

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
LLaMA	1 yr
Flight Experience	< 1 yr

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

BRIAN JAY TANG

Research Scientist - AI Security & Privacy - US Citizen

EDUCATION

Ph. D. - Computer Science & Engineering University of Michigan - Ann Arbor, MI (USA)	2021 - ongoing
B.S. - Computer Sciences University of Wisconsin - Madison, WI (USA)	2017 - 2020

RESEARCH EXPERIENCE

Graduate Research Assistant University of Michigan, Ann Arbor (MI)	Sep '21 - ongoing
<ul style="list-style-type: none"><li>Led thesis projects on augmenting vision and memory using vision language models (VLMs) and smart glasses.</li><li>Designed Eye-Shield, a real-time phone screen privacy solution.</li><li>Built and evaluated an LLM chatbot integrating personalized product ads.</li><li>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.</li></ul>	
Undergraduate Research Assistant University of Wisconsin, Madison (WI)	Sep '18 - Aug '21
<ul style="list-style-type: none"><li>Developed and evaluated Face-Off, a privacy-preserving attack tool that reduced facial recognition accuracy by 11.91% across face recognition APIs.</li><li>Analyzed anti face recognition systems, revealing demographic disparities in obfuscation performance, finding reduced efficacy for minority groups.</li></ul>	

SELECTED PUBLICATIONS

Hawkeye: Reading Illegible Text with Vision Language Models IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2026)	In Preparation
Ads that Talk Back: Injecting Personalized Advertising into LLM Chatbots Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (2025)	Revision
Eye-Shield: Real-Time Protection of Mobile Device Screen Information from Shoulder Surfing 32nd USENIX Security Symposium (2023)	Publication
Detection of Inconsistencies in Privacy Practices of Browser Extensions 44th IEEE Symposium on Security and Privacy (2023)	Publication
Confidant: A Privacy Controller for Social Robots 17th ACM/IEEE International Conference on Human-Robot Interaction (2022)	Publication
Face-Off: Adversarial Face Obfuscation 21st Symposium of Privacy Enhancing Technologies (2021)	Publication

OTHER EXPERIENCE

Roblox, Software Engineering Intern	May '19 - Aug '19
Optum UHG, Software Engineering Intern	May '18 - Aug '18