



BRIAN JAY TANG

+1 630-880-3691

byron123t@gmail.com

bjaytang@umich.edu

CV Last Updated: 2024-03-03

<https://www.linkedin.com/in/bjaytang/>

<https://github.com/byron123t>

<https://scholar.google.com/citations?user=pgkhBk8AAAAJ&hl=en>

<https://www.bjaytang.com/>

EDUCATION

PhD 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: Ensuring Privacy and Autonomy in the Era of Large Language Models

Security and Privacy (S&P): Usable Privacy, Web Privacy, Face Recognition Privacy, Social Privacy, Mobile Privacy

Artificial Intelligence (AI): Natural Language Processing, Adversarial ML, Computer Vision, ML Fairness, AGI

Human-Computer Interaction (HCI): Usable Privacy, Human-Robot Interaction, Digital Safety, AI Ethics

SKILLS

Programming: Python (Expert), JavaScript (Familiar), HTML (Familiar), SQL (Proficient), C++ (Proficient)

Software Development: GitHub, Perforce, Qt, NginX, Flask, Squish, AWS, Redis

Machine Learning: TensorFlow, PyTorch, Pandas, NumPy, D3.js, HuggingFace

Languages: English (Native), Chinese Mandarin (Spoken-Only), Japanese (Elementary), French (Elementary)

Hobbies & Interests: Reading, Drumming, Gaming, Anime, Meditation, Hiking, Camping, Flight Sim

WORK EXPERIENCE

Graduate Research Assistant

University of Michigan

Fall 2021 – Present

- Researching usable AI tools to protect user privacy, analyze online privacy, and regulate data collection/sharing.

Research Intern

University of Wisconsin - Madison

Spring 2021 – Fall 2021

- Researched fairness properties of face recognition and created privacy controller for social robots.

Undergraduate Research Assistant

University of Wisconsin - Madison

Fall 2018 – Spring 2021

- Researched security, privacy, and fairness properties of ML systems (face recognition, image recognition, and NLP).

Software Engineering Intern

Roblox Corporation

Summer 2019

- Created core features for Roblox Studio's script editor in a test-driven development setting.

Software Engineering Intern

Optum, UHG

Summer 2018

- Designed and developed data visualization application aggregating 50+ million records from security databases.

PUBLICATIONS AND PREPRINTS

- [1] **Brian Tang**, Noah T. Curran, Florian Schaub, and Kang G. Shin. "Embedding Advertising in LLM Chatbots: Risks and Ethical Considerations". In: *In Preparation: ACM CHI Conference on Human Factors in Computing Systems*. 2025.
- [2] **Brian Tang**, Duc Bui, and Kang G. Shin. "Navigating Cookie Compliance Across the Globe". In: *Under Submission: Privacy Enhancing Technologies Symposium*. 2024.
- [3] **Brian Tang** and Kang G. Shin. "Steward: Natural Language Web Automation". In: *Under Submission: The 30th Symposium on Operating Systems Principles*. 2024.

- [4] Noah T. Curran, Minkyong Cho, Ryan Feng, Liangkai Liu, **Brian Jay Tang**, Kang G. Shin, Pedram MohajerAnsari, and Mert D. Pesé. "Short: Achieving the Safety and Security of the End-to-End AV Pipeline". In: *Under Submission: ESCAR USA*. 2024.
- [5] **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>.
- [6] 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>.
- [7] 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>.
- [8] **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>.
- [9] 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>.
- [10] 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>.
- [11] Varun Chandrasekaran, **Brian Tang**, Nicolas Papernot, Kassem Fawaz, Somesh Jha, and Xi Wu. "Rearchitecting Classification Frameworks For Increased Robustness". In: (2020). URL: <https://arxiv.org/abs/1905.10900>.

HONORS AND AWARDS

3 Minute Thesis Competition (Finalist) 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 (Selected Abstract) Autonomous Vehicle Domain Adaptation	Spring 2021
CVS Health Foundation Program Scholarship (Outstanding Children of CVS Employees)	Fall 2017

PATENTS

Real-Time Protection For Mobile Devices From Shoulder Surfing[5] U.S. Pat. App. No. 63/468,650-Conf. #8672	Spring 2023 Filed
----------------------------------------------------------------------------------------------------------------------	----------------------

GRANT PROPOSAL EXPERIENCE

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

SERVICE

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

PRESENTATIONS AND TALKS

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 [5] Anaheim, CA <i>USENIX Security Symposium</i>	Aug 2023
Confidant: A Privacy Controller for Social Robots [8] The Internet <i>ACM/IEEE International Conference on Human-Robot Interaction</i>	Mar 2022
Face-Off: Adversarial Face Obfuscation [10] The Internet <i>VMWare - NSF: Data Privacy and Edge Computing</i>	Jan 2021
Face-Off: Adversarial Face Obfuscation [10] The Internet <i>Proceedings on Privacy Enhancing Technologies Symposium</i>	July 2021