Rob Romijnders

PhD in Machine Learning

About me

PhD student in Federated Machine Learning.

Specialized in large-scale and robust machine learning.

Research areas

- Robustness and calibration
- Training at scale
- Learning from video
- Computer vision
- Domain adaptation
- Federated Learning
- Differential privacy

Cited 900+ times. Published in top-tier venues such as NeurIPS, CVPR, AAAI, ICLR, and AISTATS

Community engagement

Previous organizer of Eindhoven Data Science.

Recorded talks at PyData:

- Machine Translation (2017)
  youtube.com/watch?v=HVdPWoZ_swY
- Bayesian ML (2018)
  youtube.com/watch?v=Z7VN7oRA6TY
- AI robustness (2024)
  youtube.com/watch?v=2-EjNJnV4Ec

Experience

2021–2026

PhD in Machine Learning

University of Amsterdam · Amsterdam, NL

- My main topic is robust machine learning and decentralized inference;
- Advised by Max Welling, Christos Louizos, and Yuki M. Asano;
- Thesis supervisor to three cum-laude graduates;
- Research visits with the Uni of Helsinki, Bochum and Saarbrucken;
- Sponsored by Qualcomm AI, part of EU-wide ELLIS program.

PhD Internships

Extra-curricular · internships

- **G-Research**, London, 10wk, on financial time series modeling;
- **Brave Software**, London, 12wk, on robust Large Language Models (LLM);
- **Apple Inc**, Cambridge, 14wk, on scalable and robust histogram aggregation

2019–2021

AI Researcher

Google Research · Zurich, CH

I dealt with 300+ terabytes of video data on distributed file systems, had more than 180 accepted pull requests, and created and shared 60+ internal documents. This resulted in five publications in top-tier publication venues.

2016–2019

AI Researcher

Frosha (AI startup) · Amsterdam, NL

I was the main machine learning researcher in this startup, training NLP machine learning algorithms for classification and parsing of unstructured text.

Extra curricular

Academic Reviewing

Reviewer at CVPR/ICLR/ICML/NeurIPS

Outstanding reviewer award ICCV 2021

Summer schools

GPSS summer school, UK, 2018

DLRL summer school, Canada, 2023

FoMo summer school, NL, 2024

Programming

- **Python**
- **Bash, unix**
- **C, C++**
- **Slurm, cloud**

Education

2015–2018

MSc Electrical Engineering

Eindhoven University of Technology · Eindhoven, NL

Graduated *cum laude*, top 10% of my class. Courses in signal processing, stochastic processes, dynamical systems and non-linear optimization.

Six month exchange semester with the University of Singapore in Singapore.

2011–2014

Bachelor of Science

Twente University · Enschede, NL

Graduated *cum laude*, top 10% of year; board member at AIESEC Twente.

Rob Romijnders romijndersrob@gmail.com @ *robromijnders.github.io*

Academic publications

Robust AI and Decentralized inference

2025 **NoEsis: A Modular LLM with Differentially Private Knowledge Transfer**
RR, Laskaridis, Shahin-Shamsabadi, Haddadi · ICLR 2025 workshop
Internship project at the privacy-oriented browser, Brave.

2025 **Multi-reference alignment for MIMO wireless communications**
RR, Cesa, Louizos, Pratik, Behboodi · under review

2025 **Convex Approximation of Two-Layer ReLU Networks for Hidden State DP**
RR, Koskela · NeurIPS 2025

2024 **DNA: Differentially private Neural Augmentation for contact tracing**
RR, Louizos, Asano, Welling · ICLR 2024 Private ML workshop
Code available at github.com/RobRomijnders/dna; Awarded spotlight talk at the workshop.

2024 **Protect Your Score: Contact Tracing with Differential Privacy Guarantees**
RR, Louizos, Asano, Welling · AAAI 2024
Code available; Awarded 15-minute oral talk in the main track, for top 10% of papers.

2023 **No time to waste: practical statistical contact tracing with few low-bit messages**
RR, Asano, Louizos, Welling · AISTATS 2023
Code available at github.com/QUVA-Lab/nttw

Large-scale AI and video data

2022 **Beyond transfer learning: Co-finetuning for action localisation**
Arnab, Xiong, Gritsenko, **RR**, Djolonga, Dehghani, Sun, Lucic, Schmid · arXiv preprint

2021 **Representation learning from videos in-the-wild: An object-centric approach**
RR, Mahendran, Tschannen, Djolonga, Ritter, Houlsby, Lucic · IEEE WACV 2021

2021 **SI-Score: An image dataset for fine-grained analysis of robustness**
Yung, **RR**, Kolesnikov, Beyer, Djolonga, Houlsby, Gelly, Lucic, Zhai · ICLR 2021 workshop

Robustness, calibration, and generalization

2023 **The effect of covariate shift and network training on Out-of-Distribution Detection**
Mariani, Klomp, **RR**, de With · VISAPP 2023

2021 **Impact of aliasing on generalization in deep convolutional networks**
Vasconcelos, Larochelle, Dumoulin, **RR**, Le Roux, Goroshin · ICCV 2021

2021 **Revisiting the Calibration of Modern Neural Networks**
Minderer, Djolonga, **RR**, Hubis, Zhai, Houlsby, Tran, Lucic · NeurIPS 2021

2021 **On Robustness and Transferability of Convolutional Neural Networks**
Djolonga, Yung, Tschannen, **RR**, Beyer, Kolesnikov, Puigcerver, Minderer, D'Amour, Moldovan, Gelly, Houlsby, Zhai, Lucic · CVPR 2021

2019 **Data Selection for training Semantic Segmentation CNNs with cross-dataset weak supervision**
Meletis, **RR**, Dubbelman · IEEE ITSC 2019

2019 **Domain Agnostic Normalization for Unsupervised Adversarial Domain Adaptation**
RR, Meletis, Dubbelman · IEEE WACV 2019

AI applications

2018 **Applying Deep Bidirectional LSTM and MDN for Trajectory Prediction**
Zhao, Yang, Chevalier, Shah, **RR** · Optik - Int. Journal for Light and Electron Optics, 2018

2016 **Applying Deep Learning to Basketball Trajectories**
Shah, **RR** · Sports Analytics Workshop, KDD 2016