GEORGIA INSTITUTE OF TECHNOLOGY

CS6675-CS4675 Technology Review

JAMES CHEN

SYSTEMS: GEMINI 1.5, ChatGPT-4o UPDATE: 2025.04.39

Table of Contents

Abstract

This technology review explores the privacy implications and data practices of two leading Large Language Models (LLMs): Gemini 1.5 and ChatGPT-4o (2025.04.39 update). As LLMs become integrated into society, concerns about data privacy, user control, and legal compliance have grown. This report examines how these models handle personally identifiable information (PII), their mechanisms for notice and consent, and their alignment with evolving privacy legislation. Through a detailed comparison of system architecture, data flows, access permissions, and risk mitigation strategies, this review provides an assessment of privacy safeguards.

1.1 Project Purpose and Scope

The purpose of this review is to assess the privacy practices, risks, and mitigations associated with Gemini 1.5 (Google DeepMind) and ChatGPT-4o (OpenAI). The rapid advancement of Large Language Models (LLMs) has led to widespread adoption across academic communities. Students and faculty mainly use Gemini and ChatGPT to support their learning and assist with completing academic tasks. By using large language models (LLMs), users—including students, staff, and alumni—can utilize AI-generated information to enhance their educational and professional efforts.

As these models continue to fuel educational tools, research workflows, business productivity apps, and more, understanding how they collect, store, process, and share user data is crucial. This report focuses on The types of PII and non-PII collected, the level of user control, transparency, and consent provided, mitigation strategies and comparative privacy advantages between the two models. The review is conducted in the context of academic inquiry at the Georgia Institute of Technology and aims to provide actionable insights for students, developers, and institutions considering LLM integration.

1.2 Background on LLMs and Privacy Risks

Large Language Models (LLMs) use have exploded both complexity and real-world utility. The global LLM market is predicted to go from $1590 million in 2023 to $2598 million in 2030, and estimates have 750 million apps using LLMs (SpringsApps, 2025). This has resulted in transformative applications such as education, as 62% of universities now use LLMs for tutoring systems. In healthcare, clinical documentation processing time is reduced by 30% via fine-tuned models and enterprises have $15B annual cost savings predicted in customer service automation (Information is Beautiful, 2025).

The widespread adoption of Large Language Models (LLMs) in academic and professional settings has introduced significant privacy vulnerabilities. As noted by Coralogix (2023), LLMs like ChatGPT and Gemini process user inputs that may contain sensitive personal or institutional data, creating risks including data retention, training data contamination from user queries, inference attacks leaking private training data, or third-party exposure: API integrations that route data through external servers (Coralogix, 2023).

1.3 Selected LLMs Overview

We choose to focus on two LLMs: Google Gemini 1.5 and OpenAI ChatGPT-4o.

Google Gemini 1.5 (previously Bard) is a multimodal AI system developed by Google DeepMind, with a 10M token context window and advanced reasoning capabilities across text, images, and audio (Google, 2025). It uses Google's proprietary Transformer-based architecture, optimized for real-time web search integration and enterprise applications (SpringsApps, 2024).

OpenAI's ChatGPT-4o (May 2024 release) employs a 1.76 trillion-parameter model with improved multilingual support and reduced hallucination rates (OpenAI, 2025). Unlike Gemini, ChatGPT-4o operates as a closed-system LLM, with stricter opt-out controls for user data training (OpenAI Help Center, 2025).

Data Types, Sources, and Usage

2.1 Personally Identifiable Information (PII) Collected

Using Gemini requires users to sign in, meaning they must have a Google account. Creating a Google account requires personal details such as full name, date of birth, and gender. Any personal information shared with the LLM through the Gemini interface is stored by Google as part of the user's account, with a default retention period of 18 months under the Gemini Apps Activity settings. Even if activity is off, your conversations will be retained for 72 hours. This lets Google provide the service and process any feedback (Gemini Apps Privacy Hub).

As far as a PIIs, it will collect online identifiers, such as IP address, domain name, geographic location, device information, such as hardware, operating system, browser, screen size, and usage data. It is known that personal identifiable information talked about in a conversation with Gemini will be stored. To prevent this, Gemini will advise its users not to enter any PII and remove PIIs from the memory (Google Privacy Policy 2025).

To use ChatGPT, users must create an OpenAI account, which requires an email address, name, and for paid subscriptions, payment information (OpenAI, 2025). Unlike Gemini, OpenAI does not collect birthdate or gender for account creation, though users may voluntarily provide such details for age verification or customization. All user inputs, including prompts, uploaded files (e.g., documents, images), and metadata (e.g., timestamps, device info), are generally stored in your chat data until you manually delete it. If you delete a chat, it's removed from OpenAI's systems within 30 days, though enterprise users can opt for zero-retention policies (OpenAI Privacy Policy, 2024).

Some data collected automatically include log data, usage data, device information (name of the device, operating system, device identifiers, and browser you are using), location information, and lastly, cookies and similar technologies (OpenAI Privacy Policy, 2025). Similar to Gemini, OpenAI advises against sharing PII in chats in order to prevent exposure.

2.2 Purpose of Collecting PII

The main reason Gemini, according to Google, collects personal information such as location and conversation history is to improve the service (Gemini Apps Privacy Hub). When a conversation is picked to be reviewed, Gemini will use the knowledge to prevent improve its services.

OpenAI collects and processes personal data primarily to support the delivery, improvement, and security of its services. This data helps maintain and operate ChatGPT, allowing the system to respond to user queries and function reliably. It also plays a key role in research and development, enabling the refinement of models and the creation of new features. Additionally, personal data is used for communication purposes, such as informing users about updates, policy changes, or events.

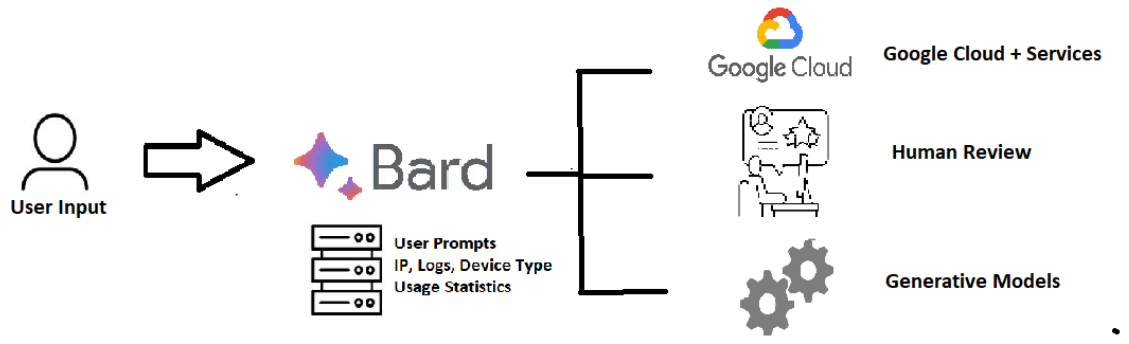
From a security and compliance standpoint, the data assists in preventing fraud, detecting abuse, and fulfilling legal requirements to protect both users and the platform. Unlike some other platforms, such as Google Gemini, which may leverage data for advertising, OpenAI emphasizes that it does not sell personal data or use it for profiling beyond the scope of service enhancement (OpenAI Privacy Policy, 2025).

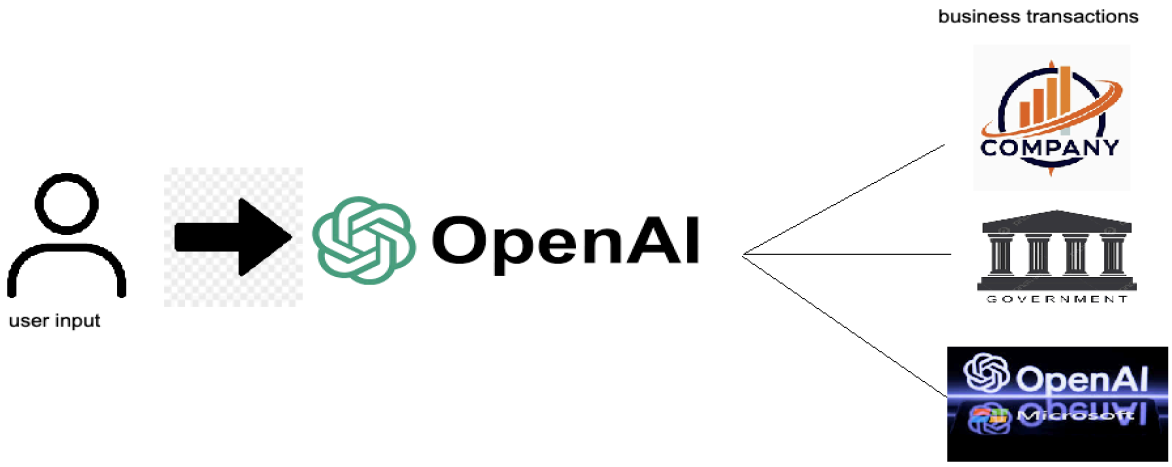
2.3 Other Systems with Access

Internal Systems	The data is managed by Google LLC (Gemini Apps Privacy Hub). Data processed in U.S. and EU (Dublin) data centers, with enterprise options for regional isolation (OpenAI, 2024).
Generative Machine-Learning Models	Gemini uses data from conversations, usage patterns, location information, and user feedback to enhance and refine its models. (Gemini Apps Privacy Hub). User inputs excluded from training if "Chat History & Training" is disabled. Enterprise data never trains models (OpenAI Help Center, 2024).

Other Services	They will use data with other services such as to develop Google products, including Google Cloud, and may also be shared with Google through sites using Google Analytics.(Gemini Apps Privacy Hub). Shares data with Azure (Microsoft) for cloud hosting and Stripe for payments under strict DPAs (OpenAI Privacy Policy, 2024). If they are sold, bankruptcy, receivership, or transition of service to another provider, the other company will get the data.
Trusted Partners	Google may get information from partners, including services and marketing directors(Google Privacy Policy 2025). OpenAI may share Personal Data to affiliates – entities that control, or are controlled by OpenAI (OpenAI Privacy Policy, 2024).
Human Review	Random samples are used, and only a small sample of information are seen to improve services(Gemini Apps Privacy Hub). <0.01% of non-enterprise chats reviewed for safety, anonymized where possible (OpenAI, 2025).
Government	Both ChatGPT and Gemini will share data with the government as legally requested.

2.4 Data Flow Diagrams and Pathways





Notice, Consent, and User Rights

3.1 User Notification Before Data Collection

OpenAI: Explicitly notifies users of data collection via its Privacy Policy and in-product banners, for example "Chats may be reviewed to improve our models". Enterprise users receive additional disclosures about data retention policies (OpenAI Help Center, 2025).

Google Gemini: Discloses data practices in the Gemini Apps Privacy Hub, including storage duration (default 18 months) and human review sampling (Google, 2025). They require acknowledgment of data usage policies upon first login.

3.2 Consent and Opt-Out Mechanisms

OpenAI: Users can disable training data usage via data controls training" (30 days). Enterprise/Business tiers allow zero-retention configurations (OpenAI, 2024).

Google Gemini: Users may adjust Gemini Apps Activity settings (3–36 months retention) or disable storage entirely (72-hour storage). Workspace admins can enforce organizational policies for institutional accounts (Google, 2024).

3.3 User Access, Control, and Correction of Data

OpenAI: can delete using tools via Settings > Data (includes prompts and responses). GDPR/CCPA requests can be submitted via Privacy Portal (OpenAI, 2024).

Google Gemini: Allows access and deletion of activity through My Activity Dashboard. Supports Takeout exports (JSON format) and auto-deletion schedules (Google, 2024).

Data Security and Lifecycle Management

4.1 Procedures for Data Accuracy and Integrity

Both OpenAI and Google have different protocols for data accuracy and quality. For openAI they have automated validation checks, human reviewers with data, and real time feedback loops where users can report inaccuracies and more to the system (OpenAI 2024).

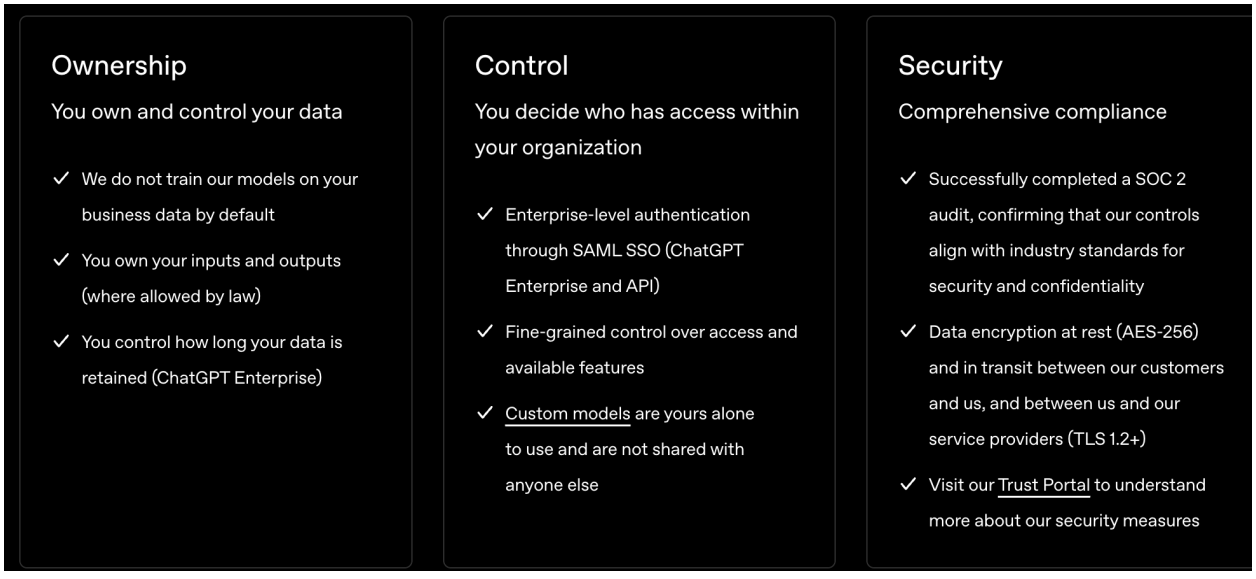
Google Gemini uses a different approach with its Fact Check API (Google Fact Check Tools API Documentation). They also also use filtration with synthetic analysis and semantic coherence scoring, with knowledge graph grounding for verify relationships. OpenAI takes a more external approach, while Gemini uses a more external based approach.

4.2 Use of PII in Testing, Training, or Research

OpenAI: Opt-in only for research data (via separate consent flow), differential privacy applied during fine-tuning), enterprise data exclusion: accounts automatically excluded from training sets

Google Gemini: Implicit consent model where all non-deleted conversations may be used, dynamic masking: auto-redaction of detected PII during model updates (Gemini Apps Privacy Hub)

4.3 Data Retention and Disposal Policies



Google Gemini: Users may adjust Gemini Apps Activity settings (3–36 months retention) or disable storage entirely (72-hour storage).

4.4 Impact of Recent Legislation on LLM Privacy Protections

The EU Artificial Intelligence Act (2024) introduced requirements that changed the practices for large language model providers. Both companies were required to implement real-time disclosure mechanisms for AI-generated content to improve transparency and reduce the misleading outputs. (European Commission) This caused Gemini to change the storage period from 36 to 18 months.

Another legislation that had caused changes is the California Delete Act (2023). This led OpenAI to develop one-click deletion portals to streamline user control over stored data and Google to implement automated PII scrubbers to protect sensitive user information during training processes (California Legislative Information). Both companies are now required to adhere to 72-hour breach notification protocols, ensuring prompt reporting of any data incidents.

However, even with this legislation, questions have arisen as to how much they follow them, as there are many instances where data retention is what they claim to be “unavoidable”. Furthermore data breaches such as the google indexing has shown their reliability to be faulty. Further investigation may be required.

Privacy Risks and Mitigation Strategies

5.1 Identified Privacy Risks (Re-Identification, Data Breach, etc.)

Model outputs may inadvertently leak PII from training data (e.g., names, emails, phone numbers). Another risk is data breaches and unauthorized access risk, as cloud-based LLM services are vulnerable to API exploits or insider threats, exposing user conversations. One example is ChatGPT’s 2023 bug temporarily exposed user chat histories.

Third parties also pose a risk, as both OpenAI and Google share data with cloud providers (Azure, Google Cloud) and government agencies under legal requests. Lastly, human reviewers can randomly sample conversations that may contain PII, despite anonymization efforts.

5.2 Historical Leaks

Both Google Gemini and OpenAI ChatGPT have experienced significant data breaches, exposing vulnerabilities in large language model (LLM) security practices.

Google Gemini AI Data Leak (2024)

In February 2024, Gemini AI user conversations were inadvertently indexed by search engines, making private chats publicly accessible through Bing search results (The Cyber Express). The leak stemmed from a data retention gap, where some Gemini subdomains were not properly restricted by robots.txt, allowing search engines to cache sensitive interactions (The Cyber Express). Users could also see that conversations could be stored for up to three years, even if manually deleted, and this created massive concerns about the risks of data usage and safety. Google later clarified the issue and removed exposed data from search indexes.

OpenAI ChatGPT Breaches (2023–2024)

March 2023 Payment Data Leak: A bug exposed user payment details and chat histories due to a Redis caching error. (Vijayan)

Samsung Proprietary Data Exposure (2023): Employees accidentally leaked internal code and meeting notes via ChatGPT, prompting a corporate ban. (Vijayan)

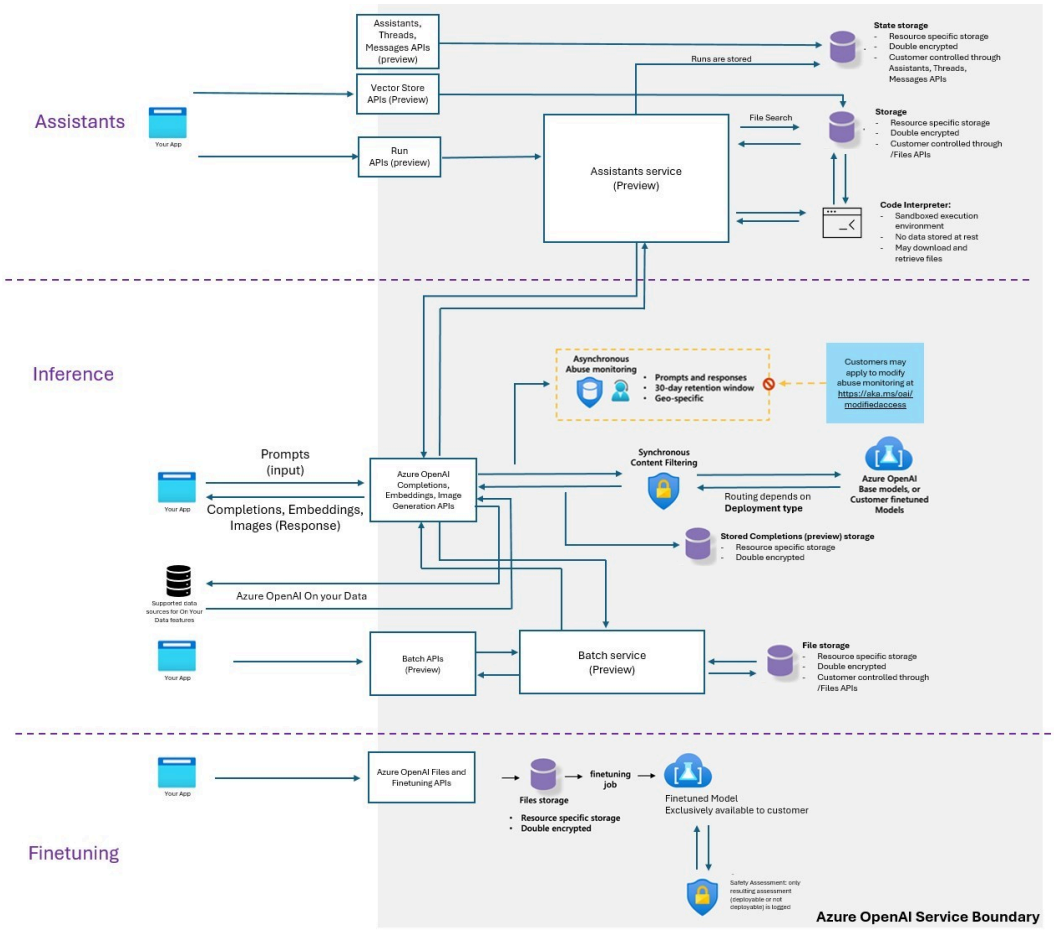
February 2024 Session Hijacking: Attackers accessed user accounts from Sri Lanka, exposing conversations and login credentials (Vijayan)

5.3 Model-Specific Safeguards and Data leak procedures

Google Cloud ("Data incident response process | Documentation | Google Cloud.")

Incident step	Goal	Description
Identification	Detection	Automated and manual processes detect potential vulnerabilities and incidents.
	Reporting	Automated and manual processes report the issue to the incident response team.
Coordination	Triage	The following activities occur: • On-call responder evaluates the nature of the incident report. • On-call responder assesses severity of the incident. • On-call responder assigns incident commander.
	Response team engagement	The following activities occur: • Incident commander completes assessment of known facts. • Incident commander designates leads from relevant teams and forms incident response team. • Incident response team evaluates incident and response effort.
Resolution	Investigation	The following activities occur: • Incident response team gathers key facts about the incident. • Additional resources are integrated as needed to allow for expedient resolution.
	Containment and recovery	Operations lead takes immediate steps to complete the following: • Limit ongoing damage. • Fix underlying issue. • Restore affected systems and services to normal operations.
	Communication	The following activities occur: • Key facts are evaluated to determine whether notification is appropriate. • Communications lead develops a communication plan with appropriate leads
Closure	Lessons learned	The following activities occur: • Incident response team retrospects on incident and response effort. • Incident command designates owners for long-term improvements.
Continuous improvement	Program development	Necessary teams, training, processes, resources, and tools are maintained.
	Prevention	Teams improve the incident response program based on lessons learned.

OpenAI Azure Data Processing ("Data, privacy, and security for Azure OpenAI Service)



5.4 How are risks Mitigated?

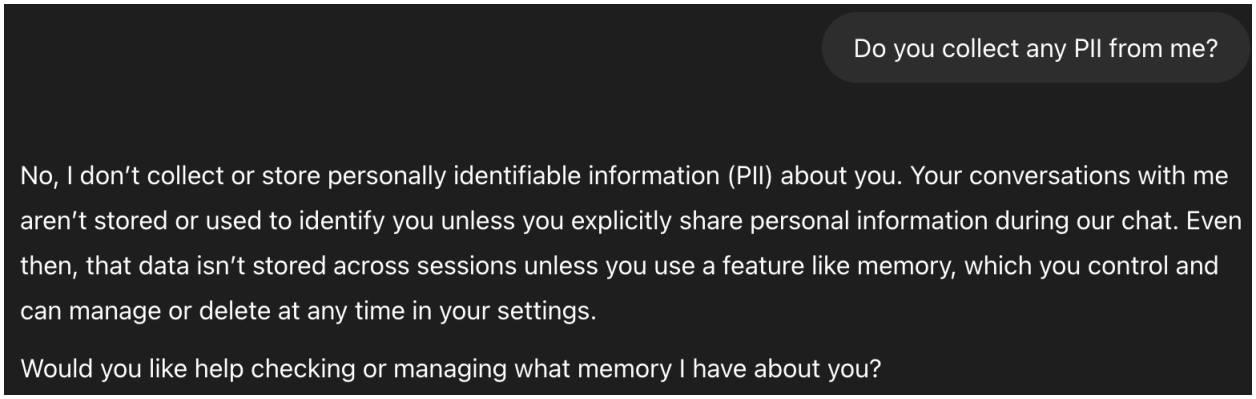
Risk	**Mitigation Strategy**
Reidentification	Gemini is trained on data that change to be anonymized as much as possible (Gemini, 2025). It has filters to ignore PII as well, as well as warnings not to enter. ChatGPT uses differential privacy during training and API-level content moderation to scrub sensitive outputs (GPT-4 System Card)

Data Leakage (internal)	To prevent internal data leakage, Gemini relies on on-device filtering and its Privacy Help Hub to educate users about unsafe inputs (Gemini Help Hub). ChatGPT allows users to disable chat history retention entirely or opt for enterprise-grade data isolation (OpenAI 2025).
Data Leakage (external)	Gemini tightened controls after its 2024 search-indexing incident, where conversations were accidentally exposed via Google Search (The Cyber Express) ChatGPT, following its March 2023 Redis cache leak, now enforces 30-day auto-deletion and end-to-end encryption for enterprise traffic (Vijayan)
Discrimination	A human review is used in addition to Gemini's anti-bias filters made with ethics scientists (Gemini Help Hub). ChatGPT uses automated reinforcement learning (RLHF) and adversarial "red teaming" to correct biases (GPT-4 System Card)
Data Storage	Gemini leverages Google Cloud's physical and software safeguards, including real-time vulnerability patching (Gemini Apps Privacy Hub) ChatGPT uses Microsoft Azure's SOC 2-compliant storage, with optional regional data isolation for enterprises (Microsoft).

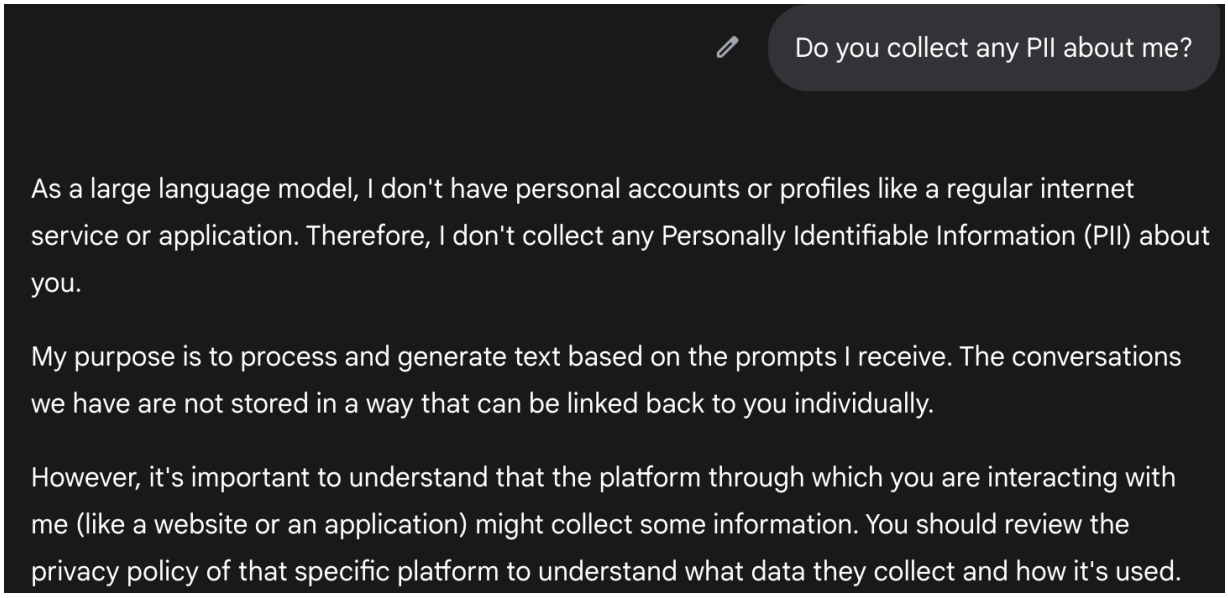
Comparative Analysis

6.1 Transparency and Privacy Comparison

ChatGPT response to prompt



Gemini response to prompt



When asked "Do you collect any PII about me" Gemeni responds with accurate and up-to-date information. ChatGPT claims conversation is not stored, which is untrue and contrary to its privacy policy (OpenAI 2024). However, when further prompted, both LLMs give correct information of its privacy measures that correspond with its privacy policy, and when asked, it correctly describes past issues.

6.2 Data Handling Comparison

Google Gemini requires a Google account (collecting name, birthdate, and gender) and retains conversations by default for 18 months (adjustable to 3-36 months), with a minimum 72-hour retention even when activity tracking is disabled. It collects extensive usage data (IP, location, device info) and warns against entering PII in chats, though filters aim to redact sensitive data during human reviews (Gemeni Privacy Hub 2025)

OpenAI ChatGPT requires only an email and name for account creation, stores free-tier chats for 30 days (deletable sooner), and offers zero-retention for enterprise users. (OpenAI Privacy Policy, 2025). Both advise against sharing PII but differ in defaults: Gemini's longer retention aligns with Google's ecosystem, while OpenAI provides stricter controls for paid tiers.

Gemini shares data broadly across Google services (Workspace, Cloud, Analytics) and marketing partners, using conversations to train models unless disabled (Gemeni Privacy Hub 2025) ChatGPT limits third-party sharing to Microsoft Azure (hosting) and Stripe (payments), with enterprise data isolated from training. Both submit to government requests.

6.3 Overall Comparison

OpenAI implements a tiered privacy system. Free users' chat data is retained for 30 days (unless disabled) and may be used for training, enterprise customers benefit from zero-retention policies and data isolation, and all users can opt out of training data collection (OpenAI 2025).

Google Gemini retains user data by default for 18 months (adjustable between 3 and 36 months) and requires users to be signed into a Google account, collecting personal information such as full name, date of birth, and gender. Conversations are stored for at least 72 hours even if activity tracking is turned off (Gemini Apps Privacy Hub).

However, in terms of full documentation, OpenAI and Google Gemini take different approaches to transparency in their policies. OpenAI provides structured technical documentation like its GPT-4 System Card, which details model capabilities, limitations, and safety evaluations (GPT System Card). Gemini notifies users via its Privacy Hub and login prompts; OpenAI uses in-app banners and detailed privacy policies.

Overall, I believe that OpenAI has more safe and more transparent privacy and security measures. While both models verbally comply with privacy policies, OpenAI's shorter retention, isolated enterprise data, and proactive disclosures make it the safer choice for privacy-conscious users. Gemini's deep Google integration and longer defaults introduce higher inherent risks.

References

California Legislative Information. *SB 362 Delete Act (2023)*. Accessed 29 Apr. 2025. https://leginfo.legislature.ca.gov.

Coralogix. "The Risks of Overreliance on Large Language Models (LLMs)." *Coralogix AI Blog*, 15 Nov. 2023. Accessed 29 Apr. 2025. https://coralogix.com/ai-blog/the-risks-of-overreliance-on-large-language-models-llms/.

European Commission. *Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (AI Act)*. Accessed 29 Apr. 2025. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206.

Gemini Trust Company, LLC. *Privacy Policy*. Gemini. Accessed 29 Apr. 2025. https://www.gemini.com/legal/privacy-policy.

Google. *Data Incident Response Process | Documentation | Google Cloud*. Accessed 29 Apr. 2025. https://cloud.google.com/docs/security/incident-response.

---. *Fact Check Tools API*. Google Developers. Accessed 29 Apr. 2025. https://developers.google.com/fact-check/tools/api.

---. *Gemini Apps Privacy Hub*. Gemini Support. Accessed 29 Apr. 2025. https://support.google.com/gemini/answer/13594961.

---. *Gemini Overview*. Google AI. Accessed 29 Apr. 2025. https://gemini.google/overview/.

---. *Privacy Policy – Privacy & Terms*. Accessed 29 Apr. 2025. https://policies.google.com/privacy.

Information is Beautiful. "The Rise of Generative AI." 2023. Accessed 29 Apr. 2025. https://informationisbeautiful.net/visualizations/the-rise-of-generative-ai-large-language-models-llms-like-chatgpt/.

Microsoft. *Data, Privacy, and Security for Azure OpenAI Service*. Microsoft Learn. Accessed 29 Apr. 2025. https://learn.microsoft.com/en-us/legal/cognitive-services/openai/data-privacy?tabs=azure-portal.

OpenAI. *GPT-4 System Card*. 2023. Accessed 29 Apr. 2025. https://cdn.openai.com/papers/gpt-4-system-card.pdf.

---. "How ChatGPT and Our Foundation Models Are Developed." *OpenAI Help Center*. Accessed 29 Apr. 2025.

https://help.openai.com/en/articles/7842364-how-chatgpt-and-our-foundation-models-are-developed.

---. *Privacy Policy for Non-EEA/UK/Switzerland Users*. Accessed 29 Apr. 2025. https://openai.com/policies/row-privacy-policy/.

SpringsApps. "Large Language Model Statistics and Numbers 2024." *SpringsApps*, 2024. Accessed 29 Apr. 2025. https://springsapps.com/knowledge/large-language-model-statistics-and-numbers-2024.

The Cyber Express. "Google Gemini AI Data Leak: What You Need to Know." Accessed 29 Apr. 2025. https://thecyberexpress.com/google-gemini-ai-data-leak/.

Vijayan, Jai. "ChatGPT Leaks Sensitive User Data; OpenAI Suspects Hack." *Spiceworks*, 27 Mar. 2023. Accessed 29 Apr. 2025. https://www.spiceworks.com/tech/artificial-intelligence/news/chatgpt-leaks-sensitive-user-data-openai-suspects-hack/.