EMILY WENGER

ewenger@uchicago.edu ◇ emilywenger.com

EDUCATION

Ph.D. in Computer Science, The University of Chicago — Expected 2023

Thesis: Anti-Facial Recognition Technology
Advisors: Ben Y. Zhao and Heather Zheng

M.S. in Computer Science, University of Chicago — 2020

Thesis: Backdoor Attacks Against Facial Recognition in the Physical World

B.S. in Math and Physics, Wheaton College (IL) — 2012-2016

EMPLOYMENT

Research Assistant	The University of Chicago	2018 - Present
Researcher	Meta AI Research	Spring 2022
Research Intern	Meta AI Research	Fall 2021
Researcher	Institute for Defense Analysis (IDA)	Summer 2019
Mathematician	Department of Defense	2016-2018
Research Assistant	Wheaton College Physics Department	2013-2016

PUBLICATIONS

Huiying Li, Shawn Shan, **Emily Wenger**, Jiayun Zhang, Yuanshun Yao, Haitao Zheng, Ben Y. Zhao. *Blacklight: Scalable Defense for Neural Networks against Query-Based Black-Box Attacks.* Proceedings of the 31st USENIX Security Symposium, August 2022.

Emily Wenger, Max Bronckers, Christian Cianfarani, Jenna Cryan, Angela Sha, Haitao Zheng, Ben Y. Zhao. *"Hello, It's Me": Deep Learning-based Speech Synthesis Attacks in the Real World.* Proceedings of the ACM Conference on Computer and Communications Security (CCS), November 2021.

Emily Wenger, Josephine Passananti, Arjun Bhagoji, Yuanshun Yao, Haitao Zheng, Ben Y. Zhao. *Backdoor Attacks Against Deep Learning Systems in the Physical World.* Proceedings of the IEEE / CVF Computer Vision and Pattern Recognition Conference (CVPR), June 2021.

Shawn Shawn*, **Emily Wenger*** (co-first authors), Jiayun Zhang, Huiying Li, Haitao Zheng, Ben Y. Zhao. *Fawkes: Protecting Personal Privacy against Unauthorized Deep Learning Models.* Proceedings of the 29th USENIX Security Symposium, August 2020.

Shawn Shan, **Emily Wenger**, Bolun Wang, Bo Li, Haitao Zheng, Ben Y. Zhao. *Using Honeypots to Catch Adversarial Attacks on Neural Networks.* Proceedings of the ACM Conference on Computer and Communications Security (CCS), November 2020.

PREPRINTS

Emily Wenger*, Mingjie Chen*, Francois Charton, Kristin Lauter. *SALSA: Attacking Lattice Cryptography with Transformers.* In Submission.

Shawn Shan, Wenxin Ding, **Emily Wenger**, Haitao Zheng, Ben Y. Zhao. *Post-breach Recovery: Protection against White-Box Adversarial Examples for Leaked DNN Models.* In Submission.

Emily Wenger, Shawn Shan, Haitao Zheng, Ben Y. Zhao. *SoK: Anti-Facial Recognition Technology.* In Submission.

Emily Wenger*, Francesca Falzon*, Josephine Passananti, Haitao Zheng, Ben Y. Zhao. *Assessing Privacy Risks from Feature Vector Reconstruction Attacks.* In Submission.

Huiying Li, **Emily Wenger**, Ben Y. Zhao, Haitao Zheng. *Piracy Resistant Watermarks for Deep Neural Networks.*

AWARDS AND FELLOWSHIPS

(2021) Harvey Fellowship

(2018) Graduate Fellowship for Stem Diversity (GFSD)

(2018) University of Chicago Neubauer Fellowship

(2016) Wheaton College Chase Senior Merit Scholarship

(2012) National Merit Scholar Finalist

MEDIA COVERAGE

Fawkes: Image Cloaking for Personal Privacy

- Covered by the **MIT Tech Review**: *How to stop AI from recognizing your selfies*
- Covered by the **New York Times**: *This Tool Could Protect Your Photos From Facial Recognition*
- Covered by **Nature Communications**: *Resisting the Rise of Facial Recognition*
- Covered by the **Verge**: *Cloak your photos with this AI privacy tool to fool facial recognition*
- Covered by **The Register (UK)**: *Sick of AI engines scraping your pics for facial recognition? Here's a way to Fawkes them right up*
- Covered by **Die Zeit (Germany)**: *Die unsichtbare Maske (The Invisible Mask)*
- And many more (see here for a full list)

Deep-Learning Based Speech Synthesis Attacks

- Covered by the **New Scientist**: *AI-generated deepfake voices can fool both humans and smart assistants*

INVITED TALKS

"Towards More Realistic Threat Models in Adversarial Machine Learning"

Duke University, April 2022

University of Wisconsin - Madison, April 2022

Northeastern University, May 2022

"Hello, It's Me: Deep Learning-based Speech Synthesis Attacks in the Real World"

"Speech as PII" Lorentz Center Workshop, November 2021

Facebook, October 2021

"Fawkes: Protecting Personal Privacy against Unauthorized Deep Learning Models"

Royal Holloway, University of London, February 2022

Microsoft Research Privacy & Cryptography Group, June 2021

Facebook, October 2020

"Are You a Robot?" Podcast October 2020

The Brave Foundation, August 2020

Boehringer-Ingleheim, August 2020

Infosec Podcast, July 2020

"Piracy Resistant Watermarks for Deep Neural Networks," EE380, **Stanford University**, November 2019

Plenary speaker, **Beyond the Binary Conference** at The University of Hartford, April 2019

TEACHING

Cryptocurrencies (TA)	University of Chicago	Winter 2019
Introductory Cryptography (TA)	WAM Program at the Institute for Advanced Studies	May 2018

WORKSHOPS

Private AI Bootcamp	Microsoft Research	November 2019

STUDENT RESEARCH ADVISING

Emilio Andere	B.S. Computer Science, University of Chicago (exp. 2022)	2022-
Josephine Passananti	B.S. Computer Science, University of Chicago (exp. 2022)	2018-22
Roma Bhattacharjee	B.S. Computer Science, Princeton University (exp. 2025)	2021
Angela Sha	B.S. Computer Science, University of Chicago (exp. 2022)	2020-21
Maximiliaan Bronckers	B.S. Economics/Computer Science, University of Chicago → M.S., Cambridge	2020-21
Talia Gifford	B.S. Physics, University of Chicago (exp. 2022)	2019-21
Esin Onal	B.S. Computer Science, University of Chicago → Deloitte	2020-21

CONFERENCE AND WORKSHOP COMMITTEES

External Revewier, *ACM Conference on Computer and Communications Security (CCS)*	2022
PC Member, *Workshop on Dependable and Secure Machine Learning (DSML)* (co-located with DSN)	2022
Reviewer, *IEEE Transactions on Pattern Analysis and Machine Intelligence*	2021-present

LEADERSHIP

Founding Member and Content Fellow, AI & Faith (2020-present)

Curatorial team member for "Traced & Traced" exhibit, Science Gallery Detroit (2020-2021)

Student Organizer, Graduate Research Opportunities for Women (GROW) Conference (2020)

Member of UChicago CS student leadership team (2020-2021)

Student representative for UChicago CS graduate admissions committee (2019-2020)

OUTREACH AND VOLUNTEERISM

Math tutor for Hope Scholars after-school program (Woodlawn, Chicago)