S3D Software and Societal Systems Department

SEMINAR SERIES

Kassem Fawaz

A Glimpse into the Pandora's Box: Demystifying On-Device AI on Instagram and TikTok

Mobile apps have embraced user privacy by moving their data processing to the user's smartphone. Advanced machine learning (ML) models, such as vision models, can now locally analyze user images to extract insights that drive several functionalities. In the first part, this talk describes how we capitalized on this new processing model of locally analyzing user images to analyze two popular social media apps, TikTok and Instagram. Our findings reveal (1) the insights vision models in both apps infer about users from their image and video data and (2) how these models exhibit performance disparities with respect to demographics. The second part of the talk explores users' understandings and perspectives on these models. We conducted a systematic study involving 21 Instagram and TikTok users to understand better how the models influenced their experiences with the apps. We found that participants generally lacked awareness of what insights these models produced and when they were active within the apps. Our findings highlight key challenges and opportunities in improving transparency around machine learning models that process user data locally.

Speaker Bio

Kassem Fawaz is the Grainger Institute of Engineering Associate Professor in the Electrical and Computer Engineering department at the University of Wisconsin–Madison, where he serves as the inaugural associate chair for research. He earned his Ph.D. in Computer Science and Engineering from the University of Michigan. His research interests include the security and privacy of user interactions with AI-powered systems. He was awarded the Caspar Bowden Award for Outstanding Research in Privacy Enhancing Technologies in 2019. He also received the National Science Foundation CAREER award in 2020, the Google Android Security and PrIvacy REsearch (ASPIRE) award in 2021, the Facebook Research Award in 2021, the Chancellor Teaching award in 2022, and the Vilas Associates Award in 2024. His research has been funded by the National Science Foundation, the Federal Highway Administration, and the Defense Advanced Research Projects. His work on privacy has beer featured in several media outlets, such as the BBC, Wired, the Wall Street Journal, the New Scientist, and ComputerWorld.

Wednesday, April 2, 2025
12:00 p.m. – 1:15 p.m
TCS Hall 358

Upcoming S3D Seminar Series Talks

April 16: Deian Stefan*

April 30: danah boyd* (joint with CSS)

***indicates part of the Distinguished Speakers Series**

S3D Software and Societal Systems Department | Carnegie Mellon University School of Computer Science | privacy ENGINEERING