+1 647 384 6001
Toronto, Canada
franziska.boenisch.fb@gmail.com

Franziska Boenisch

Postdoctoral Fellow (Vector Institute)

GitHub: fraboeni
LinkedIn: fraboeni
https://franziska-boenisch.de/

Academic and Research Experience

Tenure Track Faculty **09 2023 — present**
CISPA Institute, Saarbrücken, Germany

- Co-lead of the SprintML Research lab on Trustworthy Machine Learning

Postdoctoral Fellow **08 2022 — 08 2023**
Vector Institute, Toronto, Canada

- Research on trustworthy and private machine learning from the perspective of individual users
- Supervised by Prof. Dr. Nicolas Papernot

Research Associate (Full-Time) **09 2019 — 08 2022**
Fraunhofer AISEC, Berlin, Germany

- Research on differential privacy, and privacy quantification and metrics in machine learning models
- Project management, project acquisition in public domain and industry, grant writing, student advising

Ph.D. Research Intern (Full-Time) **07 2021 — 03 2022**
Vector Institute for Artificial Intelligence, Toronto, Canada

- Research on privacy attacks against federated learning
- Research on privacy attacks in various domains and on differential privacy

Student assistant at the BioRobotics Lab (Part-Time, 20h/week) **02 2018 — 01 2019**
Freie University, Berlin, Germany

- Implementation of an object tracking for honey bee trajectories in Matlab
- Collaboration in different research papers in the field of bio robotics and self-driving autonomous cars

Undergraduate Research Intern (Full-Time) **08 2016 — 09 2016**
Chung Cheng University, Chiayi, Taiwan

- Supported by the DAAD RISE-Scholarship
- Implementation of neural networks for food image classification

Student assistant at the Data Analytics Lab (Part-Time, 20h/week) **02 2016 — 07 2016**
Fraunhofer FOKUS, Berlin, Germany

- Prototype development and implementation of demonstrators in the field of predictive maintenance
- Implementation of applications with Apache Spark and Apache Flink

Education

Ph.D. Candidate **09 2019 — 11 2022**
Freie University Berlin, Germany *(Final Grade: summa cum laude)*

- Thesis: Secure and Private Machine Learning
- Advisors: Prof. Dr. Marian Margraf, Prof. Dr. Nicolas Papernot

M.Sc. Computer Science **10 2017 — 07 2019**
Freie University Berlin, Germany *(Final Grade: 1.0)*

- Thesis: "Differential Privacy: General Survey and Analysis of Practicability in the Context of Machine Learning"
- Advisor: Prof. Dr. Marian Margraf

Exchange Student **02 2019 — 07 2019**
Technical University Eindhoven, Netherlands *(Average 8.3/10)*

- Supported by the ERASMUS-Scholarship
- Relevant coursework: Artificial Intelligence, Statistics, Recommender Systems

B.Sc. Computer Science **04 2014 — 04 2017**
Freie University Berlin *(Final Grade: 1.2)*

- Thesis: "Feature Engineering and Probabilistic Tracking on Honey Bee Trajectories"
- Advisor: Prof. Dr. Tim Landgraf

Publications

[1] Haonan Duan, Adam Dziedzic, Nicolas Papernot, and Franziska Boenisch. Flocks of stochastic parrots: Differentially private prompt learning for large language models. In ***Thirty-seventh Conference on Neural Information Processing Systems***, 2023. URL https://openreview.net/forum?id=u6Xv3FuF8N.

[2] Jan Dubiński, Stanisław Pawlak, Franziska Boenisch, Tomasz Trzcinski, and Adam Dziedzic. Bucks for buckets (b4b): Active defenses against stealing encoders. In ***Thirty-seventh Conference on Neural Information Processing Systems***, 2023. URL https://openreview.net/forum?id=NfpYgGZC3B.

[3] Franziska Boenisch, Christopher Mühl, Adam Dziedzic, Roy Rinberg, and Nicolas Papernot. Have it your way: Individualized privacy assignment for dp-sgd. In ***Thirty-seventh Conference on Neural Information Processing Systems***, 2023. URL https://openreview.net/forum?id=XXPzBhOs4f.

[4] Mohammad Yaghini, Patty Liu, Franziska Boenisch, and Nicolas Papernot. Learning with impartiality to walk on the pareto frontier of fairness, privacy, and utility. *arXiv preprint arXiv:2302.09183*, 2023.

[5] Franziska Boenisch, Adam Dziedzic, Roei Schuster, Ali Shahin Shamsabadi, Ilia Shumailov, and Nicolas Papernot. When the curious abandon honesty: Federated learning is not private. In ***8th IEEE European Symposium on Security and Privacy (EuroS&P '23)***, 2023.

[6] Franziska Boenisch, Adam Dziedzic, Roei Schuster, Ali Shahin Shamsabadi, Ilia Shumailov, and Nicolas Papernot. Reconstructing individual data points in federated learning hardened with differential privacy and secure aggregation. In ***8th IEEE European Symposium on Security and Privacy (EuroS&P '23)***, 2023.

[7] Matteo Giomi, Franziska Boenisch, Christoph Wehmeyer, and Borbála Tasnádi. A unified framework for quantifying privacy risk in synthetic data. In ***23rd Privacy Enhancing Technologies Symposium (PoPETs)***, 2023.

[8] Franziska Boenisch, Christopher Mühl, Roy Rinberg, Jannis Ihrig, and Adam Dziedzic. Individualized pate: Differentially private machine learning with individual privacy guarantees. In ***23rd Privacy Enhancing Technologies Symposium (PoPETs)***, 2023.

[9] Karla Pizzi, Franziska Boenisch, Ugur Sahin, and Konstantin Böttinger. Introducing model inversion attacks on automatic speaker recognition. In ***Proc. 2nd Symposium on Security and Privacy in Speech Communication (SPSC)***, pages 11–16, 2022.

[10] Anvith Thudi, Ilia Shumailov, Franziska Boenisch, and Nicolas Papernot. Bounding membership inference. *arXiv preprint arXiv:2202.12232*, 2022.

[11] Adam Dziedzic, Haonan Duan, Muhammad Ahmad Kaleem, Nikita Dhawan, Jonas Guan, Yannis Cattan, Franziska Boenisch, and Nicolas Papernot. Dataset inference for self-supervised models. In ***Neural Information Processing Systems (NeurIPS)***, 2022.

[12] Franziska Boenisch, Reinhard Munz, Marcel Tiepelt, Simon Hanisch, Christiane Kuhn, and Paul Francis. Side-channel attacks on query-based data anonymization. In ***Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security (CCS)***, pages 1254–1265, 2021.

[13] Franziska Boenisch. A systematic review on model watermarking for neural networks. ***Frontiers in Big Data***, 4, 2021.

[14] Peter Sörries, Claudia Müller-Birn, Katrin Glinka, Franziska Boenisch, Marian Margraf, Sabine Sayegh-Jodehl, and Matthias Rose. Privacy needs reflection: Conceptional design rationales for privacy-preserving explanation user interfaces. ***Mensch und Computer*** *Workshop*, 2021.

[15] Franziska Boenisch, Verena Battis, Nicolas Buchmann, and Maija Poikela. "I never thought about securing my machine learning systems": A study of security and privacy awareness of machine learning practitioners. In ***Mensch und Computer*** *2021*, pages 520–546. 2021.

[16] Franziska Boenisch, Philip Sperl, and Konstantin Böttinger. Gradient masking and the underestimated robustness threats of differential privacy in deep learning. *arXiv preprint arXiv:2105.07985*, 2021.

[17] Tabea Kossen, Manuel Alexander Hirzel, Vince Istvan Madai, Franziska Boenisch, Anja Hennemuth, Kristian Hildebrand, Sebastian Pokutta, Kartikey Sharma, Adam Hilbert, Jan Sobesky, et al. Towards sharing brain images: Differentially private tof-mra images with segmentation labels using generative adversarial networks. ***Frontiers in Artificial Intelligence***, page 85.

[18] Franziska Boenisch, Benjamin Rosemann, Benjamin Wild, David Dormagen, Fernando Wario, and Tim Landgraf. Tracking all members of a honey bee colony over their lifetime using learned models of correspondence. ***Frontiers in Robotics and AI***, 5: 35, 2018.

Prizes and Honors

Fraunhofer TALENTA Start Scholarship, *Fraunhofer Society*	01 2020 — 12 2021
3^{rd} prize: Forum Junge Spitzenforscher, *German Industrial Research Foundation*	11 2020
German National Merit Foundation Scholarship, *Studienstiftung des deutschen Volkes*	04 2015 — 07 2019
Grace Hopper Celebration Travel Scholarship, *Hasso-Plattner-Institute*	09 2018
Taalunie Zomercursus Nederlands Scholarship, *Taalunie*	08 2018
DAAD RISE Research Scholarship, *DAAD (German Academic Exchange Service)*	08 2016 — 09 2016
Kulturweit Scholarship, *DAAD (German Academic Exchange Service)*	02 2013 — 02 2014
German Association of Mathematicians Higher Education Entrance Prize, *DMV (German Mathematical Society)*	07 2012

Students

Current Students

W. Wang C. Mühl *(Self-Supervised Learning)*	Ph.D., CISPA
C. Mühl *(Individualized Privacy)*	Ph.D., Faunhofer AISEC
D. Wahdany *(Privacy Attacks)*	Ph.D., Faunhofer AISEC
R. Rinberg *(Individualized Privacy)*	Master, Columbia University

Past Students (University of Toronto)

M. Yaghini *(Privacy and Fairness)*	Ph.D., University of Toronto
C. Bruckmann *(Model Attribution)*	Undergraduate, University of Toronto
P. Liu *(Privacy and Fairness)*	Undergraduate, University of Toronto
H. Duan *(Privacy in Natural Language Processing)*	Ph.D., University of Toronto
J. Guan *(Reinforcement Learning)*	Ph.D., University of Toronto

Past Students (FU Berlin or Fraunhofer AISEC)

A. Meszaros *(Taxonomy of Privacy Attacks in Machine Learning)*	Undergraduate	link to thesis
M. Nest *(Practical Design of Privacy Attacks in Machine Learning)*	Master	link to thesis
I. Fendel *(Membership Inference Attacks against Deep Neural Networks)*	Undergraduate	link to thesis
M. Krüger *(Application and Evaluation of Differential Privacy in Health Data Classification Tasks)*	Undergraduate	link to thesis
O. Bouanani *(Neural Network Architectural Choices for Privacy)*	Undergraduate	link to thesis
C. Mühl *(Personalizing Private Aggregation of Teacher Ensembles)*	Master	link to thesis
T. Känel *(Practical Evaluation of Neural Network Watermarking Approaches)*	Undergraduate	link to thesis
D. Wang *(Evaluating and Adapting Existing NN Watermarking Approaches to Online Learning)*	Undergraduate	link to thesis
D. Sosnovchyk *(Evaluating Privacy of Synthetic Data Through Metrics)*	Undergraduate	link to thesis
W. Gu *(Differential Private Synthetic Data Generation)*	Undergraduate	link to thesis
J. Ihrig *(Privacy Quantification Methods for Private Aggregation of Teacher Ensembles)*	Master	link to thesis

Services and Volunteering

Reviewer for NeurIPS conference	03 2023 — present
PC member for ACM CCS	03 2023 — present
Co-organizer of ICLR'23 workshop on trustworthy ML under limited data and compute	10 2022 — present
Mentor at Women in ML workshop (NeurIPS'23)	12 2022
PC member for IEE SaTML	01 2022 — present
Co-organizer of Workshop "Trustworthy AI in Science and Society" at Informatik2022 conference	01 2022 — 09 2022
PC member for IEEE Symposium on Security and Privacy (IEEE S&P)	01 2022 — present
Reviewer for ICLR PAIR2Struct Workshop	01 2022
Mentor at CyberMentor, an online mentoring for female high school students in CS	03 2021 — present
Open source project contributor General Data Anonymity Score	09 2019 — 12 2020
Mentor at MINToring, mentoring program of female high school students in CS *Freie University Berlin*	04 2015 — 01 2019
Organizer of Summer School *ProInformatik VI: Python Programming for Female Students* *Freie University Berlin*	07 2019
Student assistant of the Women's Representative (Physics Department), *Freie University Berlin*	01 2017 — 01 2018
Deputy representative of students in the Central Women's Council, *Freie University Berlin*	01 2016 — 12 2017
Volunteer teacher with Kulturweit Voluntary Service, *German Consulate School Izmir, Turkey*	02 2013 — 02 2014
Student representative, *Rückert High School, Berlin*	09 2010 — 07 2012

Invited Talks

What Trust Model is needed for Federated Learning to be Private?: Vector Institute, Research Symposium	2023
What Trust Model is needed for Federated Learning to be Private?: University of Toronto, AI Conference	2023
What Trust Model is needed for Federated Learning to be Private?: Apple	2023
What Trust Model is needed for Federated Learning to be Private?: University of Melbourne	2022
Federated Learning is not Private: NAACL Private NLP Workshop	2022
Federated Learning is not Private: SRI research talks	2022
Federated Learning is not Private: Microsoft Research Confidential Computing research group meeting	2022
Federated Learning is not Private: Brave research group meeting	2022
Differential Private Machine Learning: Vector Institute Demo Days	2022
Privacy Preserving Machine Learning: Threats and Solutions: Women in International Security Germany-Study Tour	2021
Mitigating Privacy Risks in Machine Learning through Differential Privacy: AI@Enterprise Conference	2021
ML and resilience against Privacy Attacks: Fraunhofer Solutions Days	2021
Privacy Preserving Machine Learning with Differential Privacy: Advanced Machine Learning Study Group (Meetup)	2021
Machine Learning Privacy Attacks: Lecture: Human-Centered Data Science (Guest Lecture, FU Berlin)	2021
Machine Learning and Privacy: Lecture: Usable Security and Privacy (Guest Lecture, FU Berlin)	2020
Machine Learning and Privacy: Lecture: Usable Security and Privacy (Guest Lecture, FU Berlin)	2020
Differential Privacy in Machine Learning: Berlin Machine Learning Group (Meetup)	2020
Privacy-Preserving Machine Learning for Health Care: Machine Learning in Healthcare Berlin (Meetup)	2019
Differential Privacy in Machine Learning for Health Care: Own Data Spring School	2019
Differential Privacy in Machine Learning: 31st Crypto Day (GI)	2019