Brian Jay Tang

Updated: 2025-10-10
☎ +1 630-880-3691
✉ byron123t@gmail.com
✉ bjaytang@umich.edu

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

Thesis: Security and Privacy Challenges with Vision-Language Models and Smart Glasses.
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

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). [9]
- Designed a real-time software privacy film for smartphones, Eye-Shield. Reduced attack rates to 24.24% for images and 15.91% for text, protecting against screen snooping on smartphones. [3]
- Developed various LLM web automation tools and document parsers for auditing data collection activities [10]. Deployed automated analysis of 47.2k Chrome Web Store extensions [4], 2.9k online trackers [7], and 1.4k cookie banners [1], finding many instances of misleading disclosures and non-compliance.
- Built and evaluated an LLM chatbot engine using GPT-4o and GPT-3.5 for serving personalized advertisements. Ran a user study with 179 participants, finding users were 13.07% more influenced by the LLM serving ads compared to the control. Undisclosed advertising led to 19.05% more positive reactions to products. [2]
- Served as server admin, social organizer, equipment curator, and mentoring role for the Real-Time Computing Lab.

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

- Researched fairness properties of face recognition systems. [5]
- Created a controller for social robots to preserve conversational privacy. [6]
- Explored using physical invariants from LiDAR to improve ML classifier robustness against adversarial attacks. [13]
- Developed an anti face recognition system using adversarial attacks to protect online photo privacy. [8]

Software Engineering Intern — Summer 2019
Roblox Corporation

- Designed and implemented production autocomplete, smart-cursor movement, and suggestion features 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.

Top-Tier Publications

[1] **Brian Tang**, Duc Bui, and Kang G. Shin. "Navigating Cookie Consent Violations Across the Globe". In: *34th USENIX Security Symposium*. *Acc Rate: 17%*. 2025. URL: https://arxiv.org/abs/2506.08996.

[2] **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. URL: https://arxiv.org/abs/2409.15436.

[3] **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. URL: https://rtcl.eecs.umich.edu/rtclweb/assets/publications/2023/usenix23-tang.pdf.

[4] 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. URL: https://www.bjaytang.com/pdfs/ExtPrivA.pdf.

[5] Harrison Rosenberg, **Brian Tang**, Kassem Fawaz, and Somesh Jha. “Fairness Properties of Face Recognition and Obfuscation Systems”. In: *32nd USENIX Security Symposium*. *Acc Rate: 17%*. 2023. URL: https://arxiv.org/abs/2108.02707.

[6] **Brian Tang**, Dakota Sullivan, Bengisu Cagiltay, Varun Chandrasekaran, Kassem Fawaz, and Bilge Mutlu. “Confidant: A Privacy Controller for Social Robots”. In: *17th ACM/IEEE International Conference on Human-Robot Interaction*. *Acc Rate: 26%*. 2022. URL: https://arxiv.org/abs/2201.02712.

[7] Duc Bui, **Brian Tang**, and Kang G. Shin. “Do Opt-Outs Really Opt Me Out”. In: *29th ACM Conference on Computer and Communications Security*. *Acc Rate: 18%*. 2022. URL: https://dl.acm.org/doi/10.1145/3548606.3560574.

[8] 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. URL: https://arxiv.org/abs/2003.08861.

Patents

Real-Time Protection For Mobile Devices From Shoulder Surfing [3] — Spring 2023
U.S. Pat. App. No. 63/468,650-Conf. #8672 — Filed

Grants

An Efficient Real-Time Knowledge Base for Smart Glasses and Smartphones — Spring 2025
Samsung (START), Converted to proposal w/ Ke Sun, Anhong Guo, Kang G. Shin — Granted, $200k, 3-Pages
Ideated Project with Postdoc, and Wrote 1 Page.

I-SEE: Intelligent Vehicular Perception and Control — Spring 2025
General Motors R&D — Granted, $55k, 3-Pages
Ideated Project with Postdoc and 2 Ph.D. Students, and Wrote 1 Page.

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, and Wrote Entire Proposal.

Securing Interactions between Driver and Vehicle Using Batteries — Summer 2023
National Science Foundation (NSF) Cloud Credits (Cloudbank) — Granted, $16k, 2-Pages
Wrote 2 Pages and Midterm Reports.

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 3 Sections.

Preprints and Small Papers

[9] **Brian Tang**, Qingyu Zhu, and Kang G. Shin. “Hawkeye: Reading Illegible Text with Vision Language Models”. In: *In Preparation: IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)* (2026).

[10] **Brian Tang** and Kang G. Shin. “Steward: Natural Language Web Automation”. In: *arXiv* (2024). URL: https://arxiv.org/abs/2409.15441.

[11] Noah T. Curran, Minkyoung Cho, Ryan Feng, Liangkai Liu, **Brian Tang**, Pedram Mohajer Ansari, Alkim Domeke, Mert D. Pesé, and Kang G. Shin. “Short: Achieving the Safety and Security of the End-to-End AV Pipeline”. In: *1st Cyber Security in Cars Workshop (CSCS) at CCS*. *Acc Rate: 39%*. 2024. URL: https://arxiv.org/abs/2409.03899v1.

[12] Bulut Gozubuyuk, **Brian Tang**, Mert D. Pesé, and Kang G. Shin. “I Know What You Did (In Your Car) Last Summer: Privacy Implications of Android Automotive OS”. In: *arXiv* (2024). URL: https://arxiv.org/abs/2409.15561.

[13] Varun Chandrasekaran, **Brian Tang**, Nicolas Papernot, Kassem Fawaz, Somesh Jha, and Xi Wu. “Rearchitecting Classification Frameworks For Increased Robustness”. In: *arXiv* (2020). URL: https://arxiv.org/abs/1905.10900.

Honors and Awards

Bloomberg Summer of Puzzles Competition (*Finalist*) Spring 2024
Puzzle Hunt Competition Free Trip to NYC HQ

Travel Grants 2023 – 2025
Rackham, UMich CoE, USENIX $4k

3 Minute Thesis Competition (*Finalist*) Fall 2023
Recovering Privacy and Autonomy in the Era of Large Language Models 1 of 26 Finalists

College of Engineering Fellowship Fall 2021
University of Michigan 1st year PhD fellowship $90k

CVS Health Foundation Program Fall 2017
Scholarship (Outstanding Children of CVS Employees) $5k

Service

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

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

Co-Chair/Organizer Fall 2025
Prof. Kang G. Shin’s Retirement Symposium
87 Attendees, 3 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.