

# MICAH GOLDBLUM

## EDUCATION

---

**University of Maryland**  
Ph.D. in Mathematics

*September 2014 - May 2020*

**University of Maryland**  
B.Sc. in Mathematics

*September 2010 - May 2014*

## EMPLOYMENT

---

**University of Maryland**  
Postdoctoral Researcher (Advised by Professor Tom Goldstein)

*May 2020 - Present*

**University of Maryland**  
Graduate Researcher (Co-Advised by Professors Wojciech Czaja and Tom Goldstein)

*March 2017 - May 2020*

**National Institute of Health**  
Research Intern

*June 2018 - September 2018*

## RESEARCH INTERESTS

---

- Further the understanding of machine learning in the data scarce regime.
- Explore security and robustness properties of neural networks.
- Design deep learning algorithms which resist data poisoning and adversarial attacks.
- Understand the mathematical underpinnings of modern neural networks.

## PUBLICATIONS

---

**Just How Toxic is Data Poisoning? A Unified Benchmark for Backdoor and Data Poisoning Attacks** *2021*

Avi Schwarzschild, **Micah Goldblum**, Arjun Gupta, John P Dickerson, Tom Goldstein  
*International Conference on Machine Learning (ICML) 2021*

**Data Augmentation for Meta-Learning** *2021*

Renkun Ni, **Micah Goldblum**, Amr Sharaf, Kezhi Kong, Tom Goldstein  
*International Conference on Machine Learning (ICML) 2021*

**The Intrinsic Dimension of Images and Its Impact on Learning** *2021*

Phil Pope, Chen Zhu, Ahmed Abdelkader, **Micah Goldblum**, Tom Goldstein  
*International Conference on Learning Representations (ICLR) 2021 (Spotlight Talk)*

**LowKey: Leveraging Adversarial Attacks to Protect Social Media Users from Facial Recognition** *2021*

Valeriia Cherepanova, **Micah Goldblum**, Harrison Foley, Shiyuan Duan, John P Dickerson, Gavin Taylor, Tom Goldstein  
*International Conference on Learning Representations (ICLR) 2021*

**Strong Data Augmentation Sanitizes Poisoning and Backdoor Attacks Without an Accuracy Tradeoff** *2021*

Eitan Borgnia, Valeriia Cherepanova, Liam Fowl, Amin Ghiasi, Jonas Geiping, **Micah Goldblum**, Tom Goldstein, Arjun Gupta  
*International Conference on Acoustics, Speech, and Signal Processing (ICASSP) 2021*

**Robust Few-Shot Learning: A Meta-Learning Approach** *2020*

**Micah Goldblum**, Liam Fowl, Tom Goldstein  
*Advances in Neural Information Processing Systems (NeurIPS) 2020*

**Unraveling Meta-Learning: Understanding Feature Representations for Few-Shot Tasks** *2020*

**Micah Goldblum**, Steven Reich, Liam Fowl, Renkun Ni, Valeriia Cherepanova, Tom Goldstein  
*International Conference on Machine Learning (ICML) 2020*

**Truth or backpropaganda? An empirical investigation of deep learning theory** *2020*

**Micah Goldblum**, Jonas Geiping, Avi Schwarzschild, Michael Moeller, Tom Goldstein  
*International Conference on Learning Representations (ICLR) 2020 (Spotlight Talk)*

- Adversarially Robust Distillation** 2020  
 Micah Goldblum, Liam Fowl, Soheil Feizi, Tom Goldstein  
*Proceedings of the AAAI Conference on Artificial Intelligence*. Vol. 34.
- WITCHcraft: Efficient PGD attacks with random step size** 2020  
 Ping-Yeh Chiang, Jonas Geiping, Micah Goldblum, Tom Goldstein, Renkun Ni, Steven Reich, Ali Shafahi  
*International Conference on Acoustics, Speech, and Signal Processing (ICASSP) 2020*.
- Sheared multi-scale weight sharing for multi-spectral superresolution** 2019  
 Micah Goldblum, Liam Fowl, Wojciech Czaja  
*Algorithms, Technologies, and Applications for Multispectral and Hyperspectral Imagery XXV*. Vol. 10986. International Society for Optics and Photonics, 2019.

## PREPRINTS

---

- Adversarial Examples Make Strong Poisons** 2021  
 Liam Fowl, Micah Goldblum, Ping-yeh Chiang, Jonas Geiping, Wojtek Czaja, Tom Goldstein  
*arXiv preprint arXiv:2106.10807*
- MetaBalance: High-Performance Neural Networks for Class-Imbalanced Data** 2021  
 Arpit Bansal, Micah Goldblum, Valeriia Cherepanova, Avi Schwarzschild, C. Bayan Bruss, Tom Goldstein  
*arXiv preprint arXiv:2106.09643*
- Sleeper Agent: Scalable Hidden Trigger Backdoors for Neural Networks Trained from Scratch** 2021  
 Hossein Souri, Micah Goldblum, Liam Fowl, Rama Chellappa, Tom Goldstein  
*arXiv preprint arXiv:2106.08970*
- Can You Learn an Algorithm? Generalizing from Easy to Hard Problems with Recurrent Networks** 2021  
 Avi Schwarzschild, Eitan Borgnia, Arjun Gupta, Furong Huang, Uzi Vishkin, Micah Goldblum, Tom Goldstein  
*arXiv preprint arXiv:2106.04537*
- SAINT: Improved Neural Networks for Tabular Data via Row Attention and Contrastive Pre-Training** 2021  
 Gowthami Somepalli, Micah Goldblum, Avi Schwarzschild, C. Bayan Bruss, Tom Goldstein  
*arXiv preprint arXiv:2106.01342*
- What Doesn't Kill You Makes You Robust(er): Adversarial Training against Poisons and Backdoors** 2021  
 Jonas Geiping, Liam Fowl, Gowthami Somepalli, Micah Goldblum, Michael Moeller, Tom Goldstein  
*arXiv preprint arXiv:2102.13624*
- The Uncanny Similarity of Recurrence and Depth** 2021  
 Avi Schwarzschild, Arjun Gupta, Amin Ghiasi, Micah Goldblum, Tom Goldstein  
*arXiv preprint arXiv:2102.11011*
- Preventing Unauthorized Use of Proprietary Data: Poisoning for Secure Dataset Release** 2021  
 Liam Fowl, Ping-yeh Chiang, Micah Goldblum, Jonas Geiping, Arpit Bansal, Wojtek Czaja, Tom Goldstein  
*arXiv preprint arXiv:2103.02683*
- Technical Challenges for Training Fair Neural Networks** 2021  
 Valeriia Cherepanova, Vedant Nanda, Micah Goldblum, John P. Dickerson, Tom Goldstein  
*arXiv preprint arXiv:2102.06764*
- Adversarial Attacks on Machine Learning Systems for High-Frequency Trading** 2020  
 Micah Goldblum, Avi Schwarzschild, Naftali Cohen, Tucker Balch, Ankit B. Patel, Tom Goldstein  
*arXiv preprint arXiv:2002.09565*
- Dataset Security for Machine Learning: Data Poisoning, Backdoor Attacks, and Defenses** 2020  
 Micah Goldblum, Dimitris Tsipras, Chulin Xie, Xinyun Chen, Avi Schwarzschild,

Dawn Song, Aleksander Madry, Bo Li, Tom Goldstein  
*arXiv preprint arXiv:2012.10544*

**Random Network Distillation as a Diversity Metric for Both Image and Text Generation** 2020  
Liam Fowl, Micah Goldblum, Arjun Gupta, Amr Sharaf, Tom Goldstein  
*arXiv preprint arXiv:2010.06715*

**An Open Review of OpenReview: A Critical Analysis of the Machine Learning Conference Review Process** 2020  
David Tran, Alex Valtchanov, Keshav Ganapathy, Raymond Feng, Eric Slud, Micah Goldblum, Tom Goldstein  
*arXiv preprint arXiv:2010.05137*

**Prepare for the Worst: Generalizing across Domain Shifts with Adversarial Batch Normalization** 2020  
Manli Shu, Zuxuan Wu, Micah Goldblum, Tom Goldstein  
*arXiv preprint arXiv:2009.08965*

**Understanding Generalization through Visualizations** 2019  
Huang, W. Ronny, Zeyad Emam, Micah Goldblum, Liam Fowl, Justin K. Terry, Furong Huang, Tom Goldstein  
*arXiv preprint arXiv:1906.03291*

---

## TEACHING EXPERIENCE

### Primary Instructor:

- Differential Equations
- Statistics
- Probability Theory

### Teaching Assistant:

- Linear Algebra
- Calculus

---

## MEDIA APPEARANCES

**Wie ich die Kontrolle über mein Gesicht verlor** 2021  
*Der Spiegel Magazine*

**Cómo evitar que los sistemas de reconocimiento facial descifren las fotos de tus redes** 2021  
*El País*

**LowKey cool: This web app will tweak your photos to flummox facial-recognition systems, apparently** 2021  
*The Register*

---

## COMMUNITY INVOLVEMENT

- Chair of the organizing committee for the NeurIPS 2020 Workshop on Dataset Curation and Security.
- Reviewed papers for conferences and journals including NeurIPS, ICML, and TPAMI.