BRIAN JAY TANG

Computer Science Researcher - AI for Security & Privacy

CONTACT & INFO

+1 630-880-3691
bjaytang@umich.edu
https://www.bjaytang.com
FULL CV
github.com/byron123t
linkedin.com/in/bjaytang
Google Scholar

SKILLS

Python	7+ yrs
Git	7+ yrs
Security	6+ yrs
Privacy	4+ yrs
Computer Vision	4+ yrs
JavaScript	4+ yrs
PyTorch	4+ yrs
Tensorflow	4+ yrs
Numpy	4+ yrs
Flask	4+ yrs
Adversarial ML	4+ yrs
OpenCV	3+ yrs
SQL	3+ yrs
YOLO	3+ yrs
D3.js	3+ yrs
HCI	3+ yrs
BERT	2+ yr
NLP and LLMs	2+ yrs
Fairness	2+ yrs
Playwright	2+ yrs
Redis	2+ yrs
Pandas	2+ yrs
OpenGL	1 yr
Electron	1 yr
Godot	1 yr
LLaMA	1 yr
Flight Experience	< 1 yr
Publications	7
Grant Proposals	7
Citations	127
h-index	6
Chinese	Spoken

SELECTED 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

National Artificial Intelligence Research Resource Pilot (NAIRR, $20k)

Evaluating Privacy and Surveillance Risks of Large Language Models

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)

RESEARCH EXPERIENCE

Graduate Research Assistant — **Sep '21 - ongoing**
University of Michigan, Ann Arbor (MI)

- Led thesis projects on evaluating vision language models (VLMs) and large language models (LLMs) for surveillance and profiling risks.
- Designed Eye-Shield, a real-time phone screen privacy solution.
- Built and evaluated an LLM chatbot integrating personalized product ads.
- Analyzed 47.2k Chrome Web Store extensions, 2.9k online trackers, and 1.4k cookie banners, finding many instances of misleading disclosures and non-compliance.

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

- Developed and evaluated Face-Off, a privacy-preserving attack tool that reduced facial recognition accuracy by 11.91% across face recognition APIs.
- Analyzed anti face recognition systems, revealing demographic disparities in obfuscation performance, finding reduced efficacy for minority groups.

SELECTED CONFERENCE PUBLICATIONS

Ads that Talk Back: Injecting Personalized Advertising into LLM Chatbots — **Submission**
Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (2025), *Acc Rate: 20%*

Eye-Shield: Real-Time Protection of Mobile Device Screen Information from Shoulder Surfing — **Publication**
32nd USENIX Security Symposium (2023), *Acc Rate: 17%*

Detection of Inconsistencies in Privacy Practices of Browser Extensions — **Publication**
44th IEEE Symposium on Security and Privacy (2023), *Acc Rate: 13%*

Fairness Properties of Face Recognition and Obfuscation Systems — **Publication**
32nd USENIX Security Symposium (2023), *Acc Rate: 17%*

Confidant: A Privacy Controller for Social Robots — **Publication**
17th ACM/IEEE International Conference on Human-Robot Interaction (2022), *Acc Rate: 26%*

Face-Off: Adversarial Face Obfuscation — **Publication**
21st Symposium of Privacy Enhancing Technologies (2021), *Acc Rate: 22%*

OTHER EXPERIENCE

Roblox, Software Engineering Intern — **May '19 - Aug '19**

Optum UHG, Software Engineering Intern — **May '18 - Aug '18**