulators Tell a Different Story

Agamjot Singh Babra

Student at Spring Dale Senior School, Amritsar
Email: *agamjot.11642[at]springdaleeducation.com*

Abstract: ***This study examines the gap between the privacy commitments communicated by major AI chatbot companies and allegations presented in recent lawsuits and regulatory actions. It also investigates users' awareness of these issues and whether such awareness influences their use of AI chatbots. A mixed-methods design combines qualitative document analysis of five major platforms, ChatGPT, Gemini, Perplexity AI, Meta AI, and Character.AI, with a survey of 209 respondents. AI chatbot use was reported by 95.7 percent of respondents, with most participants using these tools frequently. However, 52.2 percent had never read the privacy policy of their most-used AI tool, while 52.6 percent were unaware of or unsure about relevant lawsuits. Baseline trust in AI companies' protection of user data averaged 2.56 out of 5. After respondents were informed about a specific lawsuit concerning chatbot data practices, 33 percent reported that their usage would not change and 27.3 percent remained unsure. The findings indicate a privacy paradox in which concerns and limited trust coexist with continued chatbot use. The study highlights the importance of clearer privacy practices, improved consumer awareness, and appropriate regulatory oversight.***

Keywords: AI Chatbots, Data Privacy, Consumer Awareness, Consumer Trust, AI Regulation

1. Introduction

AI chatbots have become part of daily life for a large number of users within a relatively short period. Tools like ChatGPT, Gemini, and Perplexity are being used every day to write emails, answer questions, get help with assignments, and sometimes even to talk through personal problems. Most users do not spend much time thinking about what happens to those conversations once they hit send. Who can read them? What are they being used for? Are they being passed along to other companies? These are questions that barely cross most people's minds.

The companies behind these tools have plenty to say on the topic in their privacy policies. They use words like transparency, user control, and data protection. But a growing wave of class action lawsuits and regulatory investigations in 2025 and 2026 has started telling a very different story about what these companies actually do with the data that users share. This study takes that gap seriously and tries to investigate it through both document research and a real survey of 209 everyday users.

The central question guiding this research is: to what extent are users of AI chatbot platforms actually aware of how their data is collected, used, and shared, and does revealing the gap between what these companies promise and what they are actually alleged to be doing change how users feel about these tools or whether they keep using them?

1.1 A Mixed-Methods Approach Combining Document Analysis and Survey Research

This study uses two different research methods together because each one answers a different part of the research question. The first strand involved qualitative document analysis. The publicly available privacy policies and terms of service for five widely used AI chatbot platforms, which are ChatGPT, Gemini, Perplexity AI, Meta AI, and Character.AI, were reviewed and compared against publicly reported lawsuits, regulatory filings, and news coverage about what each company has actually done with user data. Going through these documents side by side made it possible to identify a consistent claims-versus-reality gap across all five companies, even though they are quite different from each other in terms of size, location, and business model.

The second strand was a primary survey distributed to a convenience sample of 209 respondents made up mostly of students and young adults. The survey examined how much respondents know about AI chatbot data practices, how their trust in these companies changed once they were shown real information about a specific controversy, and what actually drives their choice of which AI tool to use. Convenience sampling is a useful way of exploring attitudes and spotting trends, but as discussed in the limitations section, it cannot be treated as fully representative of all AI chatbot users.

1.2 Survey Administration and Analysis

The survey was circulated through the school's ICT (Information and Technology) Club, led by the author as Club President, to students in Classes 9 to 12. It was administered through Google Forms during the research period, and participation was voluntary. Eligible participants were school students in the stated class range who were reached through the Club network. The questionnaire contained 12 items, principally multiple-choice questions, together with a five-point trust-rating item. It covered chatbot use, platform preference, privacy-policy engagement, awareness of litigation, trust, intended behavioural change, and selection priorities. The disclosure stimulus described the allegation that tracking technologies on ChatGPT transmitted user-query information to Meta and Google without consent, and clearly presented the matter as an allegation in active litigation [1]. Percentages were calculated by dividing each response count by the total sample of 209 and multiplying by 100. The weighted trust score was calculated as the sum of each rating multiplied by its response count, divided by 209.

The form recorded students' names but collected no email addresses or signatures. No separate consent form or formal school ethics approval was required because the work was a voluntary, student-led ICT Club research project. Results are reported only in aggregate.

Percentage (%) = $(n_i / N) \times 100$, where N = 209

Weighted trust score = $[\Sigma_{i=1}^{5} (r_i \times n_i)] / N = 535 / 209 = 2.56$

1.3 AI Companies Pledge Privacy Control While Facing Allegations of Data Sharing

Across all the major AI chatbot companies, a similar pattern emerges across the examined companies. Each company publicly describes its data practices as something users are in control of, while active lawsuits and regulatory investigations describe something quite different happening in the background. This section examines five companies individually.

OpenAI (ChatGPT)
OpenAI's privacy policy states clearly that conversation data may be used to improve its models and that users can adjust their settings to limit this. The company frames this as a choice that belongs to the user. A May 2026 class action lawsuit called Couture v. OpenAI Global, LLC tells a different story [1]. It alleges that OpenAI embedded Meta's Facebook Pixel and Google Analytics into the ChatGPT website, and that this setup silently sent the content of users' conversations, including sensitive information about health, finances, and legal matters, to Meta and Google in real time without properly informing users that any of this was happening.

Google (Gemini)
Google states that its Smart Features for Gemini are opt-in and that Gmail content is not used to train its AI models, only to personalise features. A November 2025 class action called Thele v. Google LLC describes something different [4], [6]. It alleges that in October 2025, Google quietly switched Gemini's Smart Features on by default for all Gmail, Chat, and Meet users, giving Gemini access to entire communication histories without users meaningfully consenting to this. The lawsuit also claims that turning these features off required navigating through buried settings, which the plaintiffs argue may violate the California Invasion of Privacy Act. These are claims in active litigation rather than findings from a court ruling, but they describe a real gap between what Google publicly says and what users allege actually happened.

Perplexity AI
Perplexity AI describes its data collection as standard service-improvement practice and does not prominently mention any third-party advertising trackers. A March 2026 class action called Doe v. Perplexity AI, Inc. alleges [11] that the company embedded Meta Pixel and Google tracking code into its app, and that this code forwarded the content of users' conversations, including one plaintiff's sensitive financial and tax information, to Meta and Google for targeted advertising. The lawsuit further claims this happened even while the app's Incognito mode was active, which directly challenges the idea that privacy modes offer any real protection against outside tracking.

Meta AI
Meta updated its official policy in December 2025 to state that user interactions with its generative AI tools may be used to personalise content and advertisements on Facebook, Instagram, and other Meta-owned platforms, with controls available in account settings. Reporting from January 2026, one month after that update, found [14] that Meta had already started feeding AI chat interactions from Facebook, Instagram, and WhatsApp into its ad-personalisation systems by default, without offering any straightforward opt-out for U.S. users. A separate March 2026 lawsuit alleges [12] that footage captured through Meta's AI-powered smart glasses was reviewed by human contractors at an overseas subcontractor, including highly sensitive personal content, despite the company describing this review as mostly automated. Together, these accounts suggest Meta's AI tools may be working in ways that are more invasive than its policy language leads users to believe.

Character.AI
Character.AI's terms of service describe standard data-handling practices and include age requirements for using the platform. In January 2026, Kentucky's Attorney General filed the state's first lawsuit under its new Consumer Data Protection Act against Character.AI. The lawsuit alleges that the company failed to put proper age-verification and parental-consent systems in place, which resulted in the unlawful collection of children's personal data in violation of state consumer-protection and privacy law. This case stands out not just for what it claims about Character.AI specifically, but because it signals that state regulators are increasingly willing to apply new data-privacy laws directly against AI chatbot companies.

It is worth repeating clearly that none of the allegations described in this section have been proven in court. Each one is still an active lawsuit with no final ruling. That said, the fact that this same basic pattern appears across five completely separate companies, ranging from some of the biggest names in tech to newer AI-focused startups, strongly suggests that the gap between what these companies promise and what they are alleged to actually do is not a coincidence. This pattern may indicate a broader structural issue within current industry practices rather than an isolated problem involving one or two companies.

Previous studies have likewise identified privacy concerns, trust dynamics, and disclosure vulnerabilities in chatbot use [5], [8]-[10], [15].

2. Usage Keeps Climbing Even as Regulatory Pressure and Risk Perception Both Rise

One of the more striking things to notice when researching this topic is how little people's growing awareness of AI privacy risks actually affects what they do. Survey data from Deloitte's 2025 Connected Consumer report shows that 82 percent of generative-AI users now believe the technology could be misused, which is up from 74 percent the year before. Despite this increase,

usage has not slowed down at all. More than half of surveyed U.S. consumers are actively using or experimenting with generative AI tools, and workplace use alone has grown by more than five times since 2023. The same report found that 70 percent of people say they worry about data privacy when using digital services. But when it comes to actual behaviour, only a small minority said they would refuse to share sensitive information like financial or biometric data. There is a clear gap between what people claim to be worried about and what they actually do, and it suggests that the convenience and usefulness of these tools matters more to most people than the privacy concerns, at least for now.

Regulatory activity indicates increasing attention to this gap. Baker Botts' 2026 legal analysis identified 78 chatbot-related bills filed across 27 U.S. states in just the first part of 2026, alongside 58 active lawsuits targeting AI chatbot companies over their data practices. The report calls all of this a regulatory wave aimed specifically at AI-driven communication tools. Children's data has become a particular flashpoint within this broader trend. Kentucky's January 2026 lawsuit against Character.AI was the first time any U.S. state paired a child-specific data-protection law with AI chatbot enforcement, and it will probably not be the last. Market research from Attest adds useful context here [2]: usage is heavily concentrated in just a few major platforms, with ChatGPT at 52 percent, Google Gemini at 30 percent, and Microsoft Copilot at 20 percent. This means the regulatory pressure that is building up is landing directly on the same handful of companies that most users already depend on every day.

Putting these two observations together produces a picture of a technology that is becoming more valuable to consumers and more concerning to regulators at roughly the same pace. How this tension eventually resolves, whether through stronger consumer protections, continued user indifference, or some kind of shift in the market, is genuinely hard to predict. But it is exactly that tension that this study's own survey was designed to test at a personal, individual level.

5. Survey Findings: 209 Respondents Reveal Heavy Use, Low Engagement With Privacy Policies, and a Clear Privacy Paradox

With Privacy Policies, and a Clear Privacy Paradox

The primary survey reached 209 respondents drawn mostly from a student and young-adult demographic. The results were predictable in some places and genuinely surprising in others. What stayed consistent across all twelve questions was a picture of a generation that is deeply integrated into AI chatbot use on a daily basis but largely disconnected from the privacy terms that govern that use, and that, even when shown real evidence of alleged misconduct, remains divided on whether it would actually change anything about how they behave.

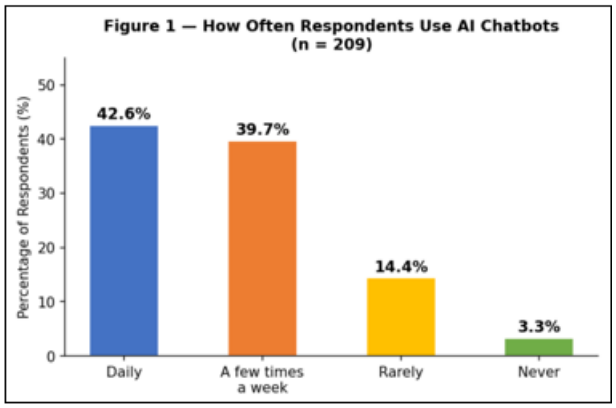

Figure 1: Frequency of AI chatbot usage among 209 respondents. Over 82 percent use these tools daily or several times a week, showing how central they have become to everyday routines

Usage was close to universal in this sample. As Figure 1 shows, 95.7 percent of respondents said they use AI chatbots. ChatGPT was the most common choice at 53.6 percent, followed by Gemini at 19.6 percent and Claude at 12.9 percent. More importantly, this is not occasional or casual use. A total of 42.6 percent said they use these tools daily, and another 39.7 percent said they use them a few times a week. This means that more than 82 percent of respondents are regular, frequent users of at least one AI chatbot platform.

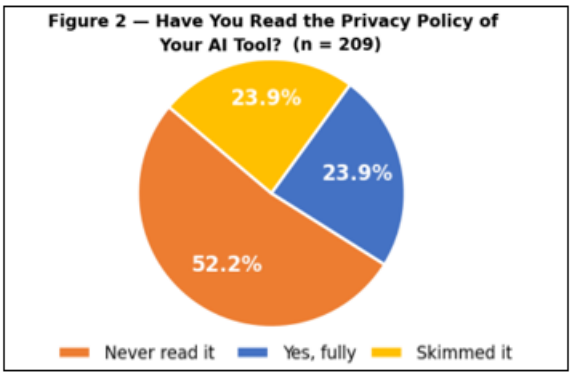

Figure 2: Privacy policy reading habits among respondents. A majority of 52.2 percent have never read the privacy policy of the AI tool they use most, and only 23.9 percent have read one fully.

Despite how frequently respondents use these tools, engagement with privacy policies is almost non-existent. Figure 2 shows that more than half of respondents, specifically 52.2 percent, said they had never read the privacy policy of the AI tool they use most. Only 23.9 percent had read one in full. Another 23.9 percent said they had only skimmed it. This means that at best, roughly three-quarters of respondents have either no real understanding or only a partial understanding of the terms they agreed to when they first started using these platforms.

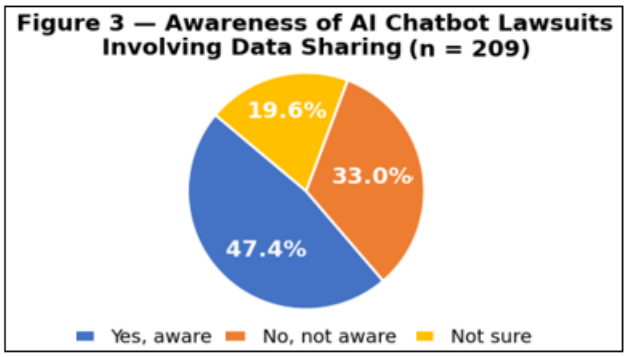

Figure 3: Awareness of AI chatbot lawsuits involving data sharing with advertisers without consent. A combined 52.6 percent of respondents were either unaware at 33 percent or unsure at 19.6 percent that such lawsuits existed

The awareness questions produced mixed results. When asked whether they knew AI chatbots might use their conversations to train models, 67.5 percent said yes, which was higher than expected. But as Figure 3 shows, awareness dropped sharply when it came to the specific lawsuits. Only 47.4 percent said they were aware that AI chatbot companies have faced lawsuits over sharing user conversations with advertisers without consent. A combined 52.6 percent either said no at 33 percent or were not sure at 19.6 percent. More than half of the respondents had no clear picture of the legal controversies directly affecting the tools they use every single day.

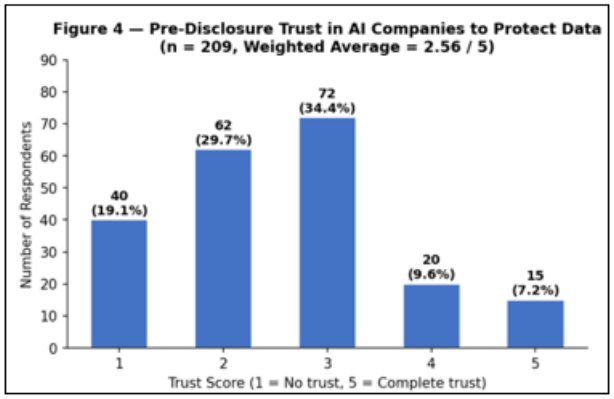

Figure 4: Pre-disclosure trust scores on a 1 to 5 scale, where 1 means no trust and 5 means complete trust. The weighted average across all 209 respondents was 2.56 out of 5, reflecting widespread distrust even before any specific lawsuit information was shared.

The pre-disclosure trust score was one of the most notable results in the entire survey. Before being shown any specific information about a lawsuit, respondents rated how much they trust AI companies to protect their data on a scale of 1 to 5. Figure 4 shows the full distribution. A total of 19.1 percent gave a rating of 1, meaning no trust at all. Another 29.7 percent gave a 2, and 34.4 percent gave a 3. This means nearly half of all respondents rated their trust at 2 or below. The weighted average came out at 2.56 out of 5. Even before seeing any specific evidence, most respondents already did not have much trust in these companies to handle their data responsibly.

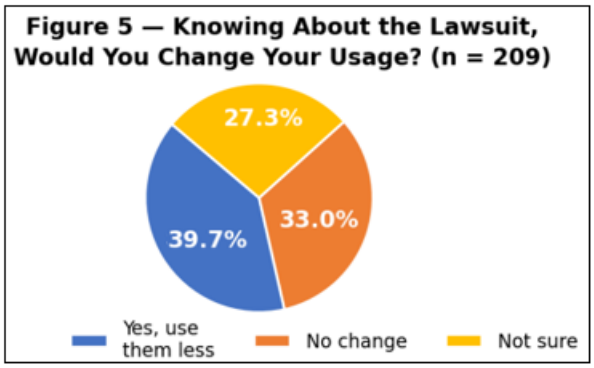

Figure 5: Whether respondents would change their AI chatbot usage after learning about the ChatGPT tracking lawsuit. A combined 60.3 percent said no change or were unsure, which is the clearest sign of the privacy paradox appearing in this study's sample

After reading a disclosure about the ChatGPT lawsuit, which stated that OpenAI allegedly embedded Facebook Pixel and Google Analytics into its website and used them to send users' queries to Meta and Google without consent, respondents were asked whether knowing this would change how they use AI chatbots. Figure 5 shows what they said. While 39.7 percent answered yes and said they would use these tools less, a significant 33 percent said nothing about their usage would change at all. Another 27.3 percent said they were not sure. This means that even when respondents were shown a specific, named, documented lawsuit about the exact tool most of them use every day, only a minority said they would definitely cut back. The majority would either maintain their habits completely or could not say they would change them.

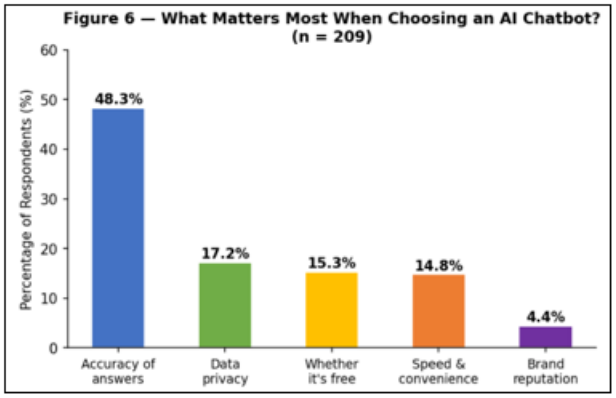

Figure 6: What respondents prioritise when choosing an AI chatbot. Accuracy of answers came first at 48.3 percent, with data privacy a distant second at 17.2 percent.

When asked what matters most when choosing which AI chatbot to use, Figure 6 shows that accuracy of answers came first at 48.3 percent. Data privacy ranked second at 17.2 percent, followed by whether the tool is free at 15.3 percent and speed and convenience at 14.8 percent. Brand reputation barely registered. This ranking tells an important story on its own. Even among respondents who had just finished answering a full survey about privacy concerns, privacy was not the thing they prioritize most when choosing a tool. Accuracy and convenience together far outweigh privacy in this sample, and that goes a long way toward explaining why trust is low and yet usage keeps climbing regardless.

Taken together, these results make the privacy paradox visible in a real and measurable way. The respondents in this sample use AI chatbots constantly, rarely read the privacy policies, have low baseline trust in the companies behind these tools, and yet when confronted with evidence of actual alleged misconduct, most are not willing to say they would behave any differently. Within this sample, convenience appears to outweigh privacy concerns for many respondents.

3. Acknowledging the Boundaries of This Study

This research has real limitations that should be considered when interpreting the findings before drawing firm conclusions from what was found.

The most important limitation is that the company-specific evidence in this study is based almost entirely on active lawsuits where courts have not yet issued final rulings. Every case described in the claims versus reality section is still ongoing, which means the allegations could

be modified, partially dismissed, or rejected entirely as they move through the legal process. Everything discussed in that section should be read as what has been credibly claimed in formal legal filings, not as what has been proven to be true.

The survey used in this study also has a built-in limitation related to how respondents were recruited. Because the sample came from a convenience approach, meaning people who were reachable and willing to participate, the group almost certainly skewed younger and more digitally active than the general population of AI chatbot users. This makes the results genuinely useful for identifying patterns and trends within that particular demographic, but it would not be accurate to assume the same findings would appear across all age groups, education levels, or countries.

Scope is another constraint worth noting. The study examined five companies specifically chosen because of their visibility and available legal documentation, and it relied almost entirely on English-language sources. There are many other AI chatbot providers operating globally, and the data practices, legal environments, and user attitudes in other markets could produce findings that look quite different from the ones in this study, or that directly contradict them.

Finally, this research represents a snapshot of a single moment in a legal and regulatory landscape that is moving at significant speed. New lawsuits, policy announcements, settlements, and regulations were appearing throughout the time this study was being conducted. Any conclusions about a specific company's practices could shift considerably in the months following this paper's completion, which is a limitation that any research in this area currently has to accept.

4. Widespread Usage, Low Trust, and Little Behavioural Change: What This Study Found and Why It Matters

This study examined whether users are aware of privacy concerns surrounding major AI chatbots and whether increased awareness influences their behaviour. The document analysis identified recurring differences between companies' stated privacy practices and allegations contained in recent lawsuits and regulatory actions, although these allegations should not be interpreted as established legal findings. The survey of 209 respondents showed frequent chatbot use alongside limited engagement with privacy policies and relatively low trust in companies' ability to protect user data. Nevertheless, only 39.7 percent of respondents reported that disclosure of a specific privacy-related lawsuit would cause them to reduce their chatbot use. These findings suggest a privacy paradox within the surveyed population, in which concern and limited trust coexist with continued use. Because the sample was based on convenience sampling and largely represented students and young adults, the findings should not be generalised to all chatbot users. Future research using larger and more diverse samples could test whether similar patterns occur across demographic groups and jurisdictions. Overall, the findings indicate that consumer awareness alone may have limited influence on behaviour and support continued examination of privacy design, transparency, and regulatory safeguards in AI chatbot services.

References

[1] Couture v. OpenAI Global, LLC, No. 3:26-cv-03000-H-GC, Class Action Complaint, U.S. District Court for the Southern District of California, filed May 13, 2026. https://stream-ai.s3.us-west-1.amazonaws.com/class-action-complaints/5-13-26/Couture_v_Openai_Global_LLC__casdce-26-03000__0001.0.pdf

[2] Attest, "2025 Consumer Adoption of AI Report," May 2, 2026. https://www.askattest.com/blog/articles/2025-consumer-adoption-of-ai-report

[3] Baker Botts, "AI Chatbot Regulation: 78 State Bills, 58 Lawsuits," Feb. 24, 2026. https://ourtake.bakerbotts.com/post/102mipe/ai-chatbot-regulation-78-state-bills-58-lawsuits

[4] Thele v. Google LLC, No. 5:25-cv-09704-NC, First Amended Class Action Complaint, U.S. District Court for the Northern District of California, filed Nov. 12, 2025. https://media.reclaimthenet.org/docs/google-gemini-smart-features-class-action-complaint.pdf

[5] T. Christakis, "You Trust Your Chatbot With Everything. Should You? Part 1: How the Controller Uses Your Chat Data," IAPP, Mar. 4, 2026. https://iapp.org/news/a/new-study-maps-the-privacy-gap-in-consumer-ai-and-proposes-a-fix

[6] ClassAction.org, "Thele v. Google LLC," Nov. 14, 2025. https://www.classaction.org/news/thele-v.-google-llc

[7] Deloitte Insights, "2025 Connected Consumer: Innovation with Trust," Sept. 25, 2025.

https://www.deloitte.com/us/en/insights/industry/telecommunications/connectivity-mobile-trends-survey.html
[8] E. Gumusel, "A Literature Review of User Privacy Concerns in Conversational Chatbots: A Social Informatics Approach," Journal of the Association for Information Science and Technology, vol. 76, no. 1, pp. 121-154, 2025. https://doi.org/10.1002/asi.24898
[9] J. Ive et al., "Privacy-Preserving Behaviour of Chatbot Users: Steering Through Trust Dynamics," arXiv:2411.17589, Nov. 26, 2024. https://arxiv.org/abs/2411.17589
[10] Z. Z. Jiang, "Self-Disclosure to AI: The Paradox of Trust and Vulnerability in Human-Machine Interactions," arXiv:2412.20564, 2024. https://arxiv.org/abs/2412.20564
[11] Doe v. Perplexity AI, Inc., No. 3:26-cv-02803, Class Action Complaint and Demand for Jury Trial, U.S. District Court for the Northern District of California, filed Mar. 31, 2026. https://ppc.land/content/files/2026/04/Doe-v-Perplexity-Complaint-3-31-26.pdf
[12] TechCrunch, "Meta Sued Over AI Smart Glasses' Privacy Concerns After Workers Reviewed Nudity, Sex, and Other Footage," Mar. 5, 2026. https://techcrunch.com/2026/03/05/meta-sued-over-ai-smart-glasses-privacy-concerns-after-workers-reviewed-nudity-sex-and-other-footage
[13] Commonwealth of Kentucky v. Character Technologies, Inc., No. 26-CI-00029, Complaint, Franklin Circuit Court, filed Jan. 8, 2026. https://www.ag.ky.gov/Press%20Release%20Attachments/CTI%20Complaint%20Motion%20and%20Order%20Filed.pdf
[14] WebProNews, "Meta's 2026 AI Policy Sparks Privacy Fury Over Chat Data Use," Jan. 6, 2026. https://webpronews.com/metas-2026-ai-policy-sparks-privacy-fury-over-chat-data-use
[15] H. Yang et al., "Determinants Affecting Consumer Trust in Communication With AI Chatbots: The Moderating Effect of Privacy Concerns," Journal of Organizational and End User Computing, vol. 35, no. 1, 2023. https://doi.org/10.4018/JOEUC.328089