Brian Jay Tang
+1 630-880-3691
byron123t@gmail.com
bjaytang@umich.edu

CV Last Updated: 2022-08-23
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 Student | ***Computer Science and Engineering*** — Fall 2021 – Present
University of Michigan - Ann Arbor — GPA: 4.00

Bachelor of Science | ***Major: Computer Science*** — Fall 2017 – Winter 2020
University of Wisconsin - Madison — GPA: 3.53

Research Interests

Security and Privacy (S&P): Usable Privacy, Web Privacy, Face Recognition Privacy, Social Privacy, Mobile S&P
Machine Learning (ML): Adversarial ML, Computer Vision, Natural Language Processing, ML Fairness
Human-Computer Interaction (HCI): Usable Privacy, Human-Robot Interaction, Digital Safety

Work Experience

Graduate Research Assistant — Fall 2021 – Present
University of Michigan

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

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

Software Engineering Intern — Summer 2019
Roblox Corporation

Software Engineering Intern — Summer 2018
Optum, UHG

Research Projects

Real-Time Protection of Mobile Device Screen Information from Shoulder Surfing[1] — Spring 2022
University of Michigan | ***In Review:*** *32nd USENIX Security Symposium 2023*

Do Opt-Outs Really Opt Me Out[5] — Spring 2022
University of Michigan | ***Accepted:*** *29th ACM Conference on Computer and Communications Security 2022* — 18.0% AR

Detection of Inconsistencies in Privacy Practices of Browser Extensions[4] — Winter 2021
University of Michigan | ***Accepted:*** *44th IEEE Symposium on Security and Privacy 2023* — 12.0% AR

Automatic Detection of Cookie Consent Violations[3] — Fall 2021
University of Michigan | ***Target:*** *The Web Conference 2023 (WWW)*

Confidant: A Privacy Controller for Social Robots[2] — Fall 2021
University of Michigan | *17th ACM/IEEE International Conference on Human-Robot Interaction 2022* — 24.8% AR

Fairness Properties of Face Recognition and Obfuscation Systems[8] — Summer 2021
University of Wisconsin - Madison | ***In Review:*** *32nd USENIX Security Symposium 2023*

Face-Off: Adversarial Face Obfuscation[7] — Summer 2020
University of Wisconsin - Madison | *21st Symposium of Privacy Enhancing Technologies 2021* — 19.0% AR

Rearchitecting Classification Frameworks For Increased Robustness[6] — Spring 2019
University of Wisconsin - Madison | *arXiv Preprint*

Personal Projects

Algorithmic Trading Framework — Summer 2019
https://github.com/ramasrirama99/AlgoTradeFramework

Transcend UW Website | ***https://www.transcenduw.com/*** — Spring 2018
University of Wisconsin - Madison | *Transcend UW*

Service

NeurIPS Summer 2022
External/Sub Reviewer

PoPETS Spring 2021
External/Sub Reviewer

USENIX Security Spring 2020
External/Sub Reviewer

Presentations and Talks

Confidant: A Privacy Controller for Social Robots[2] Mar 2022
University of Michigan | *ACM/IEEE International Conference on Human-Robot Interaction*

Face-Off: Adversarial Face Obfuscation[7] Jan 2021
University of Wisconsin - Madison | *VMWare - NSF: Data Privacy and Edge Computing*

Face-Off: Adversarial Face Obfuscation[7] July 2021
The Internet | *Proceedings on Privacy Enhancing Technologies Symposium*

Honors and Awards

WhatsApp Research Awards: Privacy Aware Program Analysis Summer 2022
Submitted proposal under review

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

Qualcomm Innovation Fellowship (Selected Abstract) Spring 2021
Selected abstract on autonomous vehicle domain adaptation

CVS Health Foundation Program Fall 2017
Scholarship for outstanding children of CVS employees

Skills

Languages: English (Native), Chinese Mandarin (Spoken-Only), Japanese (N5), French (A2)
Programming: Python, C++, JavaScript, SQL, HTML
Software Development: GitHub, Perforce, Qt, NginX, Flask, Squish, Flutter, Firebase
Machine Learning: TensorFlow, PyTorch, Pandas, NumPy, D3.js
Hobbies & Interests: Reading, Investing, Gaming, Anime, Skateboarding, Meditation

References

Kang G. Shin kgshin@umich.edu
Professor | EECS Department | University of Michigan - Ann Arbor (734) 763-0391

Kassem Fawaz kfawaz@wisc.edu
Assistant Professor | ECE Department | University of Wisconsin - Madison (608) 890-0529

Somesh Jha jha@cs.wisc.edu
Professor | CS Department | University of Wisconsin - Madison (608)-262-9519

Bilge Mutlu bilge@cs.wisc.edu
Professor | CS Department | University of Wisconsin - Madison (608) 262-6635

Publications—Preprints—Journals

[1] **Brian Tang** and Kang G. Shin. "Real-Time Protection of Mobile Device Screen Information from Shoulder Surfing". In: *In Review: 32nd USENIX Security Symposium 2023*. 2023.

[2] **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.

[3] Duc Bui, **Brian Tang**, and Kang G. Shin. "Automatic Detection of Cookie Consent Violations". In: *In Review: 32nd USENIX Security Symposium 2023*. 2023.

[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 2023*. 2023.

[5] 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*. 2022.

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

[7] 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.

[8] Harrison Rosenberg, **Brian Tang**, Kassem Fawaz, and Somesh Jha. "Fairness Properties of Face Recognition and Obfuscation Systems". In: (2021). arXiv: 2108.02707. URL: https://arxiv.org/abs/2108.02707.