

Understanding Users' Security and Privacy Concerns and Attitudes Towards Conversational AI Platforms

Mutahar Ali, Arjun Arunasalam, Habiba Farrukh

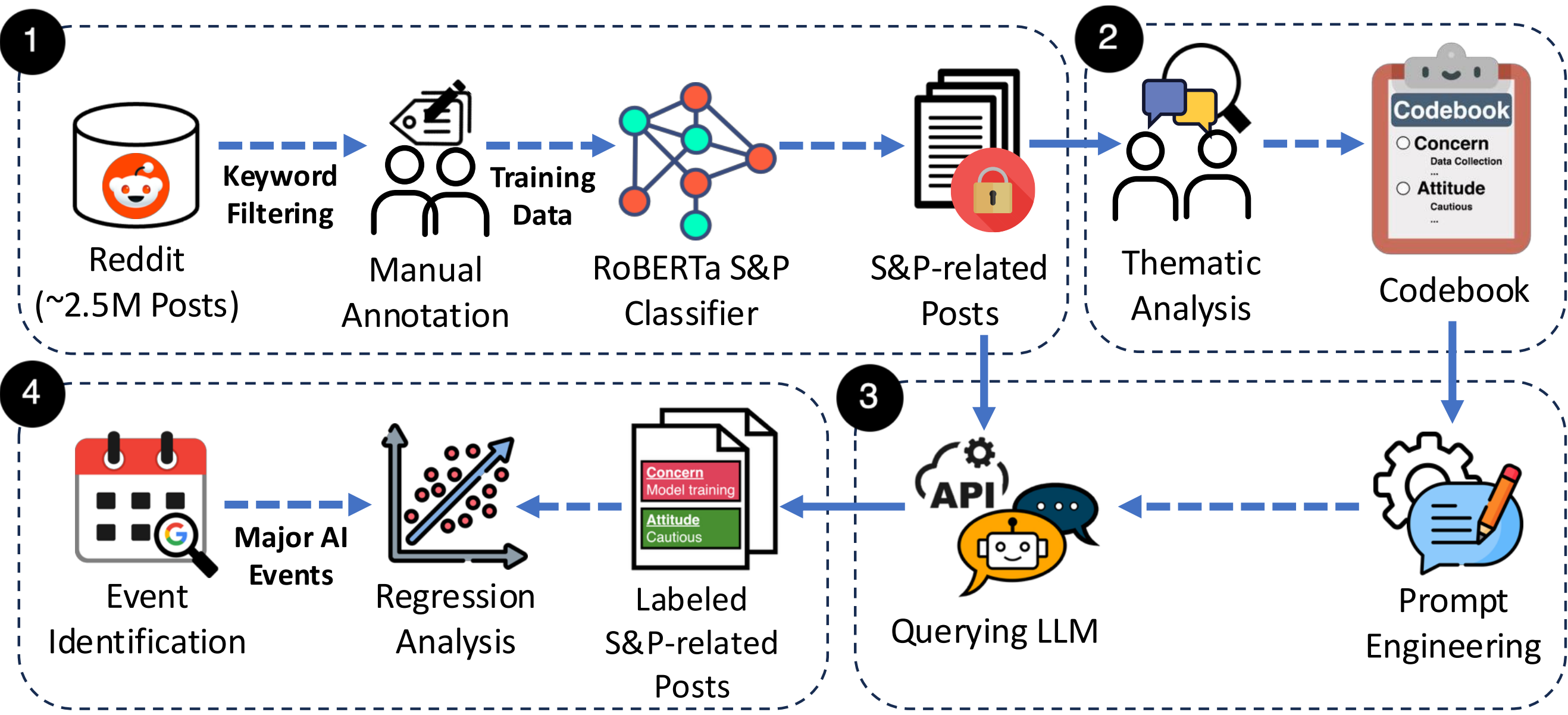


Problem

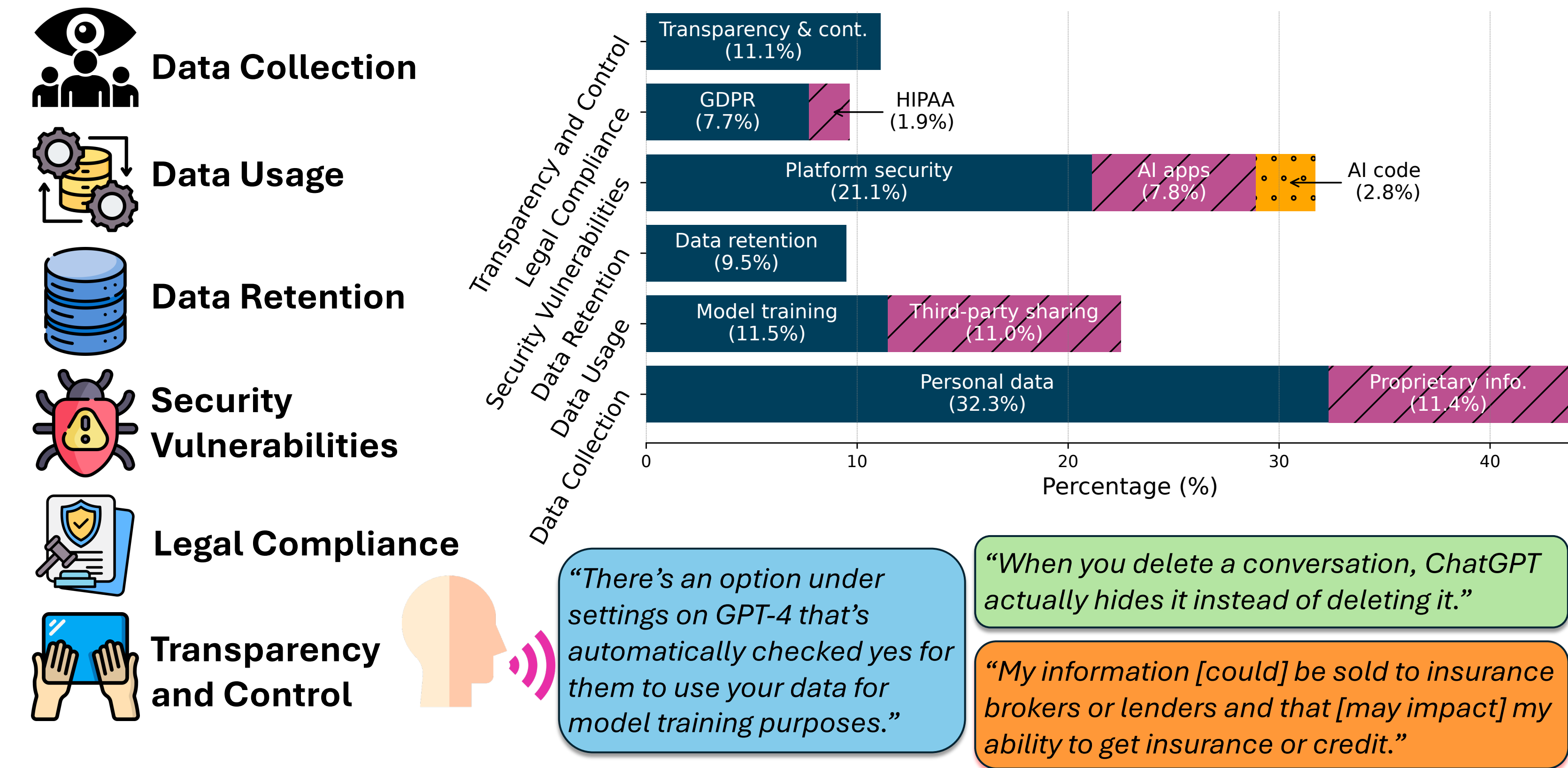
Problem: Prior work mostly focuses on technical threats (e.g., jailbreaking) in conversational AI, overlooking users' perceptions and responses to related S&P risks.

Approach: We use online content analysis of real user discussions on Reddit to surface S&P concerns, behaviors, and attitudes that technical design often overlooks.

Methodology



Concerns



Attitudes



Cautious

- Secure online interactions
- Use local solutions
- Implement guardrails



Privacy-dismissive

- Prioritize benefits over risk
- Criticize privacy regulations
- Dismiss concerns from others



Resigned

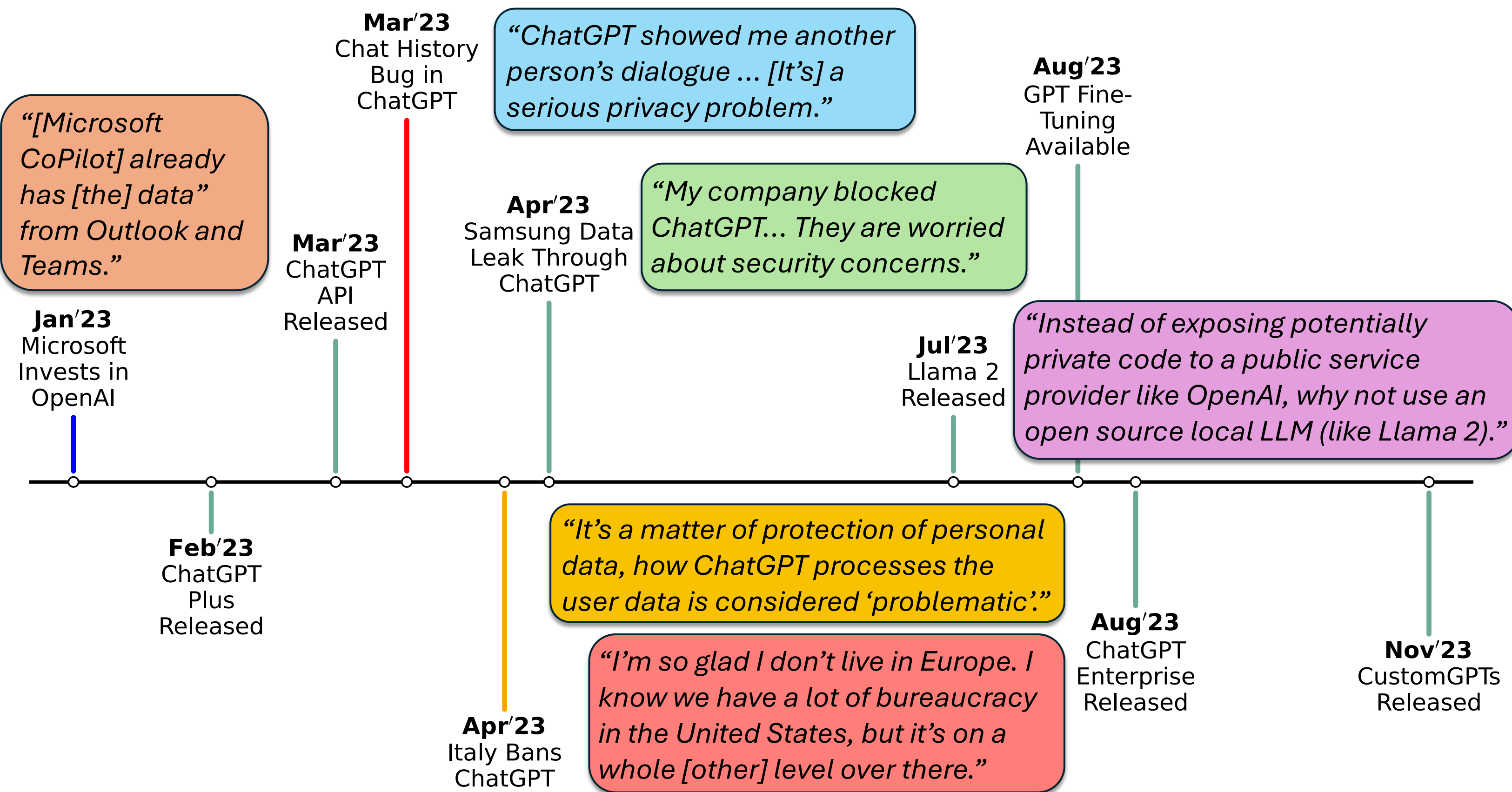
- Accept risk, use anyway



Inquisitive

- Asking for privacy advice
- Consulting the chatbot

Longitudinal Analysis



Recommendations



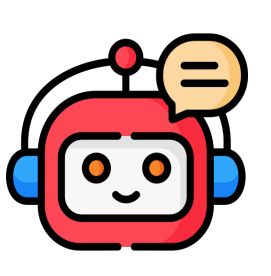
Users

- Exercise Data Controls
- Sanitize Inputs
- Read Privacy Information



Enterprises

- Clear Usage Guidelines
- Security Assessments



Platforms

- Improve Transparency
- Better Data Controls
- Educate Users



Policymakers

- Clear Regulations
- Standardization