BRIAN JAY TANG

Academic Researcher - AI for Security & Privacy

CONTACT

+1 630-880-3691

bjaytang@umich.edu

https://www.bjaytang.com

github.com/byron123t

linkedin.com/in/bjaytang

Google Scholar

Full CV

SKILLS

Python 7+ yrs

Security 6+ yrs

Privacy 4+ yrs

Computer Vision 4+ yrs

JavaScript 4+ yrs

HCI 3+ yrs

NLP and LLMs 2+ yrs

Flight Experience < 1 yr

AWARDS/GRANTS

Defense University Research Instrumentation Program (DURIP, $300k)

Securing Cyber-Physical System Communication and Control

College of Engineering Fellowship ($90k)

University of Michigan 1st year PhD Fellowship Recipient

Patent Application

Real-Time Protection For Mobile Devices From Shoulder Surfing

EDUCATION

Ph. D. - Computer Science & Engineering — 2021 - ongoing
University of Michigan - Ann Arbor, MI (USA)

B.S. - Computer Sciences — 2017 - 2020
University of Wisconsin - Madison, WI (USA)

WORK EXPERIENCE

Graduate Research Assistant — Sep 21 - May 26
University of Michigan, Ann Arbor (MI)

Researching and creating systems that enhance user privacy. Using compound AI systems to protect online data privacy, personal data, smartphone privacy, autonomous vehicle data privacy, etc.

Undergraduate Research Assistant — Sep 18 - Aug 21
University of Wisconsin, Madison (WI)

Researched security, privacy, and fairness properties of ML systems such as face recognition, image recognition, NLP, and social robots.

Software Engineering Intern — May 19 - Aug 19
Roblox, San Mateo (CA)

Developed enhancements and features for Roblox Studio's script editor.

Software Engineering Intern — May 18 - Aug 18
Optum UHG, Eden Prairie (MN)

Developed data visualization tools for analyzing security vulnerabilities.

SELECTED PUBLICATIONS

Generative Advertising: Risks of Personalizing Ads with LLMs — Submission
ACM CHI Conference on Human Factors in Computing Systems (2025)

Eye-Shield Real-Time Protection of Mobile Device Screen Information from Shoulder Surfing — Published
32nd USENIX Security Symposium (2023)

Detection of Inconsistencies in Privacy Practices of Browser Extensions — Published
44th IEEE Symposium on Security and Privacy (2023)

Fairness Properties of Face Recognition and Obfuscation Systems — Published
32nd USENIX Security Symposium (2023)

Confidant: A Privacy Controller for Social Robots — Published
17th ACM/IEEE International Conference on Human-Robot Interaction (2022)

Face-Off: Adversarial Face Obfuscation — Published
21st Symposium of Privacy Enhancing Technologies (2021)