

BRIAN JAY TANG

Updated: 2025-03-24

+1 630-880-3691

byron123t@gmail.com

bjaytang@umich.edu

<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*

University of Michigan - Ann Arbor

Fall 2021 – Present

Advised by [Kang G. Shin](#)

Bachelor of Science | *Major: Computer Science*

University of Wisconsin - Madison

Fall 2017 – Winter 2020

Advised by [Kassem Fawaz](#), [Varun Chandrasekaran](#)

RESEARCH INTERESTS

Thesis: Augmenting Vision And Memory With Smart Glasses and VLMs

Artificial Intelligence: Natural Language Processing, Adversarial ML, Computer Vision, NLP, LLM Agents, VLMs, RAG

Security and Privacy: Usable Privacy, Web Privacy, Face Recognition, Social Privacy, Mobile Privacy, Surveillance

Software Systems: Mobile Computing, Real-Time Systems, Cyber-Physical Systems, Databases, AI Systems, Robotics

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

Writing: 5 Top-Tier Security Publications, 7 Papers, 7 Grant Proposals

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, Drumming, Music Production, Game Development

WORK EXPERIENCE

Co-Founder

Fall 2023 – Present

PocketEngineer LLC

- Developed an automated system that parses and stores a company's product spec sheets and manuals.
- Built system to transcribe sales calls and generate LLM RAG 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. [8]
- Developed various LLM web automation tools and document parsers for auditing data collection activities [4]. Analyzed 47.2k Chrome Web Store extensions [9], 2.9k online trackers [12], 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. [5]

Research Intern

Spring 2021 – Fall 2021

University of Wisconsin - Madison

- Researched fairness properties of face recognition systems. [10]
- Created a controller for social robots to preserve conversational privacy. [11]

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. [14]
- Developed an anti face recognition system using adversarial attacks to protect online photo privacy. [13]

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.

Optum, UHG

- 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. "Shoulder Surveillance: AI Shoulder Surfing Attacks With Smart Glasses". In: *In Preparation: ACM CHI conference on Human Factors in Computing Systems* (2026).
- [2] **Brian Tang**, Duc Bui, and Kang G. Shin. "Navigating Cookie Consent Violations Across the Globe". In: *Under Revision: 34th USENIX Security Symposium*. 2025.
- [3] **Brian Tang**, Qingyu Zhu, and Kang G. Shin. "HawkEye: Reading the Illegible with VLMs". In: *In Preparation: The 39th Annual AAAI Conference on Artificial Intelligence* (2025).
- [4] **Brian Tang** and Kang G. Shin. "Steward: Natural Language Web Automation". In: (2024). URL: <https://arxiv.org/abs/2409.15441>.
- [5] **Brian Tang**, Kaiwen Sun, Noah T. Curran, Florian Schaub, and Kang G. Shin. "Ads that Talk Back: Injecting Personalized Advertising into LLM Chatbots". In: *Under Submission: Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*. 2024. URL: <https://arxiv.org/abs/2409.15436>.
- [6] Noah T. Curran, Minkyung 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>.
- [7] 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>.
- [8] **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>.
- [9] 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>.
- [10] 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>.
- [11] **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>.
- [12] 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>.
- [13] 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>.
- [14] 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 EXPERIENCE

An Efficient Real-Time Knowledge Base for Smart Glasses and Smartphones

Samsung Research

Spring 2025
Submission, \$150k**I-SEE: Intelligent Vehicular Perception and Control**

General Motors

Spring 2025
Submission, \$55k

Evaluating Privacy and Surveillance Risks of Large Language Models National Artificial Intelligence Research Resource Pilot (NAIRR, \$20k)	Winter 2025 Granted, \$20k
Securing Interactions between Driver and Vehicle Using Batteries National Science Foundation (NSF) Cloud Credits (Cloudbank)	Summer 2023 Granted, \$16k
Securing Cyber-Physical System Communication and Control Defense University Research Instrumentation Program (DURIP)	Spring 2023 Granted, \$300k

PATENTS

Real-Time Protection For Mobile Devices From Shoulder Surfing [8] U.S. Pat. App. No. 63/468,650-Conf. #8672	Spring 2023 Filed
---	----------------------

HONORS AND AWARDS

Bloomberg Summer of Puzzles Competition (<i>Finalist</i>) Puzzle Hunt Competition	Spring 2024
3 Minute Thesis Competition (<i>Finalist</i>) Recovering Privacy and Autonomy in the Era of Large Language Models	Fall 2023
College of Engineering Fellowship University of Michigan 1st year PhD fellowship	Fall 2021
Qualcomm Innovation Fellowship (<i>Selected Abstract</i>) Autonomous Vehicle Domain Adaptation	Spring 2021
CVS Health Foundation Program Scholarship (Outstanding Children of CVS Employees)	Fall 2017

SERVICE

External/Sub Reviewer USENIX Security 2021, PoPETS 2022, NeurIPS 2023, CHI 2024	Spring 2020 - Fall 2023
Poster Committee Member IEEE S&P 2024	Spring 2024

TEACHING EXPERIENCE

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

PRESENTATIONS AND TALKS

Steward: Natural Language Web Automation [4] Ann Arbor, MI <i>SECURITY Reading Group</i>	Mar 2024
Recovering Privacy and Autonomy in the Presence of Language Models Ann Arbor, MI <i>3 Minute Thesis Finalist Competition (Engineering Graduate Symposium)</i>	Sept 2023
Eye-Shield: Real-Time Protection of Mobile Device Screen Information from Shoulder Surfing [8] Anaheim, CA <i>USENIX Security Symposium</i>	Aug 2023
Confidant: A Privacy Controller for Social Robots [11] The Internet <i>ACM/IEEE International Conference on Human-Robot Interaction</i>	Mar 2022
Face-Off: Adversarial Face Obfuscation [13] The Internet <i>VMWare - NSF: Data Privacy and Edge Computing</i>	Jan 2021
Face-Off: Adversarial Face Obfuscation [13] The Internet <i>Proceedings on Privacy Enhancing Technologies Symposium</i>	July 2021