Carnegie Mellon University
Master of Science in Information Technology

privacy ENGINEERING

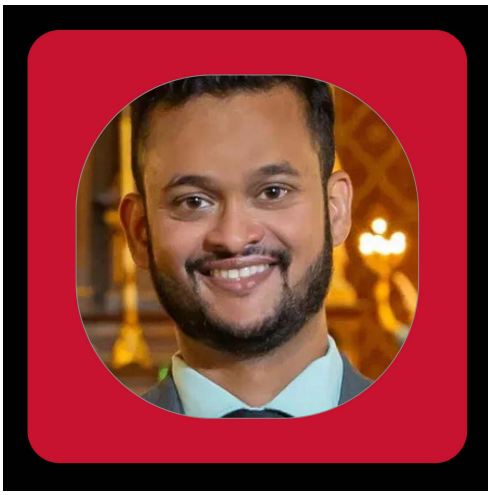
Privacy Seminar

Speaker: Sauvik Das

Title:
Privacy in the age of AI: What's changed and what should we do about it?

Abstract:

Privacy is a core tenet for engineering ethical AI products, but does AI change privacy risk? If so, what barriers do practitioners face in their privacy work for AI products? And, finally, what are ways we might address these barriers? Without an answer to these questions, we cannot hope to better support practitioners in engineering privacy-respecting AI products. To begin answering these questions, I will first present a taxonomy of AI privacy risk where we codify how the unique capabilities and requirements of AI technologies create new privacy risks (e.g., deepfake pornography, physiognomic classifiers) and exacerbate known ones (e.g., surveillance, aggregation). I will then present an interview study with 35 industry practitioners who work on AI products. We asked these practitioners to discuss how they approach privacy for AI products, and found that practitioners often have little awareness of the ways in which AI can create new or exacerbating existing privacy threats, face significant motivational barriers in their privacy work, and have little support for AI-specific privacy work. Finally, I will present our emerging work on "Privacy through Design" — where we are exploring how we might develop turnkey design methods and tools that help practitioners foreground and mitigate privacy risks in their AI design concepts.



Bio:

Dr. Sauvik Das is an Assistant Professor at the Human-Computer Interaction Institute at Carnegie Mellon University where he directs the SPUD (Security, Privacy, Usability and Design) Lab. His work, at the intersection of HCI, AI and cybersecurity, is oriented around answering the question: How can we design systems that empower people with improved agency over their personal data and experiences online? His work has recognized with several awards: a best paper at UbiComp (2013), a distinguished paper at SOUPS (2020), three best paper honorable mentions at CHI (2016, 2017, 2020), a best paper honorable mention at CSCW (2021), and an honorable mention for the NSA's Best Scientific Cybersecurity Paper (2014). He was awarded a NSF CRII in 2018 and a NSF CAREER in 2022 and has otherwise been PI on several other grants from the NSF, Meta, and Oracle. His work has also been covered by the popular press, including features in The Atlantic, The Financial Times, and Dark Reading.

WHEN: February 27th 2023
12:30-1:50pm

WHERE: Hamburg Hall Room 1002

ZOOM LINK:
https://cmu.zoom.us/j/97389172852?pwd=Q2Q5MEE2b29TaS9VeDQ4VHVXckV2dz09