THERESA STADLER

Data Privacy and Trustworthy AI

theresa.stadler@epfl.ch | Personal Web | GoogleScholar | LinkedIn

EXPERIENCE

PostDoc & Lecturer - *EPFL (CH)* **Since 2025**
Research and Teaching
Research on privacy-enhancing technologies, such as, synthetic data, privacy-preserving machine learning, and differential privacy. Lectures at BSc and MSc level on information security and privacy.

PhD Research Assistant - *EPFL (CH)* **2019 – 2024**
Research and Teaching
Several high impact publications in the fields of data privacy and trustworthy machine learning.

Research Scientist - *Privitar (UK)* **2016 – 2019**
Product Development, Research, and Consulting
Designed, developed, and prototyped enterprise software that implements privacy-enhancing technologies at scale. Several consulting projects for both public and private sector organisations.

Graduate Student Research Assistant - *Werner Reichardt Centre for Integrative Neuroscience (DE)* **2015-2016**
Experimental Research and Data Analysis
Statistical models of visual information processing in retinal ganglion cells.

Student Research Assistant - *University of Erlangen (DE)* **2012 - 2014**
Experimental Research and Data Analysis
Biophysical modelling of the molecular mechanisms of chronic pain disorders.

EDUCATION

PhD in Computer Science - *EPFL (CH), SPRING Lab* **2019 - 2024**
PhD Thesis: On the Fundamental Limits of Privacy-Enhancing Technologies.

MSc in Computational Neuroscience - *University of Tübingen (DE)* **2014 - 2016**
Lectures in Statistics, Machine Learning, Dynamic Systems, and Neuroscience

BSc in Biomathematics - *University of Erlangen (DE)* **2011 - 2014**
Lectures in Statistics, Linear Algebra, Physics, and Biology

GRANTS & AWARDS

Nominee for the EPFL Doctorate Award - *EPFL (CH)* **2024**

Teaching Assistant Award - *EPFL IC (CH)* **2021**

Graduate Grant - *Studienstiftung des Deutschen Volkes (DE)* **2011 - 2016**

SELECTED INVITED TALKS

Talk — **On the Fundamental Limits of Privacy-Enhancing Technologies -** *Nokia Bell Labs* **2025**
Invited talk at the Responsible AI seminar.

Panel — **Synthetic Data for AI -** *European Commission, DG CONNECT* **2024**
Invited talk and panel discussion

Lecture — **On the Fundamental Limits of Privacy-Preserving Data Sharing -** *Brussels Privacy Hub* **2024**
Lecture at the Summer Academy For Global Privacy Law 2024

Panel — **Looking beyond the EU data strategy: Where next for data use and regulation? -** *CPDP* **2023**
Panel discussion on the future of data use and regulations

Lecture — **Synthetic data as a privacy mechanism - A cautionary tale -** *MIT* **2022**
Invited lecture in the Health Science and Technology Program

SELECTED MEDIA COVERAGE

Podcast	**Privacy Engineering -** *They Talk Tech Podcast* Available at `frauen-technik.podigee.io`	**2025**
News Article	**Warum wollen plötzlich alle Luca? -** *Eva Wolfangel, Die Zeit* Available at `zeit.de`	**2021**
Podcast	**#22 Luca vs. Datenschutz -** *She likes Tech Podcast, NDR* Available at `ndr.de`	**2021**
News Article	**EU privacy experts push a decentralized approach to COVID-19 contacts tracing -** *TechCrunch* Available at `techcrunch.com`	**2020**
News Article	**Coronavirus apps: the risk of slipping into a surveillance state. -** *Financial Times* Available at `ft.com`	**2020**

SELECTED ACADEMIC SERVICE & INVITED REVIEWS

PC Member	**ACM ASIA Conference on Computer and Communications Security -** *AsiaCCS*	**2026**
PC Member	**Conference on Fairness, Accountability, and Transparency -** *FAccT*	**2024**
PC Member	**Privacy Enhancing Technologies Symposium -** *PETS*	**2019-2024, 2026**
Invited Reviewer	**Workshop on Privacy in Machine Learning -** *NeurIPS'21*	**2021**
Invited Reviewer	**Workshop on Synthetic Data Generation -** *ICLR*	**2021**
External Reviewer	**Conference on Computer and Communications Security -** *CCS*	**2019**
Reviewer	**Rethinking data and balancing digital power** *by the Ada Lovelace Institute* Report on a future vision for data use and regulation. Available at `adalovelaceinstitute.org`	**2022**
Reviewer	**Privacy & Online Rights** *by Carmela Troncoso* Chapter on Privacy & Online Rights in the Cyber Security Body of Knowledge. Available at `cybok.org`	**2019**

LANGUAGES

English - Fluent, **German** - Native, **French, Italian** - Good conversational skills

SELECTED PUBLICATIONS

2025

T. Stadler, C. Troncoso, and M. Kolbe-Guyot. Purpose first: The need for a paradigm shift in privacy-preserving data sharing. *C4DT Insights*, 2025

2024

T. Stadler, B. Kulynych, N. Papernot, M. Gastpar, and C. Troncoso. The fundamental limits of least-privilege learning. In *Proceedings of the 41th International Conference on Machine Learning (ICML 24)*, 2024

2022

T. Stadler, B. Oprisanu, and C. Troncoso. Synthetic data – Anonymisation Groundhog Day. In *31st USENIX Security Symposium (USENIX Security 22)*, 2022

T. Stadler and C. Troncoso. Why the search for a privacy-preserving data sharing mechanism is failing. *Nature Computational Science*, 2022

C. Troncoso, T. Stadler, D. Bogdanov, E. Bugnion, S. Chatel, C. Cremers, S. Gürses, J.-P. Hubaux, D. Jackson, J. R. Larus, et al. Deploying decentralized, privacy-preserving proximity tracing. *Communications of the ACM*, 2022

2021

T. Stadler, W. Lueks, K. Kohls, and C. Troncoso. Preliminary analysis of potential harms in the luca tracing system. *arXiv preprint arXiv:2103.11958*, 2021

2020

C. Troncoso, M. Payer, J.-P. Hubaux, M. Salathé, J. Larus, E. Bugnion, W. Lueks, T. Stadler, A. Pyrgelis, D. Antonioli, et al. Decentralized privacy-preserving proximity tracing. *arXiv preprint arXiv:2005.12273*, 2020

V. von Wyl, S. Bonhoeffer, E. Bugnion, M. A. Puhan, M. Salathé, T. Stadler, C. Troncoso, E. Vayena, and N. Low. A research agenda for digital proximity tracing apps. *Swiss Medical Weekly*, 2020

M. Salathé, C. L. Althaus, N. Anderegg, D. Antonioli, T. Ballouz, E. Bugnion, S. Capkun, D. Jackson, S.-I. Kim, J. Larus, et al. Early evidence of effectiveness of digital contact tracing for sars-cov-2 in switzerland. *medRxiv*, 2020

PATENTS

2023

J. D. McFALL, C. C. Cabot, T. J. Moran, K. F. P. Guinamard, V. M. Eatwell, B. T. Pickering, P. D. Mellor, T. Stadler, A. Petre, C. A. Smith, et al. Computer-implemented privacy engineering system and method, Nov. 9 2023. US Patent App. 18/349,223

2022

C. C. Cabot, K. F. P. Guinamard, J. D. McFALL, P.-a. Maugis, P. Hector, B. T. Pickering, T. Stadler, J.-a. Tay, and S. Weller. Method or system for querying a sensitive dataset, Sept. 1 2022. US Patent App. 17/618,765