# Current Topics in Privacy Seminar

CarnegieBosch INSTITUTE

Carnegie Mellon University Privacy Engineering & AI Governance

**Sarah Radway**
Harvard

## Priva-See: Privacy Leakage Through AI-mediated Analysis of Smartphone Data

**Abstract:** Over the past thirty years, the online advertising industry built a large-scale data collection ecosystem, with the goal of tracking a user's online activity to infer their demographics and interests. Traditionally, the ecosystem relied upon the collation and analysis of highly-structured text data like user IP addresses, GPS coordinates, e-commerce purchase histories, and visited URLs. However, recent ML models can parse not only structured text, but also multimedia files and unstructured text inputs—meaning a user's photos, videos, inboxes, and calendars are now ripe for automated analysis. The privacy risks are particularly acute in the context of smartphone apps. A user's phone already acts as a natural collation point for sensitive user information, but users may not understand that permitting an app to, for example, access a user's photo does not just give the app access to the bytes in the photo: the app also receives access to inferences about the user that are enabled by the photo.

To explore these privacy risks, we built Priva-See, an LLM-based inference system for app-collected user data; Priva-See reflects our best understanding of how real-life adtech companies would leverage machine learning to build user profiles. Through an IRB-approved user study, 465 participants deployed Priva-See on their phones; Priva-See made privacy-invasive inferences despite having access to only a subset of a user's data. We see the experience significantly impacted participant willingness to share permissions data moving forward. Based on the observed privacy violations, we suggest changes to how smartphone OSes should gather user consent for data access, to better inform users about downstream data usage capability.

**Bio:** Sarah Radway is a computer science PhD candidate at Harvard University, where she is advised by James Mickens. She is an NSF Graduate Research Fellow and an affiliate of the Berkman Klein Center. Her research involves building systems that are secure and private by design, as well as analyzing emerging technologies in ways that make privacy and security challenges understandable to policymakers and the public. She is particularly interested in privacy and security harms stemming from AI models, and is currently exploring systems-level safety interventions for frontier models.