Dr. rer. nat. Jonas Geiping

Full Name	Jonas Alexander Geiping	Offine Phone	+1 301 405 2671
Address	8125 Paint Branch Drive	Email	jgeiping@umd.edu
	20742 College Park, MD	Permanent Email	jonas.geiping@gmail.com
	United States	Website	jonasgeiping.github.io
Date of Birth	25th of March 1992, Berlin	Google Scholar	206vNCEAAAAJ

Biography

My background is in Mathematics, more specifically in mathematical optimization and its applications to deep learning. My research agenda is based on understanding machine learning constructively, testing theory, privacy and security directly, and designing more secure and private ML systems, to move our fundamental understanding of ML forward.

Experience

Sept. 2021 - University of Maryland, College Park
Postdoctoral Researcher

Research into privacy and security in machine learning and deep learning as a science, from an optimization perspective with applications in federated learning, stochastic training of neural networks and topics in security.

May 2021
July 2021 University of Siegen
Postdoctoral Associate

Postdoctoral Research: optimization and generalization in deep learning.

Oct. 2016
March 2021 University of Siegen
Research Associate

Research in the fields of mathematical optimization, machine learning and computer vision with Prof. Michael Möller with work done in non-convex composite optimization, convex relaxations, optimization for computer vision, learning of optimization objectives and bi-level optimization problems in security.

Aug. 2019
Nov. 2019 University of Maryland, College Park
Short-Term Scholar Exchange Visitor

Visiting the group of Prof. Tom Goldstein, joint research in topics of data poisoning for machine learning models and empirical evaluation of deep learning theory.

Oct 2014 -
June 2016 University of Münster (WWU) - Cells-in-Motion Cluster of Excellence
Research Assistant

CiM flexible fund project *FF-2014-06* - " Analysis of cell-cell interactions during neuronal migration in the developing cortex by live cell imaging and cell shape quantification"

Education

Dec 2016 - April 2021 University of Siegen
Dr. rer. nat. (PhD), Computer Science

Advisor: *Prof. Michael Möller*
Thesis: *Modern Optimization Techniques in Computer Vision - From Variational Models to Machine Learning Security*

Oct 2014 - Sept. 2016 Westfälische-Wilhelms Universität Münster
M.Sc., Mathematics

Advisor: Prof. Martin Burger
Thesis: *Image Analysis of Neural Tissue Development: Variational Methods for Segmentation and 3D-Reconstruction from large pinhole confocal fluorescence microscopy*

Oct 2011 - Sept. 2014 Westfälische-Wilhelms Universität Münster
B.Sc., Mathematics

Advisor: Prof. Martin Burger
Thesis: *Topology-Preserving Segmentation Methods and Application to Mitotic Cell Tracking*

Selected Publications

Jonas Geiping*, Hartmut Bauermeister*, Hannah Dröge*, and Michael Moeller. Inverting Gradients - How easy is it to break privacy in federated learning? In *Advances in Neural Information Processing Systems*, volume 33, December 2020. URL https://proceedings.neurips.cc//paper_files/paper/2020/hash/c4ede56bbd98819ae6112b20ac6bf145-Abstract.html.

Jonas Geiping*, Liam H. Fowl*, W. Ronny Huang, Wojciech Czaja, Gavin Taylor, Michael Moeller, and Tom Goldstein. Witches' Brew: Industrial Scale Data Poisoning via Gradient Matching. In *International Conference on Learning Representations*, April 2021a. URL https://openreview.net/forum?id=01olnfLIbD.

Jonas Geiping, Micah Goldblum, Phil Pope, Michael Moeller, and Tom Goldstein. Stochastic Training is Not Necessary for Generalization. In *International Conference on Learning Representations*, September 2021b. URL https://openreview.net/forum?id=ZBESeIUB5k.

Yuxin Wen*, **Jonas Geiping***, Liam Fowl, Micah Goldblum, and Tom Goldstein. Fishing for User Data in Large-Batch Federated Learning via Gradient Magnification. In *Proceedings of the 39th International Conference on Machine Learning*, pages 23668–23684. PMLR, June 2022. URL https://proceedings.mlr.press/v162/wen22a.html.

Recent Invited Talks

Oct 2022 Qualcomm AI Research - DistributedML Seminar
Privacy and Security Analysis in Federated Learning

May 2022 Federated Learning One World Seminar
New Threat Models for Privacy Attacks in Federated Learning

Feb 2022 RIKEN AIP - 5th TrustML Young Scientist Seminar
Attacks on Privacy in Federated Learning Scenarios

June 2021 Google ML privacy testing team
Inverting Gradients - A Privacy Question for Federated Learning?

Teaching

I have prepared and discussed exercises and homework in deep learning, convex optimization and variational image processing while at the University of Siegen, and have held lectures a number of times as a substitute. These courses were first developed during this time and I have learned a lot from being part of their conceptualization. I have also taught as a teaching assistant in numerical linear algebra at the University of Münster.
At the University of Maryland I have advised and helped to advise a number of graduate students as postdoctoral researcher, for example Arpit Bansal for Bansal et al. [2022], Yuxin Wen in Wen et al. [2022], Wen et al. [2022,a,b], Pedro Sandoval-Segura in Sandoval-Segura et al. [2022a,b] and Gowthami Somepalli in Somepalli et al. [2022].

Community Work

I have reviewed and continue to review for the large machine learning conferences and journals and computer vision conferences. I have been named "Top Reviewer" at the Thirty-sixth Conference on Neural Information Processing Systems (NeurIPS 2022) and "Highlighted Reviewer" at the Tenth International Conference on Learning Representations (ICLR 2022).
I am a proponent of openly available publications and code. All of my research is available as preprints on arxiv.org and our code implementations have accrued consistent interest from the community, measured in several hundred stars and forks on github. Implementations can be found for code written predominantly by me at https://github.com/JonasGeiping/ and for student publications on their respective pages.

Full List of Publications

Eitan Borgnia‡, Valeriia Cherepanova‡, Liam Fowl‡, Amin Ghiasi‡, **Jonas Geiping‡**, Micah Goldblum‡, Tom Goldstein‡, and Arjun Gupta‡. Strong Data Augmentation Sanitizes Poisoning and Backdoor Attacks Without an Accuracy Tradeoff. In *ICASSP 2021 - 2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pages 3855–3859, June 2021a. doi: 10.1109/ICASSP39728.2021.9414862.

Eitan Borgnia, **Jonas Geiping***, Valeriia Cherepanova*, Liam Fowl*, Arjun Gupta*, Amin Ghiasi*, Furong Huang, Micah Goldblum, and Tom Goldstein. DP-InstaHide: Provably Defusing Poisoning and Backdoor Attacks with Differentially Private Data Augmentations. In *ICLR 2021 Workshop on Security and Safety in Machine Learning Systems*, March 2021b. URL http://arxiv.org/abs/2103.02079.

Ping-Yeh Chiang‡, **Jonas Geiping‡**, Micah Goldblum‡, Tom Goldstein‡, Renkun Ni‡, Steven Reich‡, and Ali Shafahi‡. Witchcraft: Efficient PGD Attacks with Random Step Size. In *ICASSP 2020 - 2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pages 3747–3751, May 2020. doi: 10.1109/ICASSP40776.2020.9052930.

Liam Fowl, Ping-yeh Chiang, Micah Goldblum, **Jonas Geiping**, Arpit Bansal, Wojtek Czaja, and Tom Goldstein. Preventing Unauthorized Use of Proprietary Data: Poisoning for Secure Dataset Release. In *ICLR 2021 Workshop on Security and Safety in Machine Learning Systems*, February 2021a. URL http://arxiv.org/abs/2103.02683.

Liam Fowl, Micah Goldblum, Ping-yeh Chiang, **Jonas Geiping**, Wojciech Czaja, and Tom Goldstein. Adversarial Examples Make Strong Poisons. In *Advances in Neural Information Processing Systems*, volume 34, pages 30339–30351. Curran Associates, Inc., 2021b. URL https://proceedings.neurips.cc/paper/2021/hash/fe87435d12ef7642af67d9bc82a8b3cd-Abstract.html.

Liam Fowl*, **Jonas Geiping***, Wojciech Czaja, Micah Goldblum, and Tom Goldstein. Robbing the Fed: Directly Obtaining Private Data in Federated Learning with Modified Models. In *International Conference on Learning Representations*, September 2021c. URL https://openreview.net/forum?id=fwzUgo0FM9v.

Kanchana Vaishnavi Gandikota, **Jonas Geiping**, Zorah Lähner, Adam Czapliński, and Michael Moeller. A Simple Strategy to Provable Invariance via Orbit Mapping. In *Asian Conference on Computer Vision (ACCV)*, Macau, December 2022. arXiv. doi: 10.48550/arXiv.2209.11916. URL http://arxiv.org/abs/2209.11916.

Jonas Geiping. *Modern Optimization Techniques in Computer Vision*. Doctoral Thesis, University of Siegen, 10.25819/ubsi/9908, 2021. URL https://dspace.ub.uni-siegen.de/handle/ubsi/1897.

Jonas Geiping and Michael Moeller. Composite Optimization by Nonconvex Majorization-Minimization. *SIAM Journal on Imaging Sciences*, pages 2494–2528, January 2018. doi: 10.1137/18M1171989. URL https://epubs.siam.org/doi/10.1137/18M1171989.

Jonas Geiping and Michael Moeller. Parametric Majorization for Data-Driven Energy Minimization Methods. In *Proceedings of the IEEE International Conference on Computer Vision*, pages 10262–10273, 2019. URL http://openaccess.thecvf.com/content_ICCV_2019/html/Geiping_Parametric_Majorization_for_Data-Driven_Energy_Minimization_Methods_ICCV_2019_paper.html.

Jonas Geiping, Hendrik Dirks, Daniel Cremers, and Michael Moeller. Multiframe Motion Coupling for Video Super Resolution. In Marcello Pelillo and Edwin Hancock, editors, *Energy Minimization Methods in Computer Vision and Pattern Recognition*, Lecture Notes in Computer Science, pages 123–138. Springer International Publishing, 2018. ISBN 978-3-319-78199-0. doi: 10.1007/978-3-319-78199-0_9.

Jonas Geiping*, Hartmut Bauermeister*, Hannah Dröge*, and Michael Moeller. Inverting Gradients - How easy is it to break privacy in federated learning? In *Advances in Neural Information Processing Systems*, volume 33, December 2020a. URL https://proceedings.neurips.cc/paper/2020/hash/c4ede56bbd98819ae6112b20ac6bf145-Abstract.html.

Jonas Geiping, Fjedor Gaede, Hartmut Bauermeister, and Michael Moeller. Fast Convex Relaxations using Graph Discretizations. In *31st British Machine Vision Conference (BMVC 2020, Oral Presentation)*, Virtual, September 2020b. URL https://www.bmvc2020-conference.com/conference/papers/paper_0694.html.

Jonas Geiping, Liam Fowl, Gowthami Somepalli, Micah Goldblum, Michael Moeller, and Tom Goldstein. What Doesn't Kill You Makes You Robust(er): Adversarial Training against Poisons and Backdoors. In *ICLR 2021 Workshop on Security and Safety in Machine Learning Systems*, February 2021a. URL http://arxiv.org/abs/2102.13624.

Jonas Geiping*, Liam Fowl*, W. Ronny Huang, Wojciech Czaja, Gavin Taylor, Michael Moeller, and Tom Goldstein. Witches' Brew: Industrial Scale Data Poisoning via Gradient Matching. In *International Conference on Learning Representations*, April 2021b. URL https://openreview.net/forum?id=01olnfLIbD.

Jonas Geiping, Micah Goldblum, Phil Pope, Michael Moeller, and Tom Goldstein. Stochastic Training is Not Necessary for Generalization. In *International Conference on Learning Representations*, September 2021c. URL https://openreview.net/forum?id=ZBESeIUB5k.

Micah Goldblum*, **Jonas Geiping***, Avi Schwarzschild, Michael Moeller, and Tom Goldstein. Truth or backpropaganda? An empirical investigation of deep learning theory. In *Eighth International Conference on Learning Representations (ICLR 2020, Oral Presentation)*, April 2020. URL https://iclr.cc/virtual_2020/poster_HyxyIgHFvr.html.

Andreas Görlitz, **Jonas Geiping**, and Andreas Kolb. Piecewise Rigid Scene Flow with Implicit Motion Segmentation. In *2019 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*, pages 1758–1765, November 2019. doi: 10.1109/IROS40897.2019.8968018.

W. Ronny Huang*, **Jonas Geiping***, Liam Fowl, Gavin Taylor, and Tom Goldstein. MetaPoison: Practical General-purpose Clean-label Data Poisoning. In *Advances in Neural Information Processing Systems*, volume 33, Vancouver, Canada, December 2020. URL https://proceedings.neurips.cc//paper_files/paper/2020/hash/8ce6fc704072e351679ac97d4a985574-Abstract.html.

Pedro Sandoval-Segura, Vasu Singla, Liam Fowl, **Jonas Geiping**, Micah Goldblum, David Jacobs, and Tom Goldstein. Poisons that are learned faster are more effective. In *2022 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, pages 197–204, June 2022a. doi: 10.1109/CVPRW56347.2022.00033.

Pedro Sandoval-Segura, Vasu Singla, **Jonas Geiping**, Micah Goldblum, Tom Goldstein, and David W. Jacobs. Autoregressive Perturbations for Data Poisoning. In *Advances in Neural Information Processing Systems*, December 2022b. URL https://openreview.net/forum?id=1vusesyN7E.

Yuxin Wen*, **Jonas Geiping***, Liam Fowl, Micah Goldblum, and Tom Goldstein. Fishing for User Data in Large-Batch Federated Learning via Gradient Magnification. In *Proceedings of the 39th International Conference on Machine Learning*, pages 23668–23684. PMLR, June 2022. URL https://proceedings.mlr.press/v162/wen22a.html.

Recent Preprints

Arpit Bansal, Eitan Borgnia, Hong-Min Chu, Jie S. Li, Hamid Kazemi, Furong Huang, Micah Goldblum, **Jonas Geiping**, and Tom Goldstein. Cold Diffusion: Inverting Arbitrary Image Transforms Without Noise. *arxiv:2208.09392[cs]*, August 2022. doi: 10.48550/arXiv.2208.09392. URL http://arxiv.org/abs/2208.09392.

Liam Fowl*, **Jonas Geiping***, Steven Reich, Yuxin Wen, Wojtek Czaja, Micah Goldblum, and Tom Goldstein. Decepticons: Corrupted Transformers Breach Privacy in Federated Learning for Language Models. *arXiv:2201.12675 [cs]*, January 2022. URL http://arxiv.org/abs/2201.12675.

Kanchana Vaishnavi Gandikota, **Jonas Geiping**, Zorah Lähner, Adam Czapliński, and Michael Moeller. Training or Architecture? How to Incorporate Invariance in Neural Networks. *arXiv:2106.10044 [cs]*, June 2021. URL http://arxiv.org/abs/2106.10044.

Jonas Geiping and Tom Goldstein. Cramming: Training a Language Model on a Single GPU in One Day. *arxiv:2212.14034[cs]*, December 2022. doi: 10.48550/arXiv.2212.14034. URL http://arxiv.org/abs/2212.14034.

Jonas Geiping*, Jovita Lukasik*, Margret Keuper, and Michael Moeller. DARTS for Inverse Problems: A Study on Hyperparameter Sensitivity. *arXiv:2108.05647 [cs]*, August 2021. URL http://arxiv.org/abs/2108.05647.

Jonas Geiping, Micah Goldblum, Gowthami Somepalli, Ravid Shwartz-Ziv, Tom Goldstein, and Andrew Gordon Wilson. How Much Data Are Augmentations Worth? An Investigation into Scaling Laws, Invariance, and Implicit Regularization. *arxiv:2210.06441[cs]*, October 2022. doi: 10.48550/arXiv.2210.06441. URL http://arxiv.org/abs/2210.06441.

Renkun Ni, Ping-yeh Chiang, **Jonas Geiping**, Micah Goldblum, Andrew Gordon Wilson, and Tom Goldstein. K-SAM: Sharpness-Aware Minimization at the Speed of SGD. *arxiv:2210.12864[cs]*, October 2022. doi: 10.48550/arXiv.2210.12864. URL http://arxiv.org/abs/2210.12864.

Gowthami Somepalli, Vasu Singla, Micah Goldblum, **Jonas Geiping**, and Tom Goldstein. Diffusion Art or Digital Forgery? Investigating Data Replication in Diffusion Models. *arxiv:2212.03860[cs]*, December 2022. doi: 10.48550/arXiv.2212.03860. URL http://arxiv.org/abs/2212.03860.

Yuxin Wen, Arpit Bansal, Hamid Kazemi, Eitan Borgnia, Micah Goldblum, **Jonas Geiping**, and Tom Goldstein. Canary in a Coalmine: Better Membership Inference with Ensembled Adversarial Queries. *arxiv:2210.10750[cs]*, October 2022a. doi: 10.48550/arXiv.2210.10750. URL http://arxiv.org/abs/2210.10750.

Yuxin Wen*, **Jonas Geiping***, Liam Fowl, Hossein Souri, Rama Chellappa, Micah Goldblum, and Tom Goldstein. Thinking Two Moves Ahead: Anticipating Other Users Improves Backdoor Attacks in Federated Learning. *arxiv:2210.09305[cs]*, October 2022b. doi: 10.48550/arXiv.2210.09305. URL http://arxiv.org/abs/2210.09305.

*Shared authorship denoted by * and †. Alphabetic ordering denoted by ‡.*

Conference Presentations

March 2017 International Conference on Computer Vision 2019 and EMMCVPR 2017
Multiframe Motion Coupling for Video Super Resolution

Feb 2018 GAMM Annual Meeting 2018
Composite Optimization by Nonconvex Majorization-Minimization

June 2018 SIAM Conference on Imaging Sciences
Composite Optimization by Nonconvex Majorization-Minimization

Oct 2019 International Conference on Computer Vision 2019
Parametric Majorization for Data-Driven Energy Minimization Methods

April 2020 Eighth International Conference on Learning Representations
Truth or backpropaganda? An empirical investigation of deep learning theory

July 2020 SIAM Conference on Mathematics of Data Science 2020
Parametric Majorization for Data-Driven Energy Minimization Methods

Sep 2020 31st British Machine Vision Conference
Fast Convex Relaxations using Graph Discretizations

Dec 2020 Thirty-fourth Conference on Neural Information Processing Systems
Inverting Gradients - How easy is it to break Privacy in Federated Learning?

April 2021 Ninth International Conference on Learning Representations
Witches' Brew: Industrial Scale Data Poisoning via Gradient Matching

April 2022 Tenth International Conference on Learning Representations
Stochastic Training is not Necessary for Generalization

July 2022 Thirty-ninth International Conference on Machine Learning
Fishing for User Data in Large-Batch Federated Learning via Gradient Magnification

Dec 2022 Thirty-Sixth Conference on Neural Information Processing Systems
Autoregressive Perturbations for Data Poisoning