

Lucas Rosenblatt

Curriculum Vitae

July 2026

Assistant Professor (Tenure-track)
Williams College

Email: lr21@williams.edu

Academic Positions

Williams College, Department of Computer Science
Assistant Professor (Tenure-track)

Williamstown, MA
2026–Present

Research Areas

Machine Learning, Differential Privacy, Reinforcement Learning, Alg. Fairness, Theory of Alg., LLMs

Education

New York University
Ph.D. in Computer Science | GPA: 3.95

New York City, NY
2021 – 2026

Brown University, Honors
B.Sc. in Computer Science, B.A. English, Non-Fiction Writing | GPA: 3.8

Providence, RI
2015 – 2019

Awarded Senior Prize in CS

Senior Prize awarded for outstanding record in teaching, research and service

Regular Collaborators

Regular collaborators include Teal Witter (Claremont McKenna College), Chris Musco (NYU), Bill Howe (University of Washington) and Rachel Cummings (Columbia).

Industry Research Experience

Google Research
Student Researcher — New York City, NY

2025 – 2026

- Working with Natalia Ponomareva and Ryan McKenna as part of Sergei Vassilvitskii's group, on tabular data privacy problems with open-source Gemma models.

Microsoft AI Development Acceleration Program (MAIDAP)
ML Engineer/Researcher — Cambridge, MA

2019 – 2021

- AI rotational program serving Microsoft organizations with applied research in machine learning.
- Rotations: Grey Systems Lab, Microsoft+Harvard OpenDP (Smartnoise), Microsoft News, Fairlearn.

Conference Publications

- Hod, S., L. **Rosenblatt**, and J. Stoyanovich (2025). Do You Really Need Public Data? Surrogate Public Data for Differential Privacy on Tabular Data. In: *Proceedings of the 39th International Conference on Neural Information Processing Systems*. (NeurIPS '25). San Diego, CA, USA. <https://arxiv.org/pdf/2504.14368?>.
- Musco, C., C. Musco, L. **Rosenblatt**, and A. V. Singh (2025). Sharper Bounds for Chebyshev Moment Matching with Applications to Differential Privacy and Beyond. In: *38th Annual Conference on Learning Theory (COLT)*. <https://proceedings.mlr.press/v291/musco25a.html>.
- Rosenblatt**, L., B. Han, R. Wolfe, and B. Howe (2025). Fragments to Facts: Partial-Information Fragment Inference from LLMs. In: *Proceedings of the 42nd International Conference on Machine Learning (ICML), Vancouver, Canada*. PMLR 275, 2025. <https://icml.cc/virtual/2025/poster/45801>.
- Rosenblatt**, L., Y. Lut, E. Turok, M. Avella-Medina, and R. Cummings (2025). Differential Privacy Under Class Imbalance: Methods and Empirical Insights. In: *Proceedings of the 42nd International Conference on Machine Learning (ICML), Vancouver, Canada*. PMLR 275, 2025. <https://icml.cc/virtual/2025/poster/45213>.
- Rosenblatt**, L., B. Herman, A. Holovenko, W. Lee, J. Loftus, E. McKinnie, T. Rumezhak, A. Stadnik, B. Howe, and J. Stoyanovich (2024). Epistemic Parity: Reproducibility as an Evaluation Metric for Differential Privacy. *SIGMOD record* 53(1), 65 [Awarded SIGMOD Research Highlight, Awarded CACM Research Highlight].

6. **Rosenblatt**, L., J. Stoyanovich, and C. Musco (2024). A simple and practical method for reducing the disparate impact of differential privacy. In: *Proceedings of the Thirty-Eighth AAAI Conference on Artificial Intelligence*. AAAI'24/IAAI'24/EAAI'24. AAAI Press. <https://doi.org/10.1609/aaai.v38i19.30153>.
7. Witter, R. T. and L. **Rosenblatt** (2024). I open at the close: a deep reinforcement learning evaluation of open streets initiatives. In: *Proceedings of the Thirty-Eighth AAAI Conference on Artificial Intelligence*. AAAI'24/IAAI'24/EAAI'24. AAAI Press. <https://doi.org/10.1609/aaai.v38i20.30250>.
8. Wolfe, R., I. Slaughter, B. Han, B. Wen, Y. Yang, L. **Rosenblatt**, B. Herman, E. Brown, Z. Qu, N. Weber, and B. Howe (2024). Laboratory-Scale AI: Open-Weight Models are Competitive with ChatGPT Even in Low-Resource Settings. In: *Proceedings of the 2024 ACM Conference on Fairness, Accountability, and Transparency*. FAccT '24. Rio de Janeiro, Brazil: Association for Computing Machinery, pp.1199–1210. <https://doi.org/10.1145/3630106.3658966>.
9. Bell, A., L. Bynum, N. Drushchak, T. Herasymova, L. **Rosenblatt**, and J. Stoyanovich (2023). The Possibility of Fairness: Revisiting the Impossibility Theorem in Practice. In: *Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency*. FAccT '23. Chicago, IL, USA: Association for Computing Machinery, pp.400–422. <https://doi.org/10.1145/3593013.3594007>.
10. **Rosenblatt**, L., B. Herman, A. Holovenko, W. Lee, J. Loftus, E. McKinnie, T. Rumezhak, A. Stadnik, B. Howe, and J. Stoyanovich (July 2023). Epistemic Parity: Reproducibility as an Evaluation Metric for Differential Privacy. *Proc. VLDB Endow.* **16**(11), 3178–3191 [**Best Paper Runner-Up**].
11. Rosenblatt, L. and R. T. Witter (2023). Counterfactual fairness is basically demographic parity. In: *Proceedings of the Thirty-Seventh AAAI Conference on Artificial Intelligence*. AAAI'23/IAAI'23/EAAI'23. AAAI Press. <https://doi.org/10.1609/aaai.v37i12.26691>.
12. Ammerlaan, R., G. Antonius, M. Friedman, H. S. Hossain, A. Jindal, P. Orenberg, H. Patel, S. Qiao, V. Ramani, L. **Rosenblatt**, et al. (2021). PerfGuard: deploying ML-for-systems without performance regressions, almost! In: *Proceedings of the VLDB Endowment*. Vol. 14. VLDB Endowment, pp.3362–3375. <https://dl.acm.org/doi/10.14778/3484224.3484233>.
13. **Rosenblatt**, L., P. Carrington, K. Hara, and J. P. Bigham (2018). Vocal programming for people with upper-body motor impairments. In: *Proceedings of the 15th International Web for All Conference*, pp.1–10. <https://dl.acm.org/doi/10.1145/3192714.3192821>.
14. **Rosenblatt**, L. (2017). Vocalide: An ide for programming via speech recognition. In: *Proceedings of the 19th International ACM SIGACCESS Conference on Computers and Accessibility*, pp.417–418. <https://dl.acm.org/doi/10.1145/3132525.3134824>.

Workshop Publications

15. **Rosenblatt**, L., B. Han, E. Posthumus, T. Crimmins, and B. Howe (2023). Top-down Green-ups: Satellite Sensing and Deep Models to Predict Buffelgrass Phenology. *Tackling Climate Change with Machine Learning 2023 (@NeurIPS)*.
16. **Rosenblatt**, L., J. Allen, and J. Stoyanovich (2022). Spending Privacy Budget Fairly and Wisely. *Theory and Practice of Differential Privacy 2022 (@ICML)*.
17. **Rosenblatt**, L., L. Piedras, and J. Wilkins (2022). Critical Perspectives: A Benchmark Revealing Pitfalls in PerspectiveAPI. In: *Proceedings of the 2nd Workshop on NLP for Positive Impact (NLP4PI)*, pp.15–24.
18. Hossain, H. S., L. **Rosenblatt**, G. Antonius, I. Shaffer, R. Ammerlaan, A. Roy, M. Weimer, H. Patel, M. Friedman, S. Qiao, P. Orenberg, et al. (2020). PerfGuard: Deploying ML-for-Systems without Performance Regressions. *MLOps*.

Pre-prints

19. Kodama, S., H. Diwan, L. **Rosenblatt**, R. T. Witter, and N. Cohen (2025). SimKey: A Semantically Aware Key Module for Watermarking Language Models. *arXiv preprint arXiv:2510.12828 (under review)*.
20. **Rosenblatt**, L., B. Howe, and J. Stoyanovich (2024). Are Data Experts Buying into Differentially Private Synthetic Data? Gathering Community Perspectives. *arXiv preprint arXiv:2412.13030 (under review)*.
21. **Rosenblatt**, L. and R. T. Witter (2024). FairlyUncertain: A Comprehensive Benchmark of Uncertainty in Algorithmic Fairness. *arXiv preprint arXiv:2410.02005 (under review)*.
22. **Rosenblatt**, L., X. Liu, S. Pouyanfar, E. de Leon, A. Desai, and J. Allen (2020). Differentially private synthetic data: Applied evaluations and enhancements. *arXiv preprint arXiv:2011.05537*.

Funding

NAIRR Pilot Grant

2024 – Present

\$35,000

2023 NSF Graduate Research Fellowship

2023 – 2026

\$147,000

Center for Responsible AI PhD Fellowship

2022 – 2026

Teaching

Graduate Teaching

2022 – 2025

New York University

New York City, NY

- Full Course Instructor - CSGA-1017, Responsible Data Science (2025)
- Section Leader - CSGA-1017, Responsible Data Science (three occasions, 2023–2025)
- Teaching Assistant - CSGY-6763, Algorithmic Machine Learning and Data Science (2022)

Undergraduate Teaching

2016 – 2018

Brown University

Providence, RI

- Teaching Assistant - CS017, Computer Science: An Integrated Introduction (2016)
- Teaching Assistant - CS018, Computer Science: An Integrated Introduction (2017)
- Teaching Assistant - CS1300, User Interfaces and User Experiences (2018)

Invited Talks & Lectures

Invited Keynote @ TPDP in 2025, Title: *Theory and Practice of Differentially Private Synthetic Data*, TPDP Website.

Invited Talk @ NYC Privacy Day in 2025, Title: *Differential Privacy in Practice: Synthetic Data for Education, Surrogate Data for Research*, Website.

Invited Spotlight Talk @ FMSD in 2025, Title: *Do You Really Need Public Data? Surrogate Public Data for Differential Privacy on Tabular Data*, FMSD Website.

Invited Lightning Talk @ NAIRR Conference in 2024, Title: *Public Data Alternatives for Differential Privacy on Tabular Data*, Program

Invited Talk @ UW in 2024, Title: *On Some of Our Recent Work in Differential Privacy and Fairness*, Volitional AI Group

Invited Talk @ NYC Privacy Day in 2023, Title: *A Benchmark for Evaluating the Epistemic Parity of DP Data Synthesizers*, NYC Privacy Day Website

Invited Talk @ UCLA Synthetic Data Workshop in 2023, Title: *Theory and Practice of Differentially Private Synthetic Data*, Workshop Website

Service

Lead Organizer: NYC Privacy Day, 2026 (at NYU, website).

Lead Organizer: NYC Privacy Day, 2024 (at NYU, website).

Co-organizer: NAIRR Community-Informed Policies Workshop (at NYU, website).

Reviewer: COLT 2026, ICLR 2026, 2025, AISTATS 2026, 2025, ICML 2026, 2025, FAccT 2026, 2025, TPDP 2026, 2025, Neurips 2025, 2024, KDD 2025, SOSA 2024, CHI 2023

Patents

System and Method for Machine Learning for System Deployments Without Performance Regressions *HM Sajjad Hossain, Lucas Rosenblatt, Gilbert Antonius, Irene Shaffer, Remmelt Ammerlaan, Abhishek Roy, Markus Weimer, Hiren Patel, Marc Friedman, Shi Qiao, Peter Orenberg, Soundarajan Srinivasan, Vijay Ramani, Alekh Jindal*, (MS# 408144-US-NP)

Other Work Experience

Software Engineering Intern

2018

*Microsoft Garage**Cambridge MA*

- Developed machine learning approaches to object/shape detection for the Ink to Code platform

Human-Computer Interaction Researcher

2017 – 2018

*Carnegie Mellon University**Pittsburgh, PA*

- Advised by Dr. Jeff Bigham and Dr. Kotaro Hara, researched accessible programming interfaces
- Focused on assistive technology individuals with motor impairments and/or cerebral palsy
- Published two papers detailing VocalIDE, a vocal programming interface

Projects

Primary maintainer for SynRD | *DP, Repo*

2022 – 2024

- Collaborate with researchers at the University of Washington and with students from UCU in Lviv.

Maintainer for Smartnoise: Open Source DP Toolkit | *DP, Pytorch*

2019 – 2024

- Provide regular code updates, documentation, and pursue new offerings.
- MWEM implementation, QUAIL ensemble model, DP GANs, metrics etc.

AI for my Life | *Undergraduate Thesis*

2019 – 2021

- Nominated for “Theories in Action,” a Brown University forum for sharing undergraduate theses

VocalIDE | *Experimental Tool, Javascript*

2017 – 2018

- Developed accessible programming interface for vocal programming
- Conducted two user studies to iterate on system

Empor.co | *Start-up, Full-stack iOS*

2016 – 2018

- Co-founded a start-up with Zachary Horvitz
- Full stack/entrepreneurial experience, ultimately disbanded the company.

Skills

Familiar with... Python, C#/C, Java, SQL, JavaScript, Lean, etc.

Tools & Libraries: numpy, pandas, pytorch, aws, react, git, azure

Spoken languages: Dutch (B1, heritage speaker) and French (A2)

Software Suites: Adobe (Premier, Photoshop, Illustrator), Logic, Maya