"Learning Too Much About Me": A User Study on the Security and Privacy of Generative AI Chatbots

Pradyumna Shome Miuyin Marie Yong Wong
Georgia Institute of Technology

Motivation

Generative AI Chatbots like ChatGPT, Copilot, and Gemini have disrupted our means of working. However, is everyone comfortable using them?

What security and privacy concerns do students at a large public US university have with adopting generative AI, and how can we overcome them?

Methodology

Online survey with *N = 86* students, faculty, and staff at the Georgia Institute of Technology, focused on experiences with Generative AI chatbots.

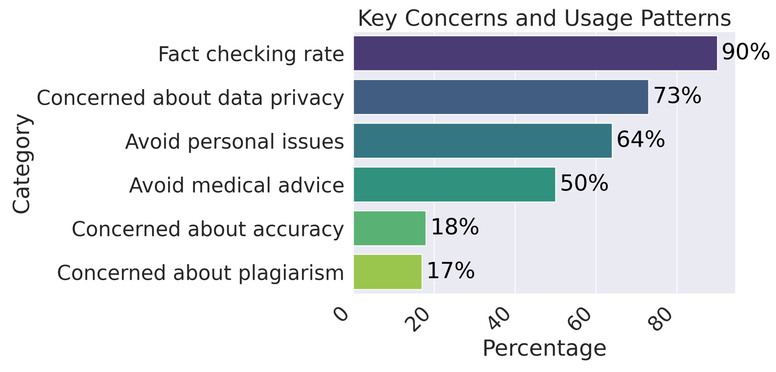
Topics addressed: Technology proficiency, levels of digital privacy concern and that of generative AI, products used, use cases, handling of sensitive queries, and use in academia.

Why look at students?

- Early adopters of technology
- Diverse backgrounds and academic / professional interests
- Soon to enter AI-integrated workplaces

Common Tasks

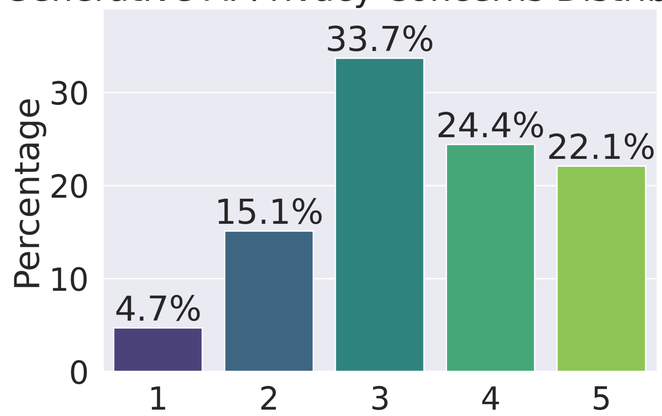
Concerns



College	Privacy Concerns	
	Overall	Chatbots
Computing	3.85	3.78
Design + Liberal Arts + Business	3.60	3.40
Engineering + Sciences	3.33	3.09

Table 1. Privacy Concerns by College (1 = Very Unconcerned. 5 = Very Concerned.)

Generative AI Privacy Concerns Distribution



1 = Very Unconcerned. 5 = Very Concerned.

Notable Trends

- **ChatGPT Plus** Paying users have more use cases.
- **Graduate Students** Fact-check more often than undergrads and get more writing help.
- **Faculty Usage Scenarios** Generating ideas for curriculum and assignments, reviewing literature, and increasing student exposure to AI.

Design Recommendations

- **Privacy Labels** Standard labels for data use policy
- **Privacy Enhancing Technologies** Differential privacy, secure hardware, and secure MPC
- **Prompt Engineering Education** Redacting secrets, asking for steps to validate results provided
- **Customizable Language Models** High integrity training data for regulated domains such as healthcare, finance, and law