Mathias Lécuyer

Assistant Professor, The University of British Columbia, Vancouver

Areas

Machine Learning, Causal Inference, Privacy, Security, Software Systems.

Education

2013–2019 **PhD in Computer Science**, *Columbia University*, New York, *GPA 4.0*.
- Thesis: *Security, Privacy, and Transparency Guarantees for Machine Learning Systems*.
- Advisors: Roxana Geambasu, Augustin Chaintreau, and Daniel Hsu.

2011–2012 **Master of Science in Computer Science**, *Columbia University*, New York, *GPA: 3.90*.

2008–2011 **Ingénieur Diplômé**, *Ecole Polytechnique*, Paris, France, *GPA: 3.90*.
Major in Computer Science, multidisciplinary training in Physics, Enonomics, and Biology.

2006–2008 **Classes Préparatoires in Science**, *Lycée Louis-le-Grand*, Paris, France, *GPA: 4.0*.
Intensive preparation in Mathematics and Physics for competitive admission into top French universities.

Work Experience

2021-Current **Assistant Professor**, *The University of British Columbia*, Vancouver.

2019-2021 **Post-Doctoral Researcher**, *Microsoft Research*, New York.
- Developped a new counterfactual estimators for system policies [12].
- Developped a new methodology to explain ML predictions based on training data [10].

2013-2019 **Research Assistant**, *Columbia University*, New York.

Summer 2017 **Research Intern**, *Microsoft Research*, New York.
- Applied reinforcement learning to systems, with a focus on off-policy evaluation [17].

2012–2014 **Teaching Assistant**, *Columbia University*, New York.
- Distributed Systems. Instructor: Roxana Geambasu.
- Data Journalism. Instructor: Mark Hansen.
- Computer Networking. Instructor: Augustin Chaintreau.

Summer 2014 **Freelance**, *Floatingapps*, New York.
- Developed a Rails application for rental data visualization, using Cassandra, Elasticsearch, d3, and React.
- Built an iOS application for email visualization as timelines in Objective-C.

Summer 2013 **Freelance**, *Milky*, Paris, France.
- Built an extended iOS application for *Le Grand Journal*, a show of major French TV Channel Canal+.

2009–2012 **Cofounder**, *Pionid*, Paris, France.
Developed the main product, an iOS group messaging application.

Research

I am broadly interested in machine learning systems, with a specific focus on applications that provide rigorous guarantees of robustness, privacy, and security. In my research, I leverage, adapt, and improve theoretical tools (differential privacy, causal inference, reinforcement learning) to enable specific applications (ML attacks/defenses, privacy preserving data management, system decisions optimization) with sound guarantees. I currently focus on two broad directions:

✉ *mathias.lecuyer@ubc.ca* ▪ *http://mathias.lecuyer.me*

ML Security, Privacy & Explainability

While data-driven systems can yield social and economic benefits, they also open new security and privacy threats, and their opacity can undermine users' trust. I develop ML models with guarantees of security, privacy, and explainability, and build the infrastructure necessary to soundly deploy and maintain them.

Certified Defenses Against Adversarial Examples.
I developed PixelDP (now called randomized smoothing), the first certified defense that both offers a guaranteed level of robustness against these attacks and scales to large models and datasets, such as Google's Inception on the ImageNet dataset [14].

Infrastructure Support for Differential Privacy in Machine Learning Workloads.
I am developing infrastructure support for differential privacy at the level of entire ML and DB query workloads. This includes designing the DP theory and systems abstractions required to keep track of privacy loss on continuously growing data streams [15, 11], adding privacy as a resource in cluster management systems, and designing scheduling algorithms for the privacy resource [13].

Increasing Explainability in Machine Learning.
I leverage causal inference theory to design black-box explainability techniques, to understand data usage in web services [23, 21], or how training data can influence a model's predictions [10]. I also work on explainable models [9].

Counterfactual Evaluation & Optimization for Systems

Machine learning and statistics present new opportunities to solve traditional systems challenges in improved ways. I leverage causal inference and reinforcement learning to evaluate and optimize systems policies with sound statistical approaches [17, 12].

Papers

[1] Mishaal Kazmi, Hadrien Lautraite, Alireza Akbari, Mauricio Soroco, Qiaoyue Tang, Tao Wang, Sébastien Gambs, and Mathias Lécuyer. PANORAMIA: Privacy Auditing of Machine Learning Models without Retraining. In *Theory and Practice of Differential Privacy (TPDP) workshop*, 2024.

[2] Amir Sabzi, Rut Vora, Swati Goswami, Margo Seltzer, Mathias Lécuyer, and Aastha Mehta. NetShaper: A Differentially Private Network Side-Channel Mitigation System. In *USENIX Security Symposium*, 2024.

[3] Shadab Shaikh, Saiyue Lyu, Frederick Shpilevskiy, Evan Shelhamer, and Mathias Lécuyer. Adaptive Randomized Smoothing for Certified Multi-Step Defence. In *Workshop on Test-Time Adaptation: Model, Adapt Thyself! (MAT), at CVPR*, 2024.

[4] Qiaoyue Tang, Frederick Shpilevskiy, and Mathias Lécuyer. DP-AdamBC: your DP-Adam is actually DP-SGD (unless you apply Bias Correction). In *Proceedings of the AAAI Conference on Artificial Intelligence* ***(Oral)***, 2024.

[5] Shiqi He, Qifan Yan, Feijie Wu, Lanjun Wang, Mathias Lécuyer, and Ivan Beschastnikh. GlueFL: Reconciling Client Sampling and Model Masking for Bandwidth Efficient Federated Learning. In *Conference on Machine Learning and Systems (MLSys)*, 2023.

[6] Kelly Kostopoulou, Pierre Tholoniat, Asaf Cidon, Roxana Geambasu, and Mathias Lécuyer. Turbo: Effective Caching in Differentially-Private Databases. In *Proceedings of the ACM Symposium on Operating Systems Principles (SOSP)*, 2023.

[7] Mauricio Soroco, Joel Hempel, Xinze Xiong, Mathias Lécuyer, and Joséphine Gantois. Flowering Onset Detection: Traditional Learning vs. Deep Learning Performance in a Sparse Label Context. In *Tackling Climate Change with Machine Learning: workshop at NeurIPS*, 2023.

[8] Qiaoyue Tang and Mathias Lécuyer. DP-Adam: Correcting DP Bias in Adam's Second Moment Estimation. In *Trustworthy and Reliable Large-Scale Machine Learning Models (RTML) Workshop at ICLR*, 2023.

[9] Ali Behrouz, Mathias Lécuyer, Cynthia Rudin, and Margo Seltzer. Fast Optimization of

Weighted Sparse Decision Trees for use in Optimal Treatment Regimes and Optimal Policy Design. In *Advances in Interpretable Machine Learning and Artificial Intelligence (AIMLAI) Workshop*, 2022.

[10] Jinkun Lin, Anqi Zhang, Mathias Lécuyer, Jinyang Li, Aurojit Panda, and Siddhartha Sen. Measuring the Effect of Training Data on Deep Learning Predictions via Randomized Experiments. In *International Conference on Machine Learning (ICML)*, 2022.

[11] Mathias Lécuyer. Practical Privacy Filters and Odometers with Rényi Differential Privacy and Applications to Differentially Private Deep Learning. *Preprint (arXiv)*, 2021.

[12] Mathias Lécuyer, Sang Hoon Kim, Mihir Nanavati, Junchen Jiang, Siddhartha Sen, Amit Sharma, and Aleksandrs Slivkins. Sayer: Using Implicit Feedback to Optimize System Policies. In *ACM Symposium on Cloud Computing (SoCC)*, 2021.

[13] Tao Luo, Mingen Pan, Pierre Tholoniat, Asaf Cidon, Roxana Geambasu, and Mathias Lécuyer. Privacy Budget Scheduling. In *Proceedings of the USENIX Symposium on Operating Systems Design and Implementation (OSDI)*, 2021.

[14] Mathias Lécuyer, Vaggelis Atlidakis, Roxana Geambasu, Daniel Hsu, and Suman Jana. Certified Robustness to Adversarial Examples with Differential Privacy. In *Proceedings of the IEEE Symposium on Security and Privacy (Oakland)*, 2019.

[15] Mathias Lécuyer, Riley Spahn, Kiran Vodrahalli, Roxana Geambasu, and Daniel Hsu. Privacy Accounting and Quality Control in the Sage Differentially Private ML Platform. In *Proceedings of the ACM Symposium on Operating Systems Principles (SOSP)*, 2019.

[16] Mathias Lécuyer, Riley Spahn, Kiran Vodrahalli, Roxana Geambasu, and Daniel Hsu. Privacy Accounting and Quality Control in the Sage Differentially Private ML Platform. In *ACM SIGOPS Operating Systems Review (OSR)*, 2019.

[17] Mathias Lécuyer, Joshua Lockerman, Lamont Nelson, Siddhartha Sen, Amit Sharma, and Aleksandrs Slivkins. Harvesting Randomness to Optimize Distributed Systems. In *The Seventeenth ACM Workshop on Hot Topics in Networks (HotNets)*, 2017.

[18] Mathias Lécuyer, Riley B. Spahn, Roxana Geambasu, Tzu-Kuo Huang, and Siddhartha Sen. Enhancing Selectivity in Big Data. *Invited paper in the IEEE Security and Privacy Symposium Magazine*, 2017.

[19] Mathias Lécuyer, Riley B. Spahn, Roxana Geambasu, Tzu-Kuo Huang, and Siddhartha Sen. Pyramid: Enhancing Selectivity in Big Data Protection with Count Featurization. In *Proceedings of the IEEE Symposium on Security and Privacy (Oakland)*, 2017.

[20] Mathias Lécuyer, Max Tucker, and Augustin Chaintreau. Improving the Transparency of the Sharing Economy. In *Proceedings of the International World Wide Web Conference (WWW)*, 2017.

[21] Mathias Lécuyer, Riley B. Spahn, Giannis Spiliopoulos, Augustin Chaintreau, Roxana Geambasu, and Daniel Hsu. Sunlight: Fine-grained Targeting Detection at Scale with Statistical Confidences. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2015.

[22] Nicolas Viennot, Mathias Lécuyer, Jonathan Bell, Roxana Geambasu, and Jason Nieh. Synapse: New Data Integration Abstractions for Agile Web Application Development. In *Proceedings of the European Conference on Computer Systems (EuroSys)*, 2015.

[23] Mathias Lécuyer, Guillaume Ducoffe, Francis Lan, Andrei Papancea, Theofilos Petsios, Riley Spahn, Augustin Chaintreau, and Roxana Geambasu. XRay: Increasing the Web's Transparency with Differential Correlation. In *Proceedings of the USENIX Security Symposium*, 2014.

Awards & Distinctions

2022 Google Research Scholar award (https://research.google/outreach/research-scholar-program/).

2017 Finalist for the Facebook PhD Fellowship (https://research.fb.com/announcing-the-2017-facebook-phd-fellows/).

2015 Finalist for the Microsoft Research Fellowship.

2011 "Bourse Carnot" Fellowship: an excellency fellowship for French students in the Unites-States, focused on Research and Entrepreneurship.

Invited Talks

2024 [Panel] *Privacy and Connected Cars*, Intelligent Transportation Systems Society of Canada (ITS Canada) Annual Conference & Expo, Vancouver.

2024 *PANORAMIA: Efficient Privacy Auditing of Machine Learning Models without Retraining*, Statistical Aspects of Trustworthy Machine Learning, Banff International Research Station (BIRS) workshop, Banff.

2023 [Tutorial] *Privacy as hypothesis testing: linking Differential Privacy, membership attacks, and privacy audits*, Canadian AI, Responsible AI Track, Montréal.

2023 *DP-AdamBC: your DP-Adam is actually DP-SGD (unless you apply Bias Correction)*, Bridge the gap: Differential Privacy and Statistical Analysis, Amii Upper Bound Workshop, Edmonton.

2020 *Towards a Practical Differentially Private Machine Learning Platform*, Northwest Data Science Seminar Series.

2019 *Privacy Accounting and Quality Control in the Sage Differentially Private ML Platform*, University of California Berkeley, Security Seminar.

2019 *Security, Privacy, and Transparency Guarantees for Machine Learning Systems*, University of British Columbia.

2019 *Security, Privacy, and Transparency Guarantees for Machine Learning Systems*, University of California Los Angeles.

2019 *Security, Privacy, and Transparency Guarantees for Machine Learning Systems*, Microsoft Research New York.

2018 *Certified Robustness to Adversarial Examples with Differential Privacy*, University of Washington, Security Seminar.

2018 *Certified Robustness to Adversarial Examples with Differential Privacy*, University of California Berkeley, Security Seminar.

2018 *Certified Robustness to Adversarial Examples with Differential Privacy*, Google Brain.

2018 *Harvesting Randomness for Counterfactual Evaluation of Systems*, Stanford, NetSeminar.

2018 *Certified Robustness to Adversarial Examples with Differential Privacy*, Stanford, Security Lunch.

2014 *XRay: Enhancing the Web's Transparency with Differential Correlation*, University of Washington and Microsoft Research Summer Institute.

2012 *Dispatch: weaving a safe web of news*, Columbia Journalism & Technology Breakfast.

Media Coverage

2021 Geneviève Lasalle, "Ottawa finance la création d'un outil pour déchiffrer les mots de passe," Radio Canada, 09 novembre 2021.

2020 Alexandra Pihen, "La vie privée en voie d'extinction," Science et Vie, Hors Série 290, 04 mars 2020.

2016 *The data republic*, "To safeguard democracy, the use of data should be made as transparent as possible," The Economist.

2016 Priya Kumar, *When Was the Last Time You Read a Privacy Policy?*, Slate.com.

2015 Tom Simonite, *Probing the Dark Side of Google's Ad-Targeting System*, MIT Technology Review.

2014 Steve Lohr, *XRay: A New Tool for Tracking the Use of Personal Data on the Web*, The New York Times.

Service

2024 Program Committee, Conference on Secure and Trustworth Machine Learning (SaTML) 2024.

2023 Program Committee, Symposium on Operating Systems Design and Implementation (OSDI) 2023.

2023 Workshop Reviewer, International Conference on Learning Representations (ICLR) 2023.

2022/2023 Program Committee, Security & Privacy (Oakland) 2023.

2022 Reviewer, International Conference on Machine Learning (ICML) 2022.

2021/2022 Program Committee, Security & Privacy (Oakland) 2022.

2021 External Reviewer, USENIX Security 2022.

2021 Reviewer, NeurIPS 2021.

2020/2021 Program Committee, USENIX Security 2021.

2021 Program Committee, Conference on Machine Learning and Systems (MLSys) 2021.

2020 Reviewer, International Conference on Machine Learning 2020.

2019 Guest Lecture, graduate class "Decentralized Security: Theory and Systems" (CS 294-163). Instructor: Raluca Ada PopaUniversity of California Berkeley

2020 External Reviewer, Security & Privacy (Oakland) 2020.

2020 Program Committee, Eurosys 2020.

2019/2020 Program Committee, USENIX Security 2020.

2019 Reviewer, Journal of Machine Learning Research.

2019 Program Committee, ACM Symposium on Cloud Computing (SoCC) 2019.

2018 Program Committee, Systems for Machine Learning Workshop at the Conference on Neural Information Processing Systems, http://learningsys.org/nips18/.

2017 Reviewer, AISys Workshop at the ACM Symposium on Operating Systems Principles, http://learningsys.org/sosp17/.

2016 Reviewer, ACM Transactions on Internet Technology.

2016 & 2014 Co-designed and delivered a programming workshop for the Annual Engineering Exploration, organized by the Society of Women Engineers for New York City high-school female students.