Research Statement - Brian Jay Tang

Motivation

Data privacy has been a significant concern at the forefront of many discussions about emerging technologies. Adequately informing users about the collection and processing of their data remains one of the biggest challenges with online privacy. Currently, data collection practices, the creation of AI technologies using collected data, and autonomous systems are shrouded in opacity. Recently, law frameworks like the GDPR and the CCPA have been created to protect user privacy and ethical AI usage, but regulators are still struggling to keep up with the newest technologies and enforce these protections on a large scale. As a result, a bulk of the responsibility falls on service providers to self-regulate and protect user privacy. Verifying the correctness/consistency/legality of privacy practices relies on a large amount of debugging, network traffic analysis, and consulting with privacy professionals. I aim to automate a large portion of these processes by creating usable tools for all stakeholders.

Prior Projects

In my previous projects, I have explored topics attempting to tackle some of these issues of correctness and transparency in privacy policies by detecting privacy violations in cookie settings [1], browser extensions [2], and opt-out mechanisms [3]. Our research suggested that many websites and platforms were in violation of articles from the GDPR, FTC Act, and CCPA. In the past, I also explored creating privacy tools for users. For example, I created a system to protect users' photos from face recognition [4], and I designed and evaluated a software version of a privacy film for protecting smartphone information from shoulder surfers [5]. I also created a framework allowing social robots to preserver users' privacy in conversations[6]. Finally, I investigated security and fairness concerns related to adversarial ML [7, 8].

Research Interests

As a student with a strong interest in the areas of Usable Security, Usable Privacy, HCI, AI Ethics, and NLP, I believe that collaborating and being exposed to new work environments is incredibly important for conducting broadly impactful research. In my ongoing interests and efforts, I am currently pursuing other research projects in the intersection of ML, HCI, and S&P research to (1) create ML systems that improve users' understanding and control of their privacy and (2) investigate ethical and privacy concerns with emerging AI technologies.

References

[1] D. Bui, **Brian Tang**, and K. G. S. , "Automatic detection of cookie consent violations," in *In Review: 32nd USENIX Security Symposium*, 2023.

[2] D. B. , **Brian Tang**, and K. G. Shin, "Detection of inconsistencies in privacy practices of browser extensions," in *Target: The Web Conference (WWW)*, 2023.

[3] D. Bui, **Brian Tang**, and K. G. Shin, "Do opt-outs really opt me out," in *29th ACM Conference on Computer and Communications Security 2022*, 2022.

[4] V. Chandrasekaran, C. Gao, **Brian Tang**, K. Fawaz, S. Jha, and S. Banerjee, "Face-off: Adversarial face obfuscation," in *21st Privacy Enhancing Technologies Symposium*, 2021. [Online]. Available: `https://arxiv.org/abs/2003.08861`.

[5] **Brian Tang** and K. G. Shin, "Real-time protection of mobile device screen information from shoulder surfing," in *Major Revision: 32nd USENIX Security Symposium*, 2023.

[6] **Brian Tang**, D. Sullivan, B. Cagiltay, V. Chandrasekaran, K. Fawaz, and B. Mutlu, "Confidant: A privacy controller for social robots," in *17th ACM/IEEE International Conference on Human-Robot Interaction*, 2022. [Online]. Available: `https://arxiv.org/abs/2201.02712`.

[7] V. Chandrasekaran, **Brian Tang**, N. Papernot, K. Fawaz, S. Jha, and X. Wu, "Rearchitecting classification frameworks for increased robustness," 2020. arXiv: 1905.10900. [Online]. Available: `https://arxiv.org/abs/1905.10900`.

[8] H. Rosenberg, **Brian Tang**, K. Fawaz, and S. Jha, "Fairness properties of face recognition and obfuscation systems," in *32nd USENIX Security Symposium*, 2023. [Online]. Available: `https://arxiv.org/abs/2108.02707`.