ADVANCING USABLE PRIVACY AND DATA MINIMIZATION THROUGH AUTOMATED NEGOTIATION WITH AI AGENTS

A research proposal prepared by JACOB HOPKINS

Data underpins many of today's innovations such as artificial intelligence. The United States has not presented cohesive legislation to safeguard the digital privacy of its citizens. Consequently, the creation of these new technologies has increased the privacy risks for much of the US population. The use of surveillance and data collection systems by public and private entities has increased. The data collected by these systems is often stored in poorly secured databases that are vulnerable to cyber-attacks and data leaks. The current privacy framework, "Notice and Consent", that governs the volunteered data collection scenario has several issues: lack of meaningful transparency, a scaling issue of privacy self-management, and a power imbalance between data subjects and data requesters. Together, these issues underscore the need for new data privacy frameworks and technologies. Therefore, this proposal investigates the design and development of a new privacy-enhancing technology (PET) using automated negotiation techniques. The proposed system will enable data subjects and data requesters to use AI agents to negotiate data practices on their behalf during these collection events. This work focuses on three key objectives to advance negotiation-based PETs: 1) investigating the perspectives of data subjects and data requesters on privacy issues and privacy tools to identify key design requirements for the proposed system; 2) development of a negotiation harness for LLM agents; 3) in-situ testing of the proposed system to validate its design and identify key usability design principles for automated negotiation systems. Collectively, these contributions aim to support the creation of new usable privacy technologies.