EMILY WENGER

ewenger@uchicago.edu ⋄ emilywenger.com

EDUCATION

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

Area of focus: machine learning security and privacy
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
Research Intern	Facebook 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

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.* CCS 2021.

Emily Wenger, Josephine Passananti, Arjun Bhagoji, Yuanshun Yao, Haitao Zheng, Ben Y. Zhao. *Backdoor Attacks Against Facial Recognition in the Physical World.* CVPR 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.* 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.* ACM CCS, November 2020

PREPRINTS

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

Huiying Li, Shawn Shan, **Emily Wenger**, Jiayun Zhang, Yuanshun Yao, Haitao Zheng, Ben Y. Zhao. *Blacklight: Defending Black-Box Adversarial Attacks on Deep Neural Networks.* In Submission.

MEDIA COVERAGE

Fawkes: Image Cloaking for Personal Privacy

- Covered by the **MIT Tech Review**: *How to stop AI from recognizing your selfies* `https://www.technologyreview.com/2021/05/05/1024613/stop-ai-recognizing-your-face-selfies-machine-learning-facial-recognition-`
- Covered by the **New York Times**: *This Tool Could Protect Your Photos From Facial Recognition* `https://www.nytimes.com/2020/08/03/technology/fawkes-tool-protects-photos-from-facial-recognition.html`
- Covered by **Nature Communications**: *Resisting the Rise of Facial Recognition* `https://www.nature.com/articles/d41586-020-03188-2`
- Covered by **MIT Tech Review**: *How to Stop AI from Recognizing Your Selfies* `https://www.technologyreview.com/2021/05/05/1024613/stop-ai-recognizing-your-face-selfies-machine-learning-facial-recognition-`

- Covered by the **Verge**: *Cloak your photos with this AI privacy tool to fool facial recognition* https://www.theverge.com/2020/8/4/21353810/facial-recognition-block-ai-selfie-cloaking-fawkes
- Covered by **The Register (UK)**: *Sick of AI engines scraping your pics for facial recognition? Here's a way to Fawkes them right up* https://www.theregister.com/2020/07/22/defeat_facial_recognition/
- Covered by **Die Zeit (Germany)**: *Die unsichtbare Maske (The Invisible Mask)* https://www.zeit.de/digital/datenschutz/2020-08/gesichtserkennung-fawkes-software-app-algorithmus-ki-bildanalyse
- And many more (see http://sandlab.cs.uchicago.edu/fawkes/ for a full list)

INVITED TALKS

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

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 Colloquium, **Stanford University**, November 2019

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

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

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

Roma Bhattacharjee	B.S. Computer Science, Princeton University (exp. 2025)	Summer 2021
Josephine Passananti	B.S. Computer Science, University of Chicago (exp. 2022)	2018 - Present
Angela Sha	B.S. Computer Science, University of Chicago (exp. 2022)	2020 - Present
Maximiliaan Bronckers	B.S. Economics & Computer Science, University of Chicago (2021)	2020 - 2021
Talia Gifford	B.S. Physics, University of Chicago (exp. 2022)	2019 - 2021
Esin Onal	B.S. Computer Science, University of Chicago (2021)	2020 - 2021

LEADERSHIP

Founding Member, AI & Faith

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

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)