LEADERSHIP CENTER FOR ATTORNEY GENERAL STUDIES

Does Your AI Remember Too Much? Understanding AI Memory and Its Risks

Authors: AG Studies Staff and Policy Fellows

Have you ever chatted with an AI assistant or chatbot and felt like it remembered something you told it before? That's likely thanks to "AI memory" – the ability of artificial intelligence systems to store and recall information about you from your conversations. AI companies are rapidly developing this feature, arguing it makes AI tools more helpful and personalized. Imagine an AI tutor remembering a student's weak spots or an AI assistant recalling your preferences without being reminded. While convenient, this growing capability raises significant concerns about your privacy, your control over your data, and even your freedom to switch services or jobs – issues that State Attorneys General are starting to address.

Your AI Remembers You (What is AI Memory?)

AI memory refers to the collection, storage, and use of personal information shared by users during interactions with AI models. This isn't just about the immediate conversation; it's about building a persistent profile. The "memories" can include:

- Facts you mention (your job, location, family members)
- Your preferences (hobbies, interests, writing style)
- Details inferred by the AI based on your interactions

AI labs like Google and OpenAI are integrating memory features into their popular tools (like Gemini and ChatGPT). The goal is often to create a more seamless and personalized experience, making the AI feel like it "knows" you. While this can be genuinely useful for tasks like personalized learning or health advice, it also means the AI is building a detailed dossier about you over time.

How Much Are You Sharing (And Do You Know It?)

A key concern is how this information is collected and whether users truly consent to it. Memories can be gathered directly from what you type or say, but AI can also infer information. Do you know exactly what details the AI is storing? Do you know how it will be used?

Consent practices vary. Some AI tools might require you to actively "opt-in" to memory features, giving you more upfront control (like Google's approach with Gemini, which also promotes tools to view and delete memories). Others might have memory turned "on" by default (like OpenAI's initial approach), meaning the AI starts remembering things unless you proactively find the setting and turn it off. Many users, especially younger ones who readily adopt new AI tools, might share sensitive personal or professional details without fully understanding how that

information is being stored, used, or potentially shared down the line.

Feeling Stuck? (The Lock-In Problem)

As an AI learns more about you, it becomes more useful *to you*. This creates a potential "lock-in" effect. If you've spent months interacting with one AI assistant that now perfectly understands your needs and preferences, switching to a competitor means starting from scratch. You lose all that personalized history.

This lack of easy transferability makes it harder for new AI companies to compete and limits consumer choice. One proposed solution is data portability – the ability for users to easily take their data (including AI memories) from one service and move it to another. While regulations promoting data portability exist in some areas (like banking), applying them to complex AI memory data presents new challenges, especially when that data involves sensitive or proprietary information.

Your Memory at Work (Workplace Concerns)

The use of AI with memory features in the workplace adds another layer of complexity. Many employees, particularly younger workers, use multiple AI tools on the job. But who controls the "memories" created in these interactions?

- Employer Ownership: Your employer might claim ownership over all data generated using company-provided AI tools, including the AI's memory of your work style, projects, and potentially even personal details shared inadvertently.

- Job Mobility: If your employer controls this data, or if you become reliant on a proprietary AI tool trained specifically to your workflow, you might feel less able to leave for a better opportunity elsewhere. This "labor lock-in" could stifle career growth and make it harder for smaller businesses to attract talent.

- Lack of Clarity: Employees might not be clear on what information shared with a work-related AI tool they can take with them if they leave their job.

Why This Matters to You

AI memory touches on fundamental aspects of your digital life:

- Privacy: Your personal and professional details are being stored, potentially without your full awareness or control.

- Control: Default settings or confusing policies might lead you to share more than intended.

- Choice: Lock-in makes it harder to switch AI providers if you're unhappy with the service or its privacy practices.

- Career: Workplace AI memory could impact your future job prospects and professional freedom.

How State Attorneys General Can Help

As chief consumer protection officers, State Attorneys General (AGs) can play a crucial role in navigating the complexities of AI memory:

- Clarifying Consent: AGs can investigate whether AI companies' methods for obtaining consent to collect and use memories are clear, transparent, and fair under state consumer protection laws (often called UDAP laws). They can push for standards requiring explicit, informed consent rather than relying on default settings or buried clauses.

- Promoting Data Portability: AGs can encourage the development of standards and regulations that allow users to take their AI-generated memories with them when switching services, fostering competition and user choice. This includes tackling the tricky issues around intellectual property in workplace settings *before* AI becomes even more deeply integrated.

- Raising Consumer Awareness: AGs can issue consumer alerts and educational materials to help the public understand how AI memory works, the potential risks involved, and what rights they have regarding their data.

Navigating the Future of AI Memory

AI's ability to remember and personalize can be powerful, but it must be balanced with strong user protections. As this technology evolves, ensuring users have meaningful control over their data, clear understanding of how it's used, and the freedom to choose services without being unfairly locked in is paramount. Vigilance from consumers and proactive engagement from State Attorneys General are essential to guide the development of AI memory in a way that respects our rights and promotes fair competition.

Sources and Additional Reading

1. *Better AI Needs Better Data Rights*, Stan. HAI, https://hai.stanford.edu/better-ai-data-rights (last visited Apr. 14, 2025).
2. Todd Bishop, *Microsoft AI CEO sees long-term memory as key to unlocking future AI experiences*, GeekWire (Feb. 15, 2024), https://www.geekwire.com/2024/microsoft-ai-ceo-sees-long-term-memory-as-key-to-unlocking-future-ai-experiences/.
3. Bobby Allyn, *Lawsuit targets Character.AI, saying chatbot gets kids hooked, harvests their data*, NPR (Feb. 12, 2024), https://www.npr.org/2024/02/12/1230901371/character-ai-lawsuit-kids-privacy.
4. Paul M. Barrett et al., *How tech platforms fuel U.S. political polarization and what government can do about it*, Brookings Inst. (Sept. 27, 2021),

https://www.brookings.edu/articles/how-tech-platforms-fuel-u-s-political-polarization-and-what-government-can-do-about-it/.
5. Hope King, *Scoop: Gen Z brings AI disruption to the workplace*, Axios (Nov. 25, 2024), https://www.axios.com/2024/11/25/gen-z-ai-work-survey.
6. *Fear of Idea Theft Stifles Workplace Innovation, TAU Study Finds*, Tel Aviv Univ. (Mar. 29, 2023), https://english.tau.ac.il/research/idea-withholding.
7. Timothy P. Glynn, *Taking Matters Into Their Own Hands: Employee Control Over the Creations of Their Labor*, 15 Geo. Mason L. Rev. 159 (2007).
8. Emilia David, *OpenAI is testing 'memory' for ChatGPT*, The Verge (Feb. 13, 2024), https://www.theverge.com/2024/2/13/24071106/chatgpt-memory-openai-ai-chatbot-history.
9. *Data Broker Market Forecasts from 2024 to 2029*, Yahoo Fin. (Mar. 14, 2024), https://finance.yahoo.com/news/data-broker-market-forecasts-2024-093500963.html.
10. Tom Wheeler & Gene Kimmelman, *Data portability and interoperability: A primer on two policy tools for regulation of digitized industries*, Brookings Inst. (Dec. 19, 2022), https://www.brookings.edu/articles/data-portability-and-interoperability-a-primer-on-two-policy-tools-for-regulation-of-digitized-industries-2/.