# BRIAN JAY TANG

Computer Science Researcher - AI for Security & Privacy

## CONTACT & INFO

+1 630-880-3691<br>
bjaytang@umich.edu<br>
***https://www.bjaytang.com***<br>
***FULL CV***<br>
github.com/byron123t<br>
linkedin.com/in/bjaytang<br>
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 |
| **React** | 1 yr |
| **LLaMA** | 1 yr |
| **Flight Experience** | < 1 yr |
| **Publications** | 7 |
| **Citations** | 107 |
| **h-index** | 5 |
| **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

**Patent: Real-Time Protection For Mobile Devices From Shoulder Surfing**

U.S. Pat. App. No. 63/468,650-Conf. #8672

## EDUCATION

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

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

## RESEARCH EXPERIENCE

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

- Led thesis projects on evaluating AI systems for surveillance and profiling risks.
- Designed Eye-Shield, a real-time phone privacy solution reduced attack rates to 24.24% for images and 15.91% for text, achieving 43 FPS on iOS.
- Built and evaluated an LLM chatbot integrating personalized product ads, finding users were 19.05% more likely to react positively to products served by GPT-4o.
- 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**<br>
**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

**"It LIED To Me": Implications of Injecting Personalized Advertising into Large Language Model Chatbots** — **Submission**<br>
ACM CHI Conference on Human Factors in Computing Systems (2025), *Acc Rate: 25%*

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

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

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

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

**Face-Off: Adversarial Face Obfuscation** — **Publication**<br>
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**