

# Stanley Wu

## CONTACT INFORMATION

Department of Computer Science  
University of Chicago  
Chicago, IL 60637

✉ [stanleywu@cs.uchicago.edu](mailto:stanleywu@cs.uchicago.edu)  
🌐 [www.stanley-wu.com](http://www.stanley-wu.com)

## EDUCATION

### University of Chicago

Started in 2023

*PhD Student, Computer Science*

*Advised by Prof. Ben Y. Zhao and Prof. Heather Zheng*

### Northeastern University

2019 - 2022

*B.S in Computer Science, Minor in Mathematics*

*Graduated Summa Cum Laude*

## PUBLICATIONS

- [1] J. Passananti\*, **S. Wu\***, S. Shan, H. Zheng, BY. Zhao. **Disrupting Style Mimicry Attacks on Video Imagery**, *arXiv preprint* 2024.
- [2] S. Shan, W. Ding, J. Passananti, **S. Wu**, H. Zheng, BY. Zhao. **Nightshade: Prompt-Specific Poisoning Attacks on Text-to-Image Generative Models**, *IEEE Symposium on Security and Privacy (Oakland)* 2024.
- [3] J. Abascal, **S. Wu**, A. Oprea, J. Ullman. **TMI! Finetuned Models Leak Private Information from their Pretraining Data**, *Privacy Enhancing Technologies Symposium (PETS)* 2024.
- [4] M. Jagielski\*, **S. Wu\***, A. Oprea, J. Ullman, R. Geambasu. **How to Combine Membership-Inference Attacks on Multiple Updated Machine Learning Models**, *Privacy Enhancing Technologies Symposium (PETS)* 2023.

## HONORS AND AWARDS

- **National Science Foundation Graduate Research Fellow** (2024)
- **Dean's List, Northeastern University** (2019 - 2022)

## ACADEMIC SERVICE

### Reviewing

- Artifact Evaluation Committee, *USENIX Security*, 2025
- PC, *NeurIPS Workshop: Towards Safe and Trustworthy Agents*, 2024
- Reviewer, *Transactions on Machine Learning Research (TMLR)*, 2024

## PROFESSIONAL EXPERIENCE

### Data Scientist

Jan 2023 - Aug 2023

*Klaviyo Inc.*

### Data Science Intern

May 2022 - Aug 2022

*Klaviyo Inc.*

**Python Software Engineer Co-op**  
*MORSE Corp*

Aug 2021 - Dec 2022

**Data Science Intern**  
*Proofpoint Inc.*

May 2021 - Aug 2021