CURRENT TOPICS IN PRIVACY SEMINAR

Marco Paes
(CMU Software Engineering Institute)

Title

Trustworthy Surveillance? Navigating Enterprise Risk and Organizational Privacy

Abstract

The intersection of privacy and insider threat mitigation presents a complex challenge for organizations navigating the demands of security, ethics, and regulatory compliance. As enterprises increasingly adopt advanced monitoring technologies—including AI-driven surveillance and data analytics—the tensions between risk management and the protection of civil liberties grow more pronounced. This seminar will explore the multifaceted relationship between insider threats, privacy preservation, and emerging technologies, while also examining the broader policy and human dimensions of the issue.

Central to the discussion is the balance between effective enterprise risk management and the ethical handling of employee data. The talk will address the spectrum of insider threats, from negligent to malicious actors, and their implications for organizational security. It will also consider the human element of privacy perceptions within enterprise environments, drawing on survey-based research to highlight tensions between security practices and individual rights.

A critical examination of governance frameworks will explore how administrative data can be leveraged for threat analysis while respecting privacy boundaries. The discussion will extend to the role of policy in shaping responsible monitoring practices, including an analysis of privacy legislation such as GDPR and CCPA, as well as proposed policy alternatives to reconcile security needs with civil liberties. Finally, the presentation will evaluate the promise and limitations of privacy-enhancing technologies, including advances in AI and encryption, in addressing insider threats while providing certain privacy guarantees. By synthesizing technical, legal, and managerial perspectives, this presentation aims to move towards accountable and transparent enterprise risk management.

Bio

Marco Paes is a Researcher in the CERT Division of Carnegie Mellon University's Software Engineering Institute, where he specializes in Human-Centered Risk Management in Enterprise Security, and the incorporation of Artificial Intelligence into security and risk management. Previously, he was a Security and Privacy Architect at MITRE, where he worked on the team developing the PANOPTIC Privacy Threat Model. He has instructed courses at George Mason University, Purdue University, and the Software Engineering Institute related to Human Factors, Machine Learning, and Information Security.

TUESDAY, APRIL 15