Brian Jay Tang

Updated: 2025-09-18
+1 630-880-3691
byron123t@gmail.com
bjaytang@umich.edu

Research Scientist, 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

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

Research Interests

Thesis: Security and Privacy Challenges in Vision-Language Models
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
Software Systems: Mobile Computing, Real-Time Systems, Cyber-Physical Systems, Databases, AI Systems

Skills

Programming: Python, JavaScript, HTML, SQL, GLSL, C++, Kotlin, Latex
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

Work Experience

Co-Founder — Fall 2023 – Present
PocketEngineer LLC

- Developed an automated system that crawls and stores a company's product spec sheets and tech manuals.
- Built system to transcribe sales calls and generate LLM RAG-based product suggestions and product Q&A in real time.

Graduate Research Assistant — Fall 2021 – Present
University of Michigan

- 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. [7]
- Developed various LLM web automation tools and document parsers for auditing data collection activities [4]. Analyzed 47.2k Chrome Web Store extensions [8], 2.9k online trackers [11], and 1.4k cookie banners [2], finding many instances of misleading disclosures and non-compliance.
- 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. [3]

Research Intern — Spring 2021 – Fall 2021
University of Wisconsin - Madison

- Researched fairness properties of face recognition systems. [9]
- Created a controller for social robots to preserve conversational privacy. [10]

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. [13]
- Developed an anti face recognition system using adversarial attacks to protect online photo privacy. [12]

Software Engineering Intern Summer 2019
Roblox Corporation

- Created core features for Roblox Studio's script editor in a test-driven development setting.
- Developed integrated JavaScript Squish tests for evaluating expected behavior of new UI features.

Software Engineering Intern Summer 2018
Optum, UnitedHealth Group

- Designed and developed data visualization application aggregating 50+ million records from security databases.
- Presented project to audience of Optum's executives, directors, security analysts, and interns.

Publications and Preprints

[1] **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).

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

[3] **Brian Tang**, Kaiwen Sun, Noah T. Curran, Florian Schaub, and Kang G. Shin. "Ads that Talk Back: Injecting Personalized Advertising into LLM Chatbots". In: *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT)*. 2025. URL: https://arxiv.org/abs/2409.15436.

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

[5] 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*. 2024. URL: https://arxiv.org/abs/2409.03899v1.

[6] 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: (2024). URL: https://arxiv.org/abs/2409.15561.

[7] **Brian Tang** and Kang G. Shin. "Eye-Shield: Real-Time Protection of Mobile Device Screen Information from Shoulder Surfing". In: *32nd USENIX Security Symposium*. 2023. URL: https://rtcl.eecs.umich.edu/rtclweb/assets/publications/2023/usenix23-tang.pdf.

[8] 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*. 2023. URL: https://www.bjaytang.com/pdfs/ExtPrivA.pdf.

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

[10] **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*. 2022. URL: https://arxiv.org/abs/2201.02712.

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

[12] Varun Chandrasekaran, Chuhan Gao, **Brian Tang**, Kassem Fawaz, Somesh Jha, and Suman Banerjee. "Face-Off: Adversarial Face Obfuscation". In: *21st Privacy Enhancing Technologies Symposium*. 2021. URL: https://arxiv.org/abs/2003.08861.

[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.

Grant Writing Experience

I-SEE: Intelligent Vehicular Perception and Control Spring 2025
General Motors Submission, $55k

Evaluating Privacy and Surveillance Risks of Large Language Models — Winter 2025
National Artificial Intelligence Research Resource Pilot (NAIRR, $10k) — Granted, $10k

Securing Interactions between Driver and Vehicle Using Batteries — Summer 2023
National Science Foundation (NSF) Cloud Credits (Cloudbank) — Granted, $16k

Securing Cyber-Physical System Communication and Control — Spring 2023
Defense University Research Instrumentation Program (DURIP) — Granted, $300k

Patents

Real-Time Protection For Mobile Devices From Shoulder Surfing [7] — Spring 2023
U.S. Pat. App. No. 63/468,650-Conf. #8672 — Filed

Honors and Awards

Bloomberg Summer of Puzzles Competition (*Finalist*) — Spring 2024
Puzzle Hunt Competition

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

College of Engineering Fellowship — Fall 2021
University of Michigan 1st year PhD fellowship

CVS Health Foundation Program — Fall 2017
Scholarship (Outstanding Children of CVS Employees)

Service

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

Poster Committee Member — Spring 2024 - Spring 2025
IEEE S&P 2024, 2025

Teaching Experience

Defending Against Deepfakes and Disinformation (Guest Lecturer) — Fall 2024
University of Michigan Law School

Presentations and Talks

Navigating Cookie Consent Violations Across The Globe [2] — Aug 2025
Seattle, WA | *USENIX Security Symposium*

Steward: Natural Language Web Automation [4] — Mar 2024
Ann Arbor, MI | *SECRIT Security Reading Group*

Recovering Privacy and Autonomy in the Presence of Language Models — Sept 2023
Ann Arbor, MI | *3 Minute Thesis Finalist Competition (Engineering Graduate Symposium)*

Eye-Shield: Real-Time Protection of Mobile Device Screen Information from Shoulder Surfing [7] — Aug 2023
Anaheim, CA | *USENIX Security Symposium*

Confidant: A Privacy Controller for Social Robots [10] — Mar 2022
The Internet | *ACM/IEEE International Conference on Human-Robot Interaction*

Face-Off: Adversarial Face Obfuscation [12] — Jan 2021
The Internet | *VMWare - NSF: Data Privacy and Edge Computing*

Face-Off: Adversarial Face Obfuscation [12] — July 2021
The Internet | *Proceedings on Privacy Enhancing Technologies Symposium*