

**Cara Bloom (MITRE)**

**Title: Privacy Threat Modeling & MITRE PANOPTIC™**

**Abstract:** Threat modeling is a process which can be used to understand potential attacks or adversaries and is essential for holistic risk modeling. As privacy moves from a compliance-based to a risk-based orientation, threat-informed defense will be crucial for privacy management as it has already become for cybersecurity management. Yet, privacy lacks a shared threat language and commonly used threat model. This talk will overview the domain of privacy threat modeling in the context of risk modeling, and present one effort to fill the privacy threat modeling gap: the Pattern & Action Nomenclature Of Privacy Threats In Context (PANOPTIC). PANOPTIC is a data-driven, threat agent-agnostic, attack-oriented taxonomy that breaks individual privacy attacks down into their constituent parts, and can be used for privacy threat assessments, risk modeling, and red teaming.

**Bio:** Cara Bloom is a Senior Privacy Scientist at MITRE, a Federally Funded Research and Development Center, where she leads initiatives on privacy threat modeling, measuring privacy expectations, and Smart City privacy. Cara has provided privacy and cybersecurity expertise on comprehensive risk models, international data protection legislation, and autonomous and connected vehicle technology; and contributed to primary research on data de-identification and self-sovereign identity. She has presented at USENIX, ACM, IEEE, and IAPP conferences. Cara is a graduate of the University of Michigan and received her Master of Science in Information Security Policy from Carnegie Mellon University where she studied with Prof. Lujio Bauer. She currently lives in Pittsburgh with her partner, toothless cat, and retired racehorse.