Securing Agentic AI

15:00-17:00 pm, January Jan 23rd, 2024
St. Johann Church
Berglistutz 3, 7270 Davos, Switzerland

As artificial intelligence progresses into the era of agentic systems—autonomous agents capable of near-human cognition—the stakes for security and privacy have never been higher. These systems leverage advanced AI techniques, including large language models, machine learning, and reinforcement learning, to operate with minimal human supervision, driving profound transformations across industries. However, the dynamic nature of agentic AI introduces complex challenges for privacy, trust, and individual rights.

This roundtable and panel brings together leaders from academia, industry, and government to explore the intersection of agentic AI and privacy. Discussions will focus on advancing privacy-enhancing technologies (PETs), harmonizing global regulations, and breaking data silos in sectors like healthcare and finance. By addressing key challenges and fostering collaboration, we aim to chart a path for ethical AI development that balances innovation with the protection of individual rights.

Agenda
15:00 - 16:00: Private expert round table discussion
16:00 - 16:10: Transition to public panel
16:15 - 16:45: Public panel summarizing the round table
16:45 - 17:00: Public Q&A

This event is part of the Leading Beyond Boundaries initiative that seeks to provide an opportunity for deep and impactful conversations among scientific, business, and policy leaders during the World Economic Forum. Leading Beyond Boundaries will record the expert round table to form a basis for a public report highlighting the most important insights (under Chatham House Rules).

Leading Beyond Boundaries is grateful to partner with MIT Connection Science, the Harvard Center on the Legal Profession, Stanford HAI, and Wisdom House to make this event possible.