Valeriia Cherepanova

✉ vcherepa@umd.edu | Google Scholar

Interests

My research goal is to develop reliable, robust, and fair machine learning systems, which can be safely and effectively used for practical applications. I am also interested in advancing our understanding of how deep neural networks function and their failure modes.

Education

University of Maryland, College Park — *College Park*
PHD IN APPLIED MATHEMATICS — *Aug 2018 - Aug 2023*

- Advisor: Prof. Tom Goldstein
- Dean's Fellowship

University College London — *London*
MSC IN MODELING BIOLOGICAL COMPLEXITY (COMPLEX) — *Sept 2017 - Sept 2018*

- Graduated with distinction

National Research University Higher School of Economics — *Moscow*
BSC IN MATHEMATICS — *Sept 2013 - June 2017*

Industry Experience

Amazon, Alexa Entertainment — *Seattle*
APPLIED SCIENTIST INTERN — *Jun 2022 - Aug 2022*

- Developed ML solutions to classify different types of Alexa mistakes for improving Alexa Voice Search on FireTV.
- Built ML models for predicting popularity of FireTV Voice Searches from time-series data.

Amazon, Alexa Monitoring — *Bellevue*
APPLIED SCIENTIST INTERN — *Jun 2021 - Aug 2021*

- Developed NLP solutions to improve transparency of 3P Alexa Skills through detecting incompliant privacy policy documents.
- Deployed the model in production and built an interactive dashboard.

Teradata — *Moscow*
DATA SCIENTIST INTERN — *Jul 2016 - Oct 2016*

- Designed a machine learning training course for engineers at the company.

Selected Publications

LowKey: Leveraging Adversarial Attacks to Protect Social Media Users from Facial Recognition
V. Cherepanova, M. Goldblum, H. Foley, S. Duan, J. P. Dickerson, G. Taylor, T. Goldstein
International Conference on Learning Representations (ICLR), 2021, [paper], [webtool]

Transfer Learning with Deep Tabular Models
R. Levin*, **V. Cherepanova***, A. Schwarzschild, A. Bansal, C. B. Bruss, T. Goldstein, A. G. Wilson, M. Goldblum
International Conference on Learning Representations (ICLR), 2023, [paper], [GitHub]

Strong Data Augmentation Sanitizes Poisoning and Backdoor Attacks Without an Accuracy Tradeoff
E. Borgnia*, **V. Cherepanova***, L. Fowl*, A. Ghiasi*, J. Geiping*, M. Goldblum*, T. Goldstein*, A. Gupta*
The International Conference on Acoustics, Speech, & Signal Processing (ICASSP), 2021, [paper]

A Deep Dive into Dataset Imbalance and Bias in Face Identification
V. Cherepanova*, S. Reich*, S. Dooley, H. Souri, M. Goldblum, T. Goldstein
AAAI/ACM Conference on AI, Ethics, and Society, 2023 [paper]

Technical Challenges for Training Fair Neural Networks
V. Cherepanova*, V. Nanda*, M. Goldblum, J. P Dickerson, T. Goldstein
RAI Workshop at the International Conference on Learning Representations (ICLR), 2021, [paper]

Unraveling Meta-Learning: Understanding Feature Representations for Few-Shot Tasks
M. Goldblum, S. Reich*, L. Fowl*, R. Ni*, **V. Cherepanova***, T. Goldstein
International Conference on Machine Learning (ICML), 2020, [paper]

MetaBalance: High-Performance Neural Networks for Class-Imbalanced Data
A. Bansal, M. Goldblum, **V. Cherepanova**, A. Schwarzschild, C. B. Bruss, T. Goldstein
arXiv preprint, [paper]

Comparing human and machine bias in face recognition
S. Dooley, R. Downing, G. Wei, N. Shankar, B. Thymes, G. Thorkelsdottir, T. Kurtz-Miott, R. Mattson, O. Obiwumi, **V. Cherepanova**, M. Goldblum, J.P. Dickerson, T. Goldstein
arXiv preprint, [paper]

DP-InstaHide: Provably Defusing Poisoning and Backdoor Attacks with Differentially Private Data Augmentations
E. Borgnia, J. Geiping, **V. Cherepanova**, L. Fowl, A. Gupta, A. Ghiasi, F. Huang, M. Goldblum, T. Goldstein
arXiv preprint, [paper]

* indicates equal contribution

Conferences and Talks

Transfer Learning with Deep Tabular Models

- Oral Presentation at the NeurIPS 2022 Table Representation Learning Workshop
- Invited Talk at Arthur AI

A Deep Dive into Dataset Imbalance and Bias in Face Identification

- NeurIPS 2022 Workshop on Trustworthy and Socially Responsible Machine Learning
- NeurIPS 2022 Workshop on Algorithmic Fairness through the Lens of Causality and Privacy
- NeurIPS 2022 Workshop on Machine Learning Safety

Technical Challenges for Training Fair Neural Networks

- ICLR 2021 Workshop on Responsible AI

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

- ICLR 2021
- NeurIPS 2020 Resistance AI Workshop
- NeurIPS 2020 Workshop on Dataset Curation and Security

Reviewer Service

ICML2023, NeurIPS 2022, ICLR 2022, NeurIPS 2021, NeurIPS 2022 TSRML Workshop, ICLR 2021 RAI Workshop, IEEE TPAMI

Relevant Coursework

Machine Learning: Deep Learning, Computer Vision, Computational Linguistics, Algorithms in Machine Learning: Guarantees and Convergence, Foundations of Deep Learning
Signal Processing: Scientific Computing, Advanced Numerical Optimization, Mathematical Statistics, Probability Theory, Applied Stochastic Processes

Technical Skills

Programming: Python (PyTorch, PySpark, Huggingface, scikit-learn), SQL