Aalto Good Life Lab, goodlife.aalto.fi
Secure Systems Group, Aalto University

Rongjun Ma, Caterina Maidhof, Juan Carlos Carrillo, Janne Lindqvist, Jose Such

Privacy Perceptions of Custom GPTs by Users and Creators

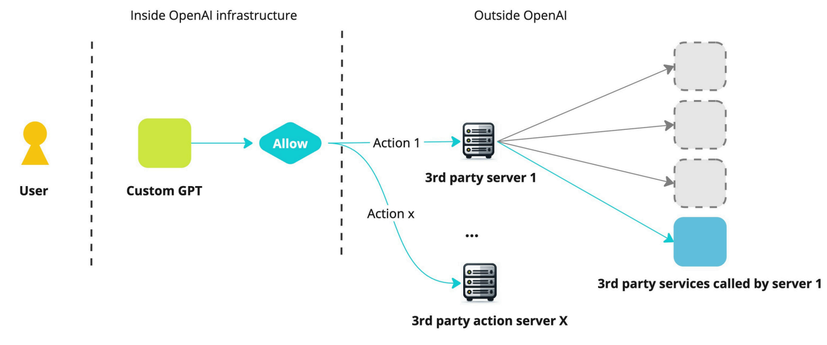
Scan to access the full paper

Background

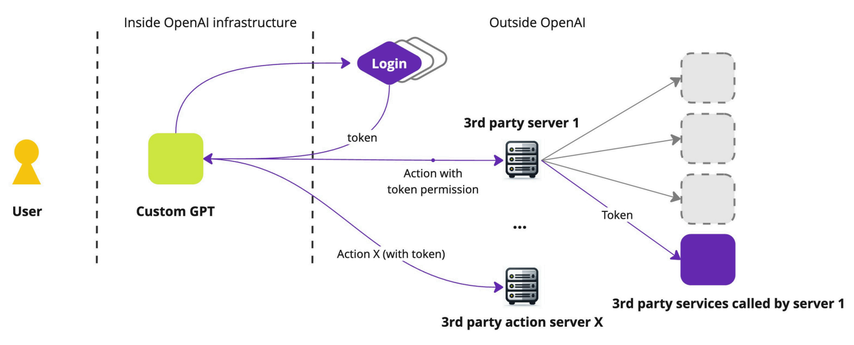
Custom GPTs are personalized applications built on LLMs and hosted on OpenAI's GPT Store.

In Scenario 1, anyone can easily create and publish a basic GPT using simple prompts — no coding required.

More advanced GPTs can also be built by connecting them to third-party services for richer functionality.



Scenario 2: Action-based GPTs



Scenario 3: Login-based GPTs

Method

We conducted semi-structured interviews (N = 23) with participants from diverse backgrounds, including 9 professional GPT creators (who have published GPTs that gained notable popularity), 8 user-creators (who create GPTs primarily for their own personal use), and 6 end users (who use GPTs but do not create them).

Findings

Privacy concerns

Privacy Concerns about GPTs		
Participant	Privacy Concerns	Brief Definition
All	UC1: Concerns about data collection	Transparency, consent, and scope of information gathering
All	UC2: Concern about data processing	Misuse, inaccuracy, or insecure processing of personal data
All	UC3: Concern about dissemination	Unauthorized exposure of information or intrusion into private life
All	UC4: Lack of privacy regulatory guidelines	Insufficient regulations, platform guidelines, and GPT verification
Creators	CC1: Concerns about creator's knowledge	GPT creators' work exploited through reverse engineering

Table 2: An overview of both User Concerns (UC) and Creator Concerns (CC) in the privacy of GPTs.

Practice practices

Privacy Practices to GPTs		
Participants	Privacy Decisions and Behavior	Brief Definition
All	UP1: Self-censorship of the input	Proactive efforts to reduce the amount of personal information shared
All	UP2: GPT evaluation	Users' continuous evaluation of GPTs for privacy and trustworthiness
All	UP3: Minimizing traces of GPT usage	The deliberate separation, deletion, and obfuscation of GPT activities
All	UP4: Accepting privacy risks for features	The compromises users make when balancing privacy concerns with utility
Creators	CP1: Knowledge protection	Actions to protect the creation of knowledge, including configuring settings
Creators	CP2: Creating privacy notices for GPTs	Practices towards protecting other users' (clients, end-users) privacy

Table 3: An overview of both User Practices (UP) and Creator Practices (CP) regarding the privacy of GPTs.

Key takeaways

- Misconceptions about GPT data flow: For example, some users believed that GPT creators could access their conversations, which is not the case in Scenario 1.
- Blurred boundaries between creator and user roles: Unclear role definitions and responsibilities lead to ambiguous privacy practices.

Aalto University

Ma, R., Maidhof, C., Carrillo, J. C., Lindqvist, J., & Such, J. (2025, April). Privacy Perceptions of Custom GPTs by Users and Creators. In Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems (pp. 1-18).

Contact: rongjun.ma@aalto.fi