Brian Jay Tang

Updated: 2025-10-10
☎ +1 630-880-3691
✉ bjaytang@umich.edu
Full CV

Researcher, US Citizen
https://www.bjaytang.com/
https://www.linkedin.com/in/bjaytang/
https://github.com/byron123t
https://scholar.google.com/citations?user=pgkhBk8AAAAJ&hl=en

Mission: Seeking a role as a Research Scientist in AI Security, Safety, or Privacy. I wish to ensure that the harms of LLMs are minimized, by ensuring that we explore opt-out methods and unconventional LLM reasoning chains.

Education

Ph.D. Candidate | ***Computer Science and Engineering*** — Fall 2021 – Present
University of Michigan - Ann Arbor — Advised by Kang G. Shin
Thesis: Security and Privacy Challenges with Vision-Language Models and Smart Glasses

Bachelor of Science | ***Major: Computer Science*** — Fall 2017 – Winter 2020
University of Wisconsin - Madison — Advised by Kassem Fawaz, Varun Chandrasekaran, Somesh Jha

Work Experience

Graduate Research Assistant — Fall 2021 – Present
University of Michigan

- Creating automated data collection and annotation methods for training vision-language models to achieve above-human performance on in-the-wild text recognition tasks (>10k samples).
- Designed and patented a real-time software privacy screen, Eye-Shield. Reduced attack success rates from 100% to 24.24% for images and from 77.27% to 15.91% for text, protecting against screen snooping on smartphones. [2]
- Deployed web automation crawler for analysis of 47.2k Chrome extensions, 2.9k online trackers, and 1.4k cookie banners, finding many instances of misleading disclosures and non-compliance. [3]
- Built and evaluated an LLM advertising chatbot using GPT-4o and GPT-3.5. Our user study with 179 participants found that ads influenced 13.07% more participants, with 19.05% more having positive reactions to products. Discovered that serving ads decreases LLM performance on math, reasoning, and reading comprehension tasks by 2-3%. [1]
- Server admin, social organizer, equipment curator, and mentor for the Real-Time Computing Lab.

Undergraduate Research Assistant — Fall 2018 – Spring 2021
University of Wisconsin - Madison

- Explored using physical invariants from LiDAR to improve ML classifier robustness against adversarial attacks.
- Developed an anti face recognition system using projected gradient descent and Carlini-Wagner L2 attacks to protect online photo privacy. [4]. Analyzed demographic fairness properties and latent space of anti face recognition systems.

Software Engineering Intern — Summer 2019
Roblox Corporation

- Designed and implemented production features: autocomplete, smart-cursor movement, and autosuggestion for Roblox Studio's script editor using TDD. Integrated 30 JavaScript Squish tests to auto-validate UI behavior and prevent errors.

Software Engineering Intern — Summer 2018
Optum, UnitedHealth Group

- Designed and implemented an attack-surface visualization that aggregated and normalized 50M+ vulnerability and asset records, produced correlated risk scores, and an interactive dashboard. Presented results to Optum's leadership.

Selected Publications *[Full List and Papers Here (URL)]*

[1] **Brian Tang**, Kaiwen Sun, Noah T. Curran, Florian Schaub, and Kang G. Shin. "Ads that Talk Back: Implications and Perceptions of Injecting Personalized Advertising into LLM Chatbots". In: *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (UbiComp/IMWUT)*. *Acc Rate: 20%*. 2025.

[2] **Brian Tang** and Kang G. Shin. "Eye-Shield: Real-Time Protection of Mobile Device Screen Information from Shoulder Surfing". In: *32nd USENIX Security Symposium*. *Acc Rate: 17%*. 2023.

[3] Duc Bui, **Brian Tang**, and Kang G. Shin. "Detection of Inconsistencies in Privacy Practices of Browser Extensions". In: *44th IEEE Symposium on Security and Privacy*. *Acc Rate: 13%*. 2023.

[4] Varun Chandrasekaran, Chuhan Gao, **Brian Tang**, Kassem Fawaz, Somesh Jha, and Suman Banerjee. "Face-Off: Adversarial Face Obfuscation". In: *21st Privacy Enhancing Technologies Symposium*. *Acc Rate: 22%*. 2021.

Patents

Real-Time Protection For Mobile Devices From Shoulder Surfing [2] Spring 2023
U.S. Pat. App. No. 63/468,650-Conf. #8672 Filed

Selected Grants

An Efficient Real-Time Knowledge Base for Smart Glasses and Smartphones Spring 2025
Samsung (START); Converted to joint proposal w/ Ke Sun, Anhong Guo, Kang G. Shin Granted, $200k, 3-Pages
Ideated Project with Liangkai Liu. Wrote 1/2 of the Proposal.

I-SEE: Intelligent Vehicular Perception and Control Spring 2025
General Motors R&D Granted, $145k, 3-Pages
Ideated Project with Postdoc and 2 Ph.D. Students. Wrote 1/2 of the Proposal.

Evaluating Privacy and Surveillance Risks of Large Language Models Winter 2025
National Artificial Intelligence Research Resource Pilot (NAIRR, $10k) Granted, $10k, 2-Pages
Outlined and Scoped Projects. Wrote Full Proposal.

Securing Cyber-Physical System Communication and Control Spring 2023
Defense University Research Instrumentation Program (DURIP). Granted, $300k, 19-Pages
Initiated and Organized Proposal Structure and 25 Equipment Orders. Wrote 1/3 of the Proposal.

Service

External/Sub Reviewer Spring 2020 – Fall 2025
USENIX Security 2021, PoPETS 2022, NeurIPS 2023, CHI 2024-2025 7 Papers

Poster PC Committee Member Spring 2024 – Spring 2025
IEEE S&P 2024-2025 5 Posters

Co-Chair/Organizer Fall 2025
Prof. Kang G. Shin's Retirement Symposium 87 Attendees
Distinguished Speakers: (Atul Prakash, Mingyan Liu, Farnam Jahanian)

Teaching Experience

Defending Against Deepfakes and Disinformation (Guest Lecturer) Fall 2024
University of Michigan Law School Link to Slides
Taught 30 Law Students About ML, GANs, Deepfakes, Stable Diffusion (1.5 Hours)

Research Interests

Artificial Intelligence: Adversarial ML, Computer Vision, NLP, DNNs, CNNs, (M)LLMs, Agents, VLMs, RAG
Security and Privacy: Usable Privacy, Online Privacy, Face Recognition, Social Privacy, Mobile Privacy, Surveillance
Human-Computer Interaction: User Studies, Social Robotics, Mobile Computing, Real-Time & Cyber-Physical Systems

Skills

Programming: Python, JavaScript, HTML, SQL, GLSL, C++, Kotlin, LaTeX, Linux, Bash
Software Development: GitHub, Perforce, Qt, NginX, Flask, Squish, AWS, Redis, PostgreSQL, OpenGL, d3.js, Electron
Machine Learning: TensorFlow, PyTorch, Keras, Pandas, NumPy, HuggingFace, Transformers, YOLO, Llama, PEFT
Languages: English (Native), Chinese Mandarin (Spoken-Only), Japanese (Beginner), French (Beginner)
Flight Experience: Cessna 172 – 2hrs | Cessna 152 – 2hrs
Hobbies & Interests: Reading, Hiking, Meditation, Camping, Music Production, Videogames, Tabletop RPGs
Clearance Eligibility: Have had prior experience in successfully completing a background investigation, polygraph, and suitability evaluation. An employment offer was extended, but I pursued other opportunities instead.