

# Rob Romijnders

Machine Learning PhD student



## About me

PhD student in Federated Machine Learning, with many open-source contributions. Projects centered around large-scale, robust and private machine learning.

## Research areas

Computer vision:

- Domain adaptation
- Robustness and calibration
- Learning from video
- Training at scale

Federated Learning:

- Decentralized inference
- Differential privacy

Co-author for the Wikipedia pages on Differential Privacy and Bayes Error Rate

600+ citations, h-index 8  
Overview of publications at [robromijnders.nl/research](https://robromijnders.nl/research)

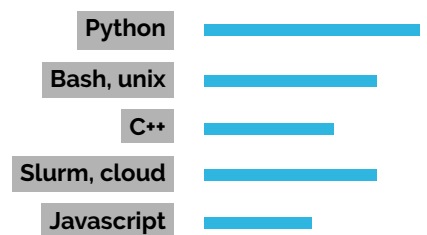
## EXPERIENCE

- |              |   |
|--------------|---|
| 2021–present | <b>PhD in Federated Machine Learning</b><br>UNIVERSITY OF AMSTERDAM · Amsterdam, NL<br>Advised by Max Welling, Christos Louizos, and Yuki M. Asano. <ul style="list-style-type: none"><li>• Supervised eight AI students and five final thesis projects.</li><li>• My main topic is differential privacy and federated learning.</li><li>• Internship programs:<ul style="list-style-type: none"><li>- G-Research, London, 10 weeks, on financial time series modeling</li><li>- Brave Software, remote, 12 weeks, on differential privacy in NLP</li></ul></li></ul> |
| 2019–2021    | <b>AI researcher</b><br>GOOGLE RESEARCH (DEEPMIND) · Zurich, CH<br>Research program within Google Research. I dealt with 300+ terabytes of video on distributed file systems, had more than 180 accepted pull requests, and created and shared 60+ slide decks. This resulted in five publications.   |
| 2016–2019    | <b>Machine Learning engineer</b><br>FROSHA · Amsterdam, NL<br>I was the main machine learning scientist in this startup, training text-based machine learning algorithms for classification and parsing.  |

## EXTRA CURRICULAR

- Academic Reviewing**  
Reviewer at CVPR/ICLR/ICML/NeurIPS  
Journal reviewer at TMLR  
Outstanding reviewer award ICCV 2021
- Summer schools**  
GPSS summer school, UK, 2018  
DLRL summer school, Canada, 2023
- PyData community member**  
Community talks on machine translation, Bayesian ML, and differential privacy

## PROGRAMMING



## EDUCATION

- |           |   |
|-----------|---|
| 2015–2018 | <b>MSc Electrical Engineering</b><br>EINDHOVEN UNIVERSITY OF TECHNOLOGY · Eindhoven, NL<br>Graduated <i>cum laude</i> , top 10% of my class. Courses in signal processing, stochastic processes, dynamical systems and non-linear optimization. |
| 2016      | <b>Minor Data Mining</b><br>NATIONAL UNIVERSITY OF SINGAPORE · Singapore, SG<br>Courses: data mining, reinforcement learning, non-linear optimization.  |
| 2014–2015 | <b>Minor Engineering</b><br>SOUTHERN FEDERAL UNIVERSITY · Rostov-on-Don, RU<br>Courses: stochastic processes, numerical methods, software verification.   |
| 2011–2014 | <b>BSc Clinical Technology</b><br>TWENTE UNIVERSITY · Enschede, NL<br>Graduated <i>cum laude</i> , top 10% of my class; volunteer at AIESEC Twente.   |

# Academic publications

## Decentralized inference and Differential Privacy

- 2025 **Membership Inference Attack on Routed Large Language Models**  
R. ROMIJNDERS, S. LASKARIDIS, H. HADDADI · under submission  
Internship project at the privacy-first browser Brave.
- 2024 **DNA: Differentially private Neural Augmentation for contact tracing**  
R. ROMIJNDERS, C. LOUIZOS, Y.M. ASANO, M. WELLING · ICLR 2024 Private ML workshop  
Code available at [github.com/RobRomijnders/dna](https://github.com/RobRomijnders/dna)  
Awarded spotlight talk at the workshop.
- 2024 **Protect Your Score: Contact Tracing with Differential Privacy Guarantees**  
R. ROMIJNDERS, C. LOUIZOS, Y.M. ASANO, M. WELLING · AAAI 2024  
Code available at [github.com/RobRomijnders/dpfn\\_aaa](https://github.com/RobRomijnders/dpfn_aaa)  
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**  
R. ROMIJNDERS, Y.M. ASANO, C. LOUIZOS, M. WELLING · AISTATS 2023  
Code available at [github.com/QUVA-Lab/nttw](https://github.com/QUVA-Lab/nttw)

## Experience with large-scale models and training on video data

- 2021 **SI-Score: An image dataset for fine-grained analysis of robustness to object location, rotation and size**  
J. YUNG, R. ROMIJNDERS, A. KOLESNIKOV, L. BEYER, J. DJOLONGA, N. HOULSBY, S. GELLY, M. LUCIC, X. ZHAI · RobustML workshop ICLR 2021  
Data available on TF Datasets
- 2022 **Beyond transfer learning: Co-finetuning for action localisation**  
A. ARNAB, X. XIONG, A. GRITSENKO, R. ROMIJNDERS, J. DJOLONGA, M. DEGHANI, C. SUN, M. LUCIC, C. SCHMID · arXiv preprint 2022
- 2021 **Representation learning from videos in-the-wild: An object-centric approach**  
R. ROMIJNDERS, A. MAHENDRAN, M. TSCHANNEN, J. DJOLONGA, M. RITTER, N. HOULSBY, M. LUCIC · IEEE WACV 2021

## Robustness, calibration, and out of distribution generalization

- 2023 **The effect of covariate shift and network training on Out-of-Distribution Detection**  
S. MARIANI, S. KLOMP, R. ROMIJNDERS, P. DE WIT · VISAPP 2023
- 2021 **Impact of aliasing on generalization in deep convolutional networks**  
C. VASCONCELOS, H. LAROCHELLE, V. DUMOULIN, R. ROMIJNDERS, N. LE ROUX, R. GOROSHIN · ICCV 2021
- 2021 **Revisiting the Calibration of Modern Neural Networks**  
M. MINDERER, J. DJOLONGA, R. ROMIJNDERS, F. HUBIS, X. ZHAI, N. HOULSBY, D. TRAN, M. LUCIC · NeurIPS 2021
- 2021 **On Robustness and Transferability of Convolutional Neural Networks**  
J. DJOLONGA, J. YUNG, M. TSCHANNEN, R. ROMIJNDERS, L. BEYER, A. KOLESNIKOV, J. PUIGSERVER, M. MINDERER, A. D'AMOUR, D. MOLDOVAN, S. GELLY, N. HOULSBY, X. ZHAI, M. LUCIC · CVPR 2021
- 2019 **Data Selection for training Semantic Segmentation CNNs with cross-dataset weak supervision**  
P. MELETIS, R. ROMIJNDERS, G. DUBBELMAN · IEEE ITSC 2019
- 2019 **Domain Agnostic Normalization for Unsupervised Adversarial Domain Adaptation**  
R. ROMIJNDERS, P. MELETIS, G. DUBBELMAN · IEEE WACV 2019  
Code available at [github.com/RobRomijnders/dan](https://github.com/RobRomijnders/dan)

## Deep learning for sports analytics

- 2016 **Applying Deep Learning to Basketball Trajectories**  
R. SHAH, R. ROMIJNDERS · Sports Analytics Workshop, KDD 2016