CS208 Spring 2025 Annotated Bibliography

James Honaker, Priyanka Nanayakkara, and Salil Vadhan

April 24, 2025

Note: The differential privacy literature has become vast and continues to grow at a rapid rate. This means this list is far from comprehensive. It also means that as you search online for references, it can be difficult to identify which papers are high quality. Publication in a strong peer-reviewed conference proceedings or journal is a useful (but still imperfect) signal. If you are unsure about some paper you've encountered, send it to us and we can try to help you gauge.

- Background Material
  - Discrete math and proofs: Lewis and Zax [2019], Solow [2013], Rosen [2012]
  - Algorithms and complexity: Roughgarden [2022], Cormen et al. [2009], Mitzenmacher and Upfal [2005]
  - Basic Probability and statistics: Ross [1998]
- General References
  - The main textbook for the course: Cowan et al. [2024]
  - A list of real-world uses of differential privacy: Desfontaines [2021]
  - Lecture Notes on Privacy in Machine Learning and Statistics: Smith and Ullman [2025]
  - "Advancing Differential Privacy: Where We Are Now and Future Directions for Real-World Deployment" Cummings et al. [2024]
- Reidentification Attacks
  - (assigned) Forbes article on Sweeney's reidentification of Personal Genome Project participants: Tanner [2013]
  - (assigned) New York Times article on reidentification from AOL Search Log release: Barbaro and Zeller [2006]
  - (assigned) Narayanan-Shmatikov opinion piece on the concept of PII: Narayanan and Shmatikov [2010]
  - Sweeney's original re-identification: Sweeney [1997]
  - Statistics on reidentification by DOB, ZIP, and Sex: Sweeney [2000], Golle [2006]
  - Paper on the Personal Genome Project reidentification: Sweeney et al. [2013]
  - Paper introducing k-anonymity: Sweeney [2002]
  - Composition attack on k-anonymity: Ganta et al. [2008]
  - Biases introduced by deidentification of EdX data: Daries et al. [2014]
  - Netflix reidentification: Narayanan and Shmatikov [2008]
  - Cancellation of 2nd Netflix Challenge after Lawsuit: Singel [2010]
  - Cohen's downcoding attacks and EdX reidentification: Cohen [2022]

  - Defenses of de-identification: Cavoukian and Castro [2014], Cavoukian and El Emam [2014]

- Reconstruction Attacks
  - Linear programming attack on Diffix: Cohen and Nissim [2018]
  - SAT Solver attack on Census data: Garfinkel et al. [2018]
  - Survey paper on attacks on aggregate statistics: Dwork et al. [2017, §1,2]
  - Paper introducing reconstruction attacks: Dinur and Nissim [2003]
  - Differencing attack on Israeli Census: Ziv [2013]
  - Debates and variants on Census reconstruction attack: Ruggles and van Riper [2022], Hullman [2021], Jarmin et al. [2023], Dick et al. [2023]

- Membership Attacks
  - (assigned) P3G Consortium responses to membership attacks on genomic data: Consortium et al. [2009]
  - Survey paper on attacks on aggregate statistics: Dwork et al. [2017, §3]
  - Membership attack on means in genomic data: Homer et al. [2008]
  - Membership attack on noisy means: Dwork et al. [2015b]
  - Membership attack on ML as a Service: Shokri et al. [2017], Carlini et al. [2022], Zarifzadeh et al. [2024]

- Other Privacy Attacks
  - Debates about whether or not statistical inference is a privacy violation Fredrikson et al. [2014], McSherry [2016], Bun et al. [2021], Hotz et al. [2022], Jarmin et al. [2023].
  - Privacy attacks on microtargeted ads: Korolova [2011, §1,4,6,8]
  - Extracting training data from AI models: Carlini et al. [2021, 2023]

- Foundations of Differential Privacy
  - Primer for non-technical audiences: Wood et al. [2018b, 2020]
  - A book about differential privacy, for programmers: Near and Abuah [2021]
  - The first textbook: Dwork and Roth [2013]
  - Survey on complexity-theoretic aspects of differential privacy: Vadhan [2017]
  - The papers leading up to and culminating in the definition of differential privacy and the first mechanisms (Laplace, histograms, implementing the SQ model): Dinur and Nissim [2003], Dwork and Nissim [2004], Blum et al. [2005], Dwork et al. [2016].
  - Attacks on floating-point implementations of differential privacy and remedies: Mironov [2012], Balcer and Vadhan [2018], Casacuberta et al. [2022], Haney et al. [2022]
  - The geometric mechanism: Ghosh et al. [2012]
  - A Bayesian interpretation of approximate DP: Kasiviswanathan and Smith [2014]
  - A survey on differential privacy for social networks: Raskhodnikova and Smith [2014]
  - The advanced and "optimal" composition theorems for approximate DP: Dwork et al. [2010], Kairouz et al. [2017], Murtagh and Vadhan [2018]
  - zero-Concentrated DP and the related Rényi DP Dwork and Rothblum [2016], Bun and Steinke [2016], Mironov [2017]
  - f-DP and a state-of-art composition method for it Dong et al. [2022], Doroshenko et al. [2022]

- Interactive DP and "concurrent" composition theorems for it Lyu [2022], Vadhan and Zhang [2023].
- Composition with the privacy-loss parameters are chosen adaptively (i.e. privacy filters and odometers) Rogers et al. [2016], Haney et al. [2023]
- Differential privacy and the Statistical Query model for machine learning: Blum et al. [2005], Kasiviswanathan et al. [2011]
- The paper that introduced the exponential mechanism: McSherry and Talwar [2007]
- Another mechanism for the median (via smooth sensitivity): Kasiviswanathan et al. [2013]
- Survey of approaches to add noise closer to the local sensitivity: [Vadhan, 2017, Ch. 3]

- Implementing Differential Privacy: One-Shot Releases
  - The stability-based histogram and other histogram algorithms for large data universes: Korolova et al. [2009], Balcer and Vadhan [2018]
  - Paper on Wikimedia Foundation use of DP Adeleye et al. [2023]
  - Early applications of DP synthetic data to commuting patterns and mobility data: Machanavajjhala et al. [2008], Mir et al. [2013]
  - Census Bureau's TopDown Algorithm and some other studies of it: JASON [2022], Bureau et al. [2023], Abowd et al. [2022], Gong et al. [2022]
  - Differentially private synthetic data generation: Hardt and Rothblum [2010], Hardt et al. [2012], Gaboardi et al. [2017], McKenna et al. [2022], Vietri et al. [2022], Liu et al. [2023], see also [Cowan et al., 2024, Ch. 10]
  - The Opportunity Atlas and the underlying privacy mechanism: Chetty et al. [2018], Chetty and Friedman [2019]
  - Use of DP to study the New Digital Divide Pereira et al. [2024]
  - An approach to comparing DP algorithms: Hay et al. [2016a]

- Communicating Differential Privacy to Data Subjects
  - Spinner explanation of randomized response technique Bullek et al. [2017]
  - Explanations of ϵ Nanayakkara et al. [2023], Franzen et al. [2022], Smart et al. [2022], Wood et al. [2018a]
  - Metaphors Karegar et al. [2022], Smart et al. [2024]
  - Local vs. central model Smart et al. [2024], Xiong et al. [2023]
  - Textual descriptions Cummings et al. [2021], Xiong et al. [2020]
  - For a more comprehensive set of references, see Dibia et al. [2024]

- Machine Learning and Statistical Inference with DP
  - "A Primer on Private Statistics" Kamath and Ullman [2020]
  - "How to DP-fy ML: A Practical Guide to Machine Learning with Differential Privacy," Ponomareva et al. [2023]
  - Large models can memorize their training data: Zhang et al. [2017], Carlini et al. [2018, 2021, 2023] (See also Membership Inference attacks on ML from the Attacks section of the course.)
  - 2022 state of art in training large models with DP Bu et al. [2022], Klause et al. [2022], De et al. [2022]
  - Near-tightness of current analyses of DP-SGD Nasr et al. [2023].

- DP as a protection against overfitting: Dwork et al. [2015a], Bassily et al. [2016]
- Output perturbation and objective perturbation: Chaudhuri et al. [2011].
- Differentially private PAC learning, the exponential mechanism for differentially private learning, and the equivalence between SQ learning and local DP learning: Vadhan [2017, Ch. 8], Kasiviswanathan et al. [2011].
- Negative results for differentially private PAC learning (requires finite data universes even for simple models like threshold functions, can require computing time exponential in dimensionality): Bun and Zhandry [2016], Alon et al. [2018]
- Differentially private gradient descent and stochastic gradient descent in the centralized and local models: Williams and Mcsherry [2010], Jain et al. [2012], Song et al. [2013], Bassily et al. [2014], Abadi et al. [2016], Duchi et al. [2014], Smith et al. [2017]
- Survey on federated learning and privacy: Bonawitz et al. [2022]
- Background on machine learning (without privacy): Kearns and Vazirani [1994], Stanford cs231 lecture notes, Deep learning tutorial, Tensorflow visual demo

• Implementing Differential Privacy: Programming Frameworks, Query Systems, and Interfaces

- Survey on programming frameworks for DP Gaboardi et al. [2024]
- Survey on differential privacy for databases Near and He [2021]
- Timing attacks on implementations of DP and defenses: Haeberlen et al. [2011], Jin et al. [2022], Ben Dov et al. [2023], Ratliff and Vadhan [2024]
- Survey on formal verification of DP and recent developments: Barthe et al. [2016], Zhang and Kifer [2017], Albarghouthi and Hsu [2017]
- Interactive paradigms and interfaces for data analysts, data curators: Gaboardi et al. [2018], Nanayakkara et al., St. John et al. [2021], Bittner et al. [2020], Thaker et al. [2020], Hay et al. [2016c], Nanayakkara et al. [2024]

• Distributed Models of DP

- Tutorial: Cormode et al. [2018], see also videos online
- Survey talk by Adam Smith: `http://www.bu.edu/hic/files/2018/06/2018-06-05-Adam.Smith_.pptx` (Change file extension to `.pdf` to open.)
- History of randomized response in the survey literature, and some current applications: Gingerich [2015, 2010], Blair et al. [2015]
- Equivalence of local DP and the SQ model: Kasiviswanathan et al. [2011]
- The Shuffle Model: Bittau et al. [2017], Cheu et al. [2019], Erlingsson et al. [2019], Balle et al. [2019], Feldman et al. [2022], Cheu [2022]
- Differential Privacy meets Multiparty Computation workshop: `http://www.bu.edu/hic/dpmpc-2018/`
- Recent papers on combining DP and secure multiparty computation, including privacy-preserving randomized control trials: He et al. [2017], Archer et al. [2018], Movahedi et al. [2021]
- Google's RAPPOR: Erlingsson et al. [2014]
- Apple's "learning with privacy at scale": `https://machinelearning.apple.com/2017/12/06/learning-with-privacy-at-scale.html`
- Microsoft's "Collecting telemetry data privately": `https://www.microsoft.com/en-us/research/blog/collecting-telemetry-data-privately/`, Ding et al. [2017]
- Critiques of deployments of local DP: `https://www.wired.com/story/apple-differential-privacy-shortcom`, Tang et al. [2017]

- Local DP for Evolving Data: Joseph et al. [2018]

- Evaluating Utility of Downstream Analyses
  - Utility of Census data protected under DP for redistricting Kenny et al. [2021], Cohen et al. [2022] and funding allocation Steed et al. [2022], and impacts on counts of minority groups Radway and Christ [2023]
  - Evaluating and comparing accuracy across differentially-private algorithms Hay et al. [2016b]

- Societal Perspectives on (Differential) Privacy
  - Contextual Integrity and an Attempt to Integrate it with DP: Nissenbaum [2009], Benthall and Cummings [2024].
  - Law & Policy: Nissim and Wood [2018], Solove [2006], Cohen [2013], Altman et al. [2021]
  - Science and Technology Studies: Winner [1980], Green and Viljoen [2020], Mulligan et al. [2017], Sarathy [2022], boyd and Sarathy [2022], Abdu et al. [2024]

- Software
  - See Gaboardi et al. [2024] for a more updated list.
  - OpenDP: `http://opendp.org/`
  - Tumult Analytics: `http://tumult.dev/`
  - Opacus (DP for Pytorch ML models): `https://opacus.ai/`
  - JAX-Privacy: `https://github.com/google-deepmind/jax_privacy`
  - TensorFlow Privacy: `https://github.com/tensorflow/privacy`
  - ViP (for visualizing privacy budget tradeoffs): `https://priyakalot.github.io/ViP-demo/`
  - DualQuery: `https://github.com/ejgallego/dualquery`
  - MWEM: `https://github.com/mrtzh/PrivateMultiplicativeWeights.jl`
  - PinQ: `https://www.microsoft.com/en-us/download/details.aspx?id=52363`
  - εktelo: `https://ektelo.github.io/`
  - FLEX (SQL, deployed by Uber): `http://www.uvm.edu/~jnear/elastic/`
  - PSI: `http://psiprivacy.org/about/`
  - LightDP: `https://github.com/RyanWangGit/lightdp`
  - RAPPOR: `https://github.com/google/rappor`
  - Prochlo: `https://github.com/google/prochlo`
  - DPComp (for comparing DP algorithms): `https://www.dpcomp.org/`
  - Membership Inference Attacks: `https://www.comp.nus.edu.sg/~reza/files/datasets.html`
  - DiffPriv (Easy Differential Privacy): `https://cran.r-project.org/web/packages/diffpriv/index.html`
  - DPML (Differentially Private Convex Optimization, including SGD): `https://github.com/sunblaze-ucb/dpml-benchmark`

References

Martin Abadi, Andy Chu, Ian Goodfellow, H. Brendan McMahan, Ilya Mironov, Kunal Talwar, and Li Zhang. Deep learning with differential privacy. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, CCS '16, pages 308–318, New York, NY, USA, 2016. ACM. ISBN 978-1-4503-4139-4. doi: 10.1145/2976749.2978318. URL http://doi.acm.org/10.1145/2976749.2978318.

Amina A Abdu, Lauren M Chambers, Deirdre K Mulligan, and Abigail Z Jacobs. Algorithmic transparency and participation through the handoff lens: Lessons learned from the us census bureau's adoption of differential privacy. In *Proceedings of the 2024 ACM Conference on Fairness, Accountability, and Transparency*, pages 1150–1162, 2024.

John M. Abowd, Robert Ashmead, Ryan Cumings-Menon, Simson Garfinkel, Micah Heineck, Christine Heiss, Robert Johns, Daniel Kifer, Philip Leclerc, Ashwin Machanavajjhala, Brett Moran, William Sexton, Matthew Spence, and Pavel Zhuravlev. The 2020 Census Disclosure Avoidance System TopDown Algorithm. *Harvard Data Science Review*, (Special Issue 2), jun 24 2022. https://hdsr.mitpress.mit.edu/pub/7evz361i.

Temilola Adeleye, Skye Berghel, Damien Desfontaines, Michael Hay, Isaac Johnson, Cléo Lemoisson, Ashwin Machanavajjhala, Tom Magerlein, Gabriele Modena, David Pujol, Daniel Simmons-Marengo, and Hal Triedman. Publishing wikipedia usage data with strong privacy guarantees. *CoRR*, abs/2308.16298, 2023. doi: 10.48550/ARXIV.2308.16298. URL https://doi.org/10.48550/arXiv.2308.16298.

Aws Albarghouthi and Justin Hsu. Synthesizing coupling proofs of differential privacy. *Proc. ACM Program. Lang.*, 2(POPL):58:1–58:30, December 2017. ISSN 2475-1421. doi: 10.1145/3158146. URL http://doi.acm.org/10.1145/3158146.

Noga Alon, Roi Livni, Maryanthe Malliaris, and Shay Moran. Private PAC learning implies finite littlestone dimension. *CoRR*, abs/1806.00949, 2018. URL http://arxiv.org/abs/1806.00949.

Micah Altman, Aloni Cohen, Kobbi Nissim, and Alexandra Wood. What a hybrid legal-technical analysis teaches us about privacy regulation: The case of singling out. *BU School of Law Journal of Science Technology Law*, 27(1), 2021.

David W. Archer, Dan Bogdanov, Liina Kamm, Y. Lindell, Kurt Nielsen, Jakob Illeborg Pagter, Nigel P. Smart, and Rebecca N. Wright. From keys to databases – real-world applications of secure multi-party computation. Cryptology ePrint Archive, Report 2018/450, 2018. https://eprint.iacr.org/2018/450.

Victor Balcer and Salil Vadhan. Differential Privacy on Finite Computers. In Anna R. Karlin, editor, *9th Innovations in Theoretical Computer Science Conference (ITCS 2018)*, volume 94 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 43:1–43:21, Dagstuhl, Germany, 2018. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik. ISBN 978-3-95977-060-6. doi: 10.4230/LIPIcs.ITCS.2018.43. URL http://drops.dagstuhl.de/opus/volltexte/2018/8353.

Borja Balle, James Bell, Adrià Gascón, and Kobbi Nissim. The privacy blanket of the shuffle model. *CoRR*, abs/1903.02837, 2019. URL http://arxiv.org/abs/1903.02837.

Michael Barbaro and Tom Zeller, Jr. A face is exposed for AOL searcher no. 4417749. *The New York Times*, 9 August 2006. URL https://www.nytimes.com/2006/08/09/technology/09aol.html.

Gilles Barthe, Marco Gaboardi, Justin Hsu, and Benjamin Pierce. Programming language techniques for differential privacy. *ACM SIGLOG News*, 3(1):34–53, February 2016. ISSN 2372-3491. doi: 10.1145/2893582.2893591. URL http://doi.acm.org/10.1145/2893582.2893591.

Raef Bassily, Adam Smith, and Abhradeep Thakurta. Private empirical risk minimization: efficient algorithms and tight error bounds. In *55th Annual IEEE Symposium on Foundations of Computer Science—FOCS 2014*, pages 464–473. IEEE Computer Soc., Los Alamitos, CA, 2014. doi: 10.1109/FOCS.2014.56. URL http://dx.doi.org/10.1109/FOCS.2014.56.

Raef Bassily, Kobbi Nissim, Adam Smith, Thomas Steinke, Uri Stemmer, and Jonathan Ullman. Algorithmic stability for adaptive data analysis. In *48th Annual Symposium on the Theory of Computing (STOC'16)*, June 2016. Preliminary version available at http://arxiv.org/abs/1511.02513.

Yoav Ben Dov, Liron David, Moni Naor, and Elad Tzalik. Resistance to Timing Attacks for Sampling and Privacy Preserving Schemes. In Kunal Talwar, editor, *4th Symposium on Foundations of Responsible Computing (FORC 2023)*, volume 256 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 11:1–11:23, Dagstuhl, Germany, 2023. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. ISBN 978-3-95977-272-3. doi: 10.4230/LIPIcs.FORC.2023.11. URL https://drops.dagstuhl.de/entities/document/10.4230/LIPIcs.FORC.2023.11.

Sebastian Benthall and Rachel Cummings. Integrating differential privacy and contextual integrity. In *Proceedings of the Symposium on Computer Science and Law*, CSLAW '24, page 9–15, New York, NY, USA, 2024. Association for Computing Machinery. ISBN 9798400703331. doi: 10.1145/3614407.3643702. URL https://doi.org/10.1145/3614407.3643702.

Andrea Bittau, Úlfar Erlingsson, Petros Maniatis, Ilya Mironov, Ananth Raghunathan, David Lie, Mitch Rudominer, Ushasree Kode, Julien Tinnes, and Bernhard Seefeld. Prochlo: Strong privacy for analytics in the crowd. In *Proceedings of the 26th Symposium on Operating Systems Principles*, SOSP '17, pages 441–459, New York, NY, USA, 2017. ACM. ISBN 978-1-4503-5085-3. doi: 10.1145/3132747.3132769. URL http://doi.acm.org/10.1145/3132747.3132769.

Daniel M Bittner, Alejandro E Brito, Mohsen Ghassemi, Shantanu Rane, Anand D Sarwate, and Rebecca N Wright. Understanding Privacy-Utility Tradeoffs in Differentially Private Online Active Learning. *Journal of Privacy and Confidentiality*, 10(2), 2020.

Graeme Blair, Kosuke Imai, and Yang-Yang Zhou. Design and analysis of the randomized response technique. *Journal of the American Statistical Association*, 110(511):1304–1319, 2015.

Avrim Blum, Cynthia Dwork, Frank McSherry, and Kobbi Nissim. Practical privacy: the SuLQ framework. In *Proceedings of the 24th ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems*, pages 128–138. ACM, 2005.

Kallista Bonawitz, Peter Kairouz, Brendan Mcmahan, and Daniel Ramage. Federated learning and privacy. *Commun. ACM*, 65(4):90–97, March 2022. ISSN 0001-0782. doi: 10.1145/3500240. URL https://doi.org/10.1145/3500240.

danah boyd and Jayshree Sarathy. Differential perspectives: Epistemic disconnects surrounding the us census bureau's use of differential privacy. *Harvard Data Science Review*, 2022.

Zhiqi Bu, Jialin Mao, and Shiyun Xu. Scalable and efficient training of large convolutional neural networks with differential privacy. In Sanmi Koyejo, S. Mohamed, A. Agarwal, Danielle Belgrave, K. Cho, and A. Oh, editors, *Advances in Neural Information Processing Systems 35: Annual Conference on Neural Information Processing Systems 2022, NeurIPS 2022, New Orleans, LA, USA, November 28 - December 9, 2022*, 2022. URL http://papers.nips.cc/paper_files/paper/2022/hash/fa5617c176e76fee83f3f9947fdf9f3f-Abstract-Conference.html.

Brooke Bullek, Stephanie Garboski, Darakhshan J Mir, and Evan M Peck. Towards understanding differential privacy: When do people trust randomized response technique? In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, pages 3833–3837, 2017.

Mark Bun and Thomas Steinke. Concentrated differential privacy: Simplifications, extensions, and lower bounds. *CoRR*, abs/1605.02065, 2016. URL http://arxiv.org/abs/1605.02065.

Mark Bun and Mark Zhandry. Order-revealing encryption and the hardness of private learning. In *Theory of Cryptography Conference (TCC '16A)*, pages 176–206. Springer, 10–13 January 2016. Full version available at https://eprint.iacr.org/2015/417.

Mark Bun, Damien Desfontaines, Cynthia Dwork, Moni Naor, Kobbi Nissim, Aaron Roth, Adam Smith, Thomas Steinke, Jon Ullman, and Salil Vadhan. Statistical inference is not a privacy violation. Blog post on *differentialprivacy.org*, 3 June 2021. URL https://differentialprivacy.org/inference-is-not-a-privacy-violation/.

The Population Reference Bureau, the U.S. Census Bureau's 2020 Census Data Products, and Dissemination Team. Disclosure avoidance and the 2020 census: How the topdown algorithm works. 2020 Census Briefs C2020BR-04, March 2023. URL https://www2.census.gov/library/publications/decennial/2020/census-briefs/c2020br-04.pdf.

Nicholas Carlini, Chang Liu, Jernej Kos, Úlfar Erlingsson, and Dawn Song. The secret sharer: Measuring unintended neural network memorization & extracting secrets. *CoRR*, abs/1802.08232, 2018. URL http://arxiv.org/abs/1802.08232.

Nicholas Carlini, Florian Tramèr, Eric Wallace, Matthew Jagielski, Ariel Herbert-Voss, Katherine Lee, Adam Roberts, Tom B. Brown, Dawn Song, Úlfar Erlingsson, Alina Oprea, and Colin Raffel. Extracting training data from large language models. In Michael D. Bailey and Rachel Greenstadt, editors, *30th USENIX Security Symposium, USENIX Security 2021, August 11-13, 2021*, pages 2633–2650. USENIX Association, 2021. URL https://www.usenix.org/conference/usenixsecurity21/presentation/carlini-extracting.

Nicholas Carlini, Steve Chien, Milad Nasr, Shuang Song, Andreas Terzis, and Florian Tramèr. Membership inference attacks from first principles. In *43rd IEEE Symposium on Security and Privacy, SP 2022, San Francisco, CA, USA, May 22-26, 2022*, pages 1897–1914. IEEE, 2022. doi: 10.1109/SP46214.2022.9833649. URL https://doi.org/10.1109/SP46214.2022.9833649.

Nicholas Carlini, Jamie Hayes, Milad Nasr, Matthew Jagielski, Vikash Sehwag, Florian Tramèr, Borja Balle, Daphne Ippolito, and Eric Wallace. Extracting training data from diffusion models. In Joseph A. Calandrino and Carmela Troncoso, editors, *32nd USENIX Security Symposium, USENIX Security 2023, Anaheim, CA, USA, August 9-11, 2023*, pages 5253–5270. USENIX Association, 2023. URL https://www.usenix.org/conference/usenixsecurity23/presentation/carlini.

Sílvia Casacuberta, Michael Shoemate, Salil Vadhan, and Connor Wagaman. Widespread underestimation of sensitivity in differentially private libraries and how to fix it. In *Proceedings of the 29th ACM SIGSAC Conference on Computer and Communications Security (CCS '22)*, page 471–484, 7–11 November 2022. ISBN 9781450394505. doi: 10.1145/3548606.3560708. Preprint posted as arXiv:2207.10635 [cs.CR].

Ann Cavoukian and Daniel Castro. Big data and innovation, setting the record straight: De-identification *does* work. Information and Privacy Commissioner, Ontario, Canada, June 2014. https://itif.org/publications/2014/06/16/setting-record-straight-de-identification-does-work/.

Ann Cavoukian and Khaled El Emam. De-identification protocols: Essential for protecting privacy. Information and Privacy Commissioner, Ontario, Canada, June 2014. https://www.ipc.on.ca/resource/de-identification-protocols-essential-for-protecting-privacy/.

Kamalika Chaudhuri, Claire Monteleoni, and Anand D. Sarwate. Differentially private empirical risk minimization. *J. Mach. Learn. Res.*, 12:1069–1109, July 2011. ISSN 1532-4435. URL http://dl.acm.org/citation.cfm?id=1953048.2021036.

Raj Chetty and John Friedman. A practical method to reduce privacy loss when disclosing statistics based on small samples. *American Economic Review Papers and Proceedings*, May 2019. URL https://opportunityinsights.org/paper/. To appear.

Raj Chetty, John Friedman, Nathaniel Hendren, Maggie R. Jones, and Sonya R. Porter. The opportunity atlas: Mapping the childhood roots of social mobility. Working Paper, October 2018. URL https://opportunityinsights.org/paper/.

Albert Cheu. Differential privacy in the shuffle model: A survey of separations, 2022. URL https://arxiv.org/abs/2107.11839.

Albert Cheu, Adam Smith, Jonathan Ullman, David Zeber, and Maxim Zhilyaev. Distributed differential privacy via shuffling. Cryptology ePrint Archive, Report 2019/245, 2019. https://eprint.iacr.org/2019/245.

Aloni Cohen. Attacks on deidentification's defenses. In Kevin R. B. Butler and Kurt Thomas, editors, *31st USENIX Security Symposium, USENIX Security 2022, Boston, MA, USA, August 10-12, 2022*, pages 1469–1486. USENIX Association, 2022. URL https://www.usenix.org/conference/usenixsecurity22/presentation/cohen.

Aloni Cohen and Kobbi Nissim. Linear program reconstruction in practice. *CoRR*, abs/1810.05692, 2018. URL http://arxiv.org/abs/1810.05692.

Aloni Cohen, Moon Duchin, JN Matthews, and Bhushan Suwal. Census topdown: The impacts of differential privacy on redistricting. *arXiv preprint arXiv:2203.05085*, 2022.

Julie E. Cohen. What privacy is for. *Harvard Law Review*, 126, May 2013.

P3G Consortium, George Church, Catherine Heeney, Naomi Hawkins, Jantina de Vries, Paula Boddington, Jane Kaye, Martin Bobrow, and Bruce Weir. Public access to genome-wide data: Five views on balancing research with privacy and protection. *PLOS Genetics*, 5(10):1–4, 10 2009. doi: 10.1371/journal.pgen.1000665. URL https://doi.org/10.1371/journal.pgen.1000665.

Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, and Clifford Stein. *Introduction to Algorithms, Third Edition*. The MIT Press, 3rd edition, 2009. ISBN 0262033844, 9780262033848. URL https://mitpress.mit.edu/books/introduction-algorithms-third-edition.

Graham Cormode, Somesh Jha, Tejas Kulkarni, Ninghui Li, Divesh Srivastava, and Tianhao Wang. Privacy at scale: Local differential privacy in practice. In *Proceedings of the 2018 International Conference on Management of Data*, SIGMOD '18, pages 1655–1658, New York, NY, USA, 2018. ACM. ISBN 978-1-4503-4703-7. doi: 10.1145/3183713.3197390. URL http://doi.acm.org/10.1145/3183713.3197390.

Ethan Cowan, Michael Shoemate, and Mayana Pereira. *Hands-On Differential Privacy*. O'Reilly Media, 2024. URL https://www.oreilly.com/library/view/hands-on-differential-privacy/9781492097730/.

Rachel Cummings, Gabriel Kaptchuk, and Elissa M Redmiles. " i need a better description": An investigation into user expectations for differential privacy. In *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, pages 3037–3052, 2021.

Rachel Cummings, Damien Desfontaines, David Evans, Roxana Geambasu, Yangsibo Huang, Matthew Jagielski, Peter Kairouz, Gautam Kamath, Sewoong Oh, Olga Ohrimenko, Nicolas Papernot, Ryan Rogers, Milan Shen, Shuang Song, Weijie Su, Andreas Terzis, Abhradeep Thakurta, Sergei Vassilvitskii, Yu-Xiang Wang, Li Xiong, Sergey Yekhanin, Da Yu, Huanyu Zhang, and Wanrong Zhang. Advancing Differential Privacy: Where We Are Now and Future Directions for Real-World Deployment. *Harvard Data Science Review*, 6(1), jan 16 2024. https://hdsr.mitpress.mit.edu/pub/sl9we8gh.

Jon P. Daries, Justin Reich, Jim Waldo, Elise M. Young, Jonathan Whittinghill, Andrew Dean Ho, Daniel Thomas Seaton, and Isaac Chuang. Privacy, anonymity, and big data in the social sciences. *Communication of the ACM*, 57(9):56–63, September 2014. ISSN 0001-0782. doi: 10.1145/2643132. URL http://doi.acm.org/10.1145/2643132.

Soham De, Leonard Berrada, Jamie Hayes, Samuel L. Smith, and Borja Balle. Unlocking high-accuracy differentially private image classification through scale, 2022. URL https://arxiv.org/abs/2204.13650.

Damien Desfontaines. A list of real-world uses of differential privacy. https://desfontain.es/privacy/real-world-differential-privacy.html, 2021. Blog post (last updated 10/21).

Onyinye Dibia, Brad Stenger, Steven Baldasty, Mako Bates, Ivoline C Ngong, Yuanyuan Feng, and Joseph P Near. Sok: Usability studies in differential privacy. *arXiv preprint arXiv:2412.16825*, 2024.

Travis Dick, Cynthia Dwork, Michael Kearns, Terrance Liu, Aaron Roth, Giuseppe Vietri, and Zhiwei Steven Wu. Confidence-ranked reconstruction of census microdata from published statistics. *Proceedings of the National Academy of Sciences*, 120(8):e2218605120, 2023. doi: 10.1073/pnas.2218605120. URL https://www.pnas.org/doi/abs/10.1073/pnas.2218605120.

Bolin Ding, Janardhan Kulkarni, and Sergey Yekhanin. Collecting telemetry data privately. In Isabelle Guyon, Ulrike von Luxburg, Samy Bengio, Hanna M. Wallach, Rob Fergus, S. V. N. Vishwanathan, and Roman Garnett, editors, *Advances in Neural Information Processing Systems 30: Annual Conference on Neural Information Processing Systems 2017, 4-9 December 2017, Long Beach, CA, USA*, pages 3574–3583, 2017. URL http://papers.nips.cc/paper/6948-collecting-telemetry-data-privately.

Irit Dinur and Kobbi Nissim. Revealing information while preserving privacy. In *Proceedings of the Twenty-second ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems*, PODS '03, pages 202–210, New York, NY, USA, 2003. ACM. doi: 10.1145/773153.773173.

Jinshuo Dong, Aaron Roth, and Weijie J. Su. Gaussian differential privacy. *Journal of the Royal Statistical Society Series B: Statistical Methodology*, 84(1):3–37, 02 2022. ISSN 1369-7412. doi: 10.1111/rssb.12454. URL https://doi.org/10.1111/rssb.12454.

Vadym Doroshenko, Badih Ghazi, Pritish Kamath, Ravi Kumar, and Pasin Manurangsi. Connect the dots: Tighter discrete approximations of privacy loss distributions. *Proc. Priv. Enhancing Technol.*, 2022(4):552–570, 2022. doi: 10.56553/POPETS-2022-0122. URL https://doi.org/10.56553/popets-2022-0122.

John C. Duchi, Michael I. Jordan, and Martin J. Wainwright. Privacy aware learning. *Journal of the ACM*, 61(6):Art. 38, 57, 2014. ISSN 0004-5411. doi: 10.1145/2666468. URL http://dx.doi.org/10.1145/2666468.

Cynthia Dwork and Kobbi Nissim. Privacy-preserving datamining on vertically partitioned databases. In *Advances in Cryptology–CRYPTO 2004*, pages 528–544. Springer, 2004.

Cynthia Dwork and Aaron Roth. The algorithmic foundations of differential privacy. *Foundations and Trends® in Theoretical Computer Science*, 9(3–4):211–407, 2013. ISSN 1551-305X. doi: 10.1561/0400000042. URL http://dx.doi.org/10.1561/0400000042.

Cynthia Dwork and Guy N. Rothblum. Concentrated differential privacy. *CoRR*, abs/1603.01887, 2016. URL http://arxiv.org/abs/1603.01887.

Cynthia Dwork, Guy Rothblum, and Salil Vadhan. Boosting and differential privacy. In *Proceedings of the 51st Annual IEEE Symposium on Foundations of Computer Science (FOCS '10)*, pages 51–60. IEEE, 23–26 October 2010.

Cynthia Dwork, Vitaly Feldman, Moritz Hardt, Toniann Pitassi, Omer Reingold, and Aaron Roth. The reusable holdout: Preserving validity in adaptive data analysis. *Science*, 349(6248):636–638, 2015a. ISSN 0036-8075. doi: 10.1126/science.aaa9375. URL https://science.sciencemag.org/content/349/6248/636.

Cynthia Dwork, Adam Smith, Thomas Steinke, Jonathan Ullman, and Salil Vadhan. Robust traceability from trace amounts. In *Proceedings of the 2015 IEEE 56th Annual Symposium on Foundations of Computer Science (FOCS)*, FOCS '15, pages 650–669, Washington, DC, USA, 2015b. IEEE Computer Society. ISBN 978-1-4673-8191-8. doi: 10.1109/FOCS.2015.46. URL http://dx.doi.org/10.1109/FOCS.2015.46.

Cynthia Dwork, Frank McSherry, Kobbi Nissim, and Adam Smith. Calibrating noise to sensitivity in private data analysis. *Journal of Privacy and Confidentiality*, 7(3), 2016. To appear. Preliminary version in *Proc. TCC '06*.

Cynthia Dwork, Adam Smith, Thomas Steinke, and Jonathan Ullman. Exposed! a survey of attacks on private data. *Annual Review of Statistics and Its Application*, 4(1):61–84, 2017. doi: 10.1146/annurev-statistics-060116-054123. URL https://doi.org/10.1146/annurev-statistics-060116-054123.

Úlfar Erlingsson, Vasyl Pihur, and Aleksandra Korolova. Rappor: Randomized aggregatable privacy-preserving ordinal response. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, CCS '14, pages 1054–1067, New York, NY, USA, 2014. ACM. ISBN 978-1-4503-2957-6. doi: 10.1145/2660267.2660348. URL http://doi.acm.org/10.1145/2660267.2660348.

Úlfar Erlingsson, Vitaly Feldman, Ilya Mironov, Ananth Raghunathan, Kunal Talwar, and Abhradeep Thakurta. Amplification by shuffling: From local to central differential privacy via anonymity. In *Proceedings of the Thirtieth Annual ACM-SIAM Symposium on Discrete Algorithms*, SODA '19, pages 2468–2479, Philadelphia, PA, USA, 2019. Society for Industrial and Applied Mathematics. URL http://dl.acm.org/citation.cfm?id=3310435.3310586.

Vitaly Feldman, Audra McMillan, and Kunal Talwar. Hiding among the clones: A simple and nearly optimal analysis of privacy amplification by shuffling. In *2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS)*, pages 954–964, 2022. doi: 10.1109/FOCS52979.2021.00096.

Daniel Franzen, Saskia Nuñez von Voigt, Peter Sörries, Florian Tschorsch, and Claudia Müller-Birn. Am i private and if so, how many? communicating privacy guarantees of differential privacy with risk communication formats. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, pages 1125–1139, 2022.

Matthew Fredrikson, Eric Lantz, Somesh Jha, Simon Lin, David Page, and Thomas Ristenpart. Privacy in pharmacogenetics: An end-to-end case study of personalized warfarin dosing. In Kevin Fu and Jaeyeon Jung, editors, *Proceedings of the 23rd USENIX Security Symposium, San Diego, CA, USA, August 20-22, 2014.*, pages 17–32. USENIX Association, 2014. URL https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/fredrikson_matthew.

Marco Gaboardi, Emilio Gallego Arias, Justin Hsu, Aaron Roth, and Zhiwei Wu. Dual query: Practical private query release for high dimensional data. *Journal of Privacy and Confidentiality*, 7(2), 2017. doi: 10.29012/jpc.v7i2.650. URL https://doi.org/10.29012/jpc.v7i2.650.

Marco Gaboardi, James Honaker, Gary King, Jack Murtagh, Kobbi Nissim, Jonathan Ullman, and Salil Vadhan. PSI (Ψ): a Private data Sharing Interface, 2018.

Marco Gaboardi, Michael Hay, and Salil Vadhan. Programming frameworks for differential privacy. arXiv:2403.11088 [cs.CR], 2024. URL https://arxiv.org/abs/2403.11088. To appear as a chapter in *Differential Privacy in Artificial Intelligence—From Theory to Practice*.

Srivatsava Ranjit Ganta, Shiva Prasad Kasiviswanathan, and Adam Smith. Composition attacks and auxiliary information in data privacy. In *Proceedings of the 14th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, KDD '08, pages 265–273, New York, NY, USA, 2008. ACM. ISBN 978-1-60558-193-4. doi: 10.1145/1401890.1401926. URL http://doi.acm.org/10.1145/1401890.1401926.

Simson Garfinkel, John M. Abowd, and Christian Martindale. Understanding database reconstruction attacks on public data. *Queue*, 16(5):50:28–50:53, October 2018. ISSN 1542-7730. doi: 10.1145/3291276.3295691. URL http://doi.acm.org/10.1145/3291276.3295691.

A. Ghosh, T. Roughgarden, and M. Sundararajan. Universally utility-maximizing privacy mechanisms. *SIAM Journal on Computing*, 41(6):1673–1693, 2012. doi: 10.1137/09076828X. URL https://doi.org/10.1137/09076828X.

Daniel Gingerich. Randomized response: Foundations and new developments. *Comparative Politics Newsletter (The Organized Section in Comparative Politics of the American Political Science Association)*, 25(1): 16–27, 2015.

Daniel W Gingerich. Understanding off-the-books politics: Conducting inference on the determinants of sensitive behavior with randomized response surveys. *Political Analysis*, 18(3):349–380, 2010.

Philippe Golle. Revisiting the uniqueness of simple demographics in the us population. In *Proceedings of the 5th ACM Workshop on Privacy in Electronic Society*, WPES '06, pages 77–80, New York, NY, USA, 2006. ACM. ISBN 1-59593-556-8. doi: 10.1145/1179601.1179615. URL http://doi.acm.org/10.1145/1179601.1179615.

Ruobin Gong, Erica L. Groshen, and Salil Vadhan, editors. *Special Issue on Differential Privacy for the 2020 U.S. Census: Can We Make Data Both Private and Useful?* Harvard Data Science Review. June 2022. URL https://hdsr.mitpress.mit.edu/specialissue2.

Ben Green and Salomé Viljoen. Algorithmic realism: expanding the boundaries of algorithmic thought. In *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency*, FAT* '20, page 19–31, New York, NY, USA, 2020. Association for Computing Machinery. ISBN 9781450369367. doi: 10.1145/3351095.3372840. URL https://doi.org/10.1145/3351095.3372840.

Andreas Haeberlen, Benjamin C. Pierce, and Arjun Narayan. Differential privacy under fire. In *Proceedings of the 20th USENIX Conference on Security*, SEC'11, pages 33–33, Berkeley, CA, USA, 2011. USENIX Association. URL http://dl.acm.org/citation.cfm?id=2028067.2028100.

Samuel Haney, Damien Desfontaines, Luke Hartman, Ruchit Shrestha, and Michael Hay. Precision-based attacks and interval refining: how to break, then fix, differential privacy on finite computers. *CoRR*, abs/2207.13793, 2022. doi: 10.48550/ARXIV.2207.13793. URL https://doi.org/10.48550/arXiv.2207.13793.

Samuel Haney, Michael Shoemate, Grace Tian, Salil P. Vadhan, Andrew Vyrros, Vicki Xu, and Wanrong Zhang. Concurrent composition for interactive differential privacy with adaptive privacy-loss parameters. In Weizhi Meng, Christian Damsgaard Jensen, Cas Cremers, and Engin Kirda, editors, *Proceedings of the 30th ACM SIGSAC Conference on Computer and Communications Security (CCS '23)*, pages 1949–1963. ACM, 2023. doi: 10.1145/3576915.3623128. URL https://doi.org/10.1145/3576915.3623128. Received a CCS '23 Distinguished Paper Award and invited to Special Issue of *J. Privacy & Confidentiality* on TPDP '23. Preliminary version presented as a poster at TPDP '23 and posted as arXiv:2309.05901 [cs.CR].

Moritz Hardt and Guy N. Rothblum. A multiplicative weights mechanism for privacy-preserving data analysis. In *Proceedings of the 51st Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 61–70, Oct 2010. doi: 10.1109/FOCS.2010.85.

Moritz Hardt, Katrina Ligett, and Frank McSherry. A simple and practical algorithm for differentially private data release. In *Proceedings of the 25th International Conference on Neural Information Processing Systems - Volume 2*, NIPS'12, pages 2339–2347, USA, 2012. Curran Associates Inc. URL http://dl.acm.org/citation.cfm?id=2999325.2999396.

Michael Hay, Ashwin Machanavajjhala, Gerome Miklau, Yan Chen, and Dan Zhang. Principled evaluation of differentially private algorithms using dpbench. In *Proceedings of the 2016 International Conference on Management of Data*, SIGMOD '16, pages 139–154, New York, NY, USA, 2016a. ACM. ISBN 978-1-4503-3531-7. doi: 10.1145/2882903.2882931. URL http://doi.acm.org/10.1145/2882903.2882931.

Michael Hay, Ashwin Machanavajjhala, Gerome Miklau, Yan Chen, and Dan Zhang. Principled evaluation of differentially private algorithms using dpbench. In *Proceedings of the 2016 International Conference on Management of Data*, pages 139–154, 2016b.

Michael Hay, Ashwin Machanavajjhala, Gerome Miklau, Yan Chen, Dan Zhang, and George Bissias. Exploring privacy-accuracy tradeoffs using dpcomp. In *Proceedings of the 2016 International Conference on Management of Data*, pages 2101–2104, 2016c.

Xi He, Ashwin Machanavajjhala, Cheryl Flynn, and Divesh Srivastava. Composing differential privacy and secure computation: A case study on scaling private record linkage. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, CCS '17, pages 1389–1406, New York, NY, USA, 2017. ACM. ISBN 978-1-4503-4946-8. doi: 10.1145/3133956.3134030. URL http://doi.acm.org/10.1145/3133956.3134030.

Nils Homer, Szabolcs Szelinger, Margot Redman, David Duggan, Waibhav Tembe, Jill Muehling, John V Pearson, Dietrich A Stephan, Stanley F Nelson, and David W Craig. Resolving individuals contributing trace amounts of dna to highly complex mixtures using high-density snp genotyping microarrays. *PLoS genetics*, 4(8):e1000167, 2008. URL https://doi.org/10.1371/journal.pgen.1000167.

V. Joseph Hotz, Christopher R. Bollinger, Tatiana Komarova, Charles F. Manski, Robert A. Moffitt, Denis Nekipelov, Aaron Sojourner, and Bruce D. Spencer. Balancing data privacy and usability in the federal statistical system. *Proceedings of the National Academy of Sciences*, 119(31):e2104906119, 2022. doi: 10.1073/pnas.2104906119. URL https://www.pnas.org/doi/abs/10.1073/pnas.2104906119.

Jessica Hullman. Shots taken, shots returned regarding the census' motivation for using differential privacy (and btw, it's not an algorithm). Blog post, 27 August 2021. URL https://statmodeling.stat.columbia.edu/2021/08/27/shots-taken-shots-returned-regarding-the-census-motivation-for-using-differential-privacy-and-btw-it

Prateek Jain, Pravesh Kothari, and Abhradeep Thakurta. Differentially private online learning. In Shie Mannor, Nathan Srebro, and Robert C. Williamson, editors, *Proceedings of the 25th Annual Conference on Learning Theory*, volume 23 of *Proceedings of Machine Learning Research*, pages 24.1–24.34, Edinburgh, Scotland, 25–27 Jun 2012. PMLR. URL http://proceedings.mlr.press/v23/jain12.html.

Ron S. Jarmin, John M. Abowd, Robert Ashmead, Ryan Cumings-Menon, Nathan Goldschlag, Michael B. Hawes, Sallie Ann Keller, Daniel Kifer, Philip Leclerc, Jerome P. Reiter, Rolando A. Rodríguez, Ian Schmutte, Victoria A. Velkoff, and Pavel Zhuravlev. An in-depth examination of requirements for disclosure risk assessment. *Proceedings of the National Academy of Sciences*, 120(43):e2220558120, 2023. doi: 10.1073/pnas.2220558120. URL https://www.pnas.org/doi/abs/10.1073/pnas.2220558120.

JASON. Consistency of data products and formal privacy methods for the 2020 census. Technical Report JSR-21-02, The Mitre Corporation, January 2022. URL https://www2.census.gov/programs-surveys/decennial/2020/program-management/planning-docs/2020-census-data-products-privacy-methods.pdf.

Jiankai Jin, Eleanor McMurtry, Benjamin I. P. Rubinstein, and Olga Ohrimenko. Are we there yet? timing and floating-point attacks on differential privacy systems. In *43rd IEEE Symposium on Security and Privacy, SP 2022, San Francisco, CA, USA, May 22-26, 2022*, pages 473–488. IEEE, 2022. doi: 10.1109/SP46214.2022.9833672. URL https://doi.org/10.1109/SP46214.2022.9833672.

Matthew Joseph, Aaron Roth, Jonathan Ullman, and Bo Waggoner. Local differential privacy for evolving data. In S. Bengio, H. Wallach, H. Larochelle, K. Grauman, N. Cesa-Bianchi, and R. Garnett, editors, *Advances in Neural Information Processing Systems 31*, pages 2375–2384. Curran Associates, Inc., 2018. URL http://papers.nips.cc/paper/7505-local-differential-privacy-for-evolving-data.pdf.

P. Kairouz, S. Oh, and P. Viswanath. The composition theorem for differential privacy. *IEEE Transactions on Information Theory*, 63(6):4037–4049, June 2017. ISSN 0018-9448. doi: 10.1109/TIT.2017.2685505.

Gautam Kamath and Jonathan Ullman. A primer on private statistics, 2020. URL https://arxiv.org/abs/2005.00010.

Farzaneh Karegar, Ala Sarah Alaqra, and Simone Fischer-Hübner. Exploring {User-Suitable} metaphors for differentially private data analyses. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*, pages 175–193, 2022.

Shiva P. Kasiviswanathan and Adam Smith. On the 'semantics' of differential privacy: A bayesian formulation. *Journal of Privacy and Confidentiality*, 6(1), 2014.

Shiva Prasad Kasiviswanathan, Homin K. Lee, Kobbi Nissim, Sofya Raskhodnikova, and Adam Smith. What can we learn privately? *SIAM J. Comput.*, 40(3):793–826, 2011. doi: 10.1137/090756090.

Shiva Prasad Kasiviswanathan, Kobbi Nissim, Sofya Raskhodnikova, and Adam Smith. Analyzing graphs with node differential privacy. In *TCC*, pages 457–476, 2013. doi: 10.1007/978-3-642-36594-2_26. URL http://dx.doi.org/10.1007/978-3-642-36594-2_26.

Michael J. Kearns and Umesh V. Vazirani. *An introduction to computational learning theory*. MIT Press, Cambridge, MA, 1994. ISBN 0-262-11193-4.

Christopher T Kenny, Shiro Kuriwaki, Cory McCartan, Evan TR Rosenman, Tyler Simko, and Kosuke Imai. The use of differential privacy for census data and its impact on redistricting: The case of the 2020 us census. *Science advances*, 7(41):eabk3283, 2021.

Helena Klause, Alexander Ziller, Daniel Rueckert, Kerstin Hammernik, and Georgios Kaissis. Differentially private training of residual networks with scale normalisation, 2022. URL https://arxiv.org/abs/2203.00324.

Aleksandra Korolova. Privacy violations using microtargeted ads: A case study. *Journal of Privacy and Confidentiality*, 3, 2011. URL https://doi.org/10.29012/jpc.v3i1.594.

Aleksandra Korolova, Krishnaram Kenthapadi, Nina Mishra, and Alexandros Ntoulas. Releasing search queries and clicks privately. In *Proceedings of the 18th International Conference on World Wide Web*, WWW '09, pages 171–180, New York, NY, USA, 2009. ACM. ISBN 978-1-60558-487-4. doi: 10.1145/1526709.1526733. URL http://doi.acm.org/10.1145/1526709.1526733.

Harry Lewis and Rachel Zax. *Essential Discrete Mathematics for Computer Science*. Princeton University Press, USA, 2019. ISBN 0691179298.

Terrance Liu, Jingwu Tang, Giuseppe Vietri, and Steven Wu. Generating private synthetic data with genetic algorithms. In Andreas Krause, Emma Brunskill, Kyunghyun Cho, Barbara Engelhardt, Sivan Sabato, and Jonathan Scarlett, editors, *Proceedings of the 40th International Conference on Machine Learning*, volume 202 of *Proceedings of Machine Learning Research*, pages 22009–22027. PMLR, 23–29 Jul 2023. URL https://proceedings.mlr.press/v202/liu23ag.html.

Xin Lyu. Composition theorems for interactive differential privacy. *Advances in Neural Information Processing Systems*, 35:9700–9712, 2022.

Ashwin Machanavajjhala, Daniel Kifer, John Abowd, Johannes Gehrke, and Lars Vilhuber. Privacy: Theory meets practice on the map. In *Proceedings of the 2008 IEEE 24th International Conference on Data Engineering*, ICDE '08, pages 277–286, Washington, DC, USA, 2008. IEEE Computer Society. ISBN 978-1-4244-1836-7. doi: 10.1109/ICDE.2008.4497436. URL https://doi.org/10.1109/ICDE.2008.4497436.

Ryan McKenna, Brett Mullins, Daniel Sheldon, and Gerome Miklau. AIM: an adaptive and iterative mechanism for differentially private synthetic data. *Proc. VLDB Endow.*, 15(11):2599–2612, July 2022. ISSN 2150-8097. doi: 10.14778/3551793.3551817. URL https://doi.org/10.14778/3551793.3551817.

Frank McSherry. Statistical inference considered harmful. Blog post, 14 June 2016. URL https://github.com/frankmcsherry/blog/blob/master/posts/2016-06-14.md.

Frank McSherry and Kunal Talwar. Mechanism design via differential privacy. In *Proceedings of the 48th Annual IEEE Symposium on Foundations of Computer Science*, FOCS '07, pages 94–103, Washington, DC, USA, 2007. IEEE Computer Society. doi: 10.1109/FOCS.2007.41.

D. J. Mir, S. Isaacman, R. Cáceres, M. Martonosi, and R. N. Wright. Dp-where: Differentially private modeling of human mobility. In *2013 IEEE International Conference on Big Data*, pages 580–588, Oct 2013. doi: 10.1109/BigData.2013.6691626.

Ilya Mironov. On significance of the least significant bits for differential privacy. In *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, CCS '12, pages 650–661, New York, NY, USA, 2012. ACM. ISBN 978-1-4503-1651-4. doi: 10.1145/2382196.2382264. URL http://doi.acm.org/10.1145/2382196.2382264.

Ilya Mironov. Rényi differential privacy. In *30th IEEE Computer Security Foundations Symposium, CSF 2017, Santa Barbara, CA, USA, August 21-25, 2017*, pages 263–275. IEEE Computer Society, 2017. ISBN 978-1-5386-3217-8. doi: 10.1109/CSF.2017.11. URL https://doi.org/10.1109/CSF.2017.11.

Michael Mitzenmacher and Eli Upfal. *Probability and Computing: Randomized Algorithms and Probabilistic Analysis*. Cambridge University Press, New York, NY, USA, 2nd edition, 2005. ISBN 0521835402. URL https://doi.org/10.1017/CBO9780511813603.

Mahnush Movahedi, Benjamin M. Case, James Honaker, Andrew Knox, Li Li, Yiming Paul Li, Sanjay Saravanan, Shubho Sengupta, and Erik Taubeneck. Privacy-preserving randomized controlled trials: A protocol for industry scale deployment. In *Proceedings of the 2021 on Cloud Computing Security Workshop*, CCSW '21, page 59–69, New York, NY, USA, 2021. Association for Computing Machinery. ISBN 9781450386531. doi: 10.1145/3474123.3486764. URL https://doi.org/10.1145/3474123.3486764.

Deirdre K. Mulligan, Colin Koopman, and Nick Doty. Privacy is an essentially contested concept: a multi-dimentional analytic for mapping privacy. *Philosophical Transactions of the Royal Society A*, 374 (20160118), 2017.

Jack Murtagh and Salil Vadhan. The complexity of computing the optimal composition of differential privacy. *Theory of Computing*, 14(8):1–35, 2018. doi: 10.4086/toc.2018.v014a008. URL http://www.theoryofcomputing.org/articles/v014a008.

Priyanka Nanayakkara, Johes Bater, Xi He, Jessica Hullman, and Jennie Rogers. Visualizing privacy-utility trade-offs in differentially private data releases. *PETS, year=2022*.

Priyanka Nanayakkara, Mary Anne Smart, Rachel Cummings, Gabriel Kaptchuk, and Elissa M Redmiles. What are the chances? explaining the epsilon parameter in differential privacy. In *32nd USENIX Security Symposium (USENIX Security 23)*, pages 1613–1630, 2023.

Priyanka Nanayakkara, Hyeok Kim, Yifan Wu, Ali Sarvghad, Narges Mahyar, Gerome Miklau, and Jessica Hullman. Measure-observe-remeasure: An interactive paradigm for differentially-private exploratory analysis. In *2024 IEEE Symposium on Security and Privacy (SP)*, pages 1047–1064. IEEE, 2024.

Arvind Narayanan and Vitaly Shmatikov. Robust de-anonymization of large sparse datasets. In *2008 IEEE Symposium on Security and Privacy (S&P 2008), 18-21 May 2008, Oakland, California, USA*, pages 111–125. IEEE Computer Society, 2008. ISBN 978-0-7695-3168-7. doi: 10.1109/SP.2008.33. URL http://dx.doi.org/10.1109/SP.2008.33.

Arvind Narayanan and Vitaly Shmatikov. Myths and fallacies of "personally identifiable information". *Communications of the ACM*, 53(6):24–26, June 2010. ISSN 0001-0782. doi: 10.1145/1743546.1743558. URL http://doi.acm.org/10.1145/1743546.1743558.

Milad Nasr, Jamie Hayes, Thomas Steinke, Borja Balle, Florian Tramèr, Matthew Jagielski, Nicholas Carlini, and Andreas Terzis. Tight auditing of differentially private machine learning. In Joseph A. Calandrino and Carmela Troncoso, editors, *32nd USENIX Security Symposium, USENIX Security 2023, Anaheim, CA, USA, August 9-11, 2023*, pages 1631–1648. USENIX Association, 2023. URL https://www.usenix.org/conference/usenixsecurity23/presentation/nasr.

Joseph P. Near and Chiké Abuah. *Programming Differential Privacy*. 2021. https://programming-dp.com/.

Joseph P. Near and Xi He. Differential privacy for databases. *Foundations and Trends® in Databases*, 11(2):109–225, 2021. ISSN 1931-7883. doi: 10.1561/1900000066. URL http://dx.doi.org/10.1561/1900000066.

Helen Nissenbaum. *Privacy In Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press, 2009.

Kobbi Nissim and Alexandra Wood. Is privacy *privacy? Philosophical Transactions of the Royal Society A*, 376(20170358), 2018.

Mayana Pereira, Shane Greenstein, Raffaella Sadun, Prasanna Tambe, Lucia Ronchi Darre, Tammy Glazer, Allen Kim, Rahul Dodhia, and Juan Lavista Ferres. The new digital divide. Working Paper 32932, National Bureau of Economic Research, September 2024. URL http://www.nber.org/papers/w32932.

Natalia Ponomareva, Hussein Hazimeh, Alex Kurakin, Zheng Xu, Carson Denison, H. Brendan McMahan, Sergei Vassilvitskii, Steve Chien, and Abhradeep Guha Thakurta. How to dp-fy ML: A practical guide to machine learning with differential privacy. *J. Artif. Intell. Res.*, 77:1113–1201, 2023. doi: 10.1613/JAIR.1.14649. URL https://doi.org/10.1613/jair.1.14649.

Sarah Radway and Miranda Christ. The impact of de-identification on single-year-of-age counts in the us census. *arXiv preprint arXiv:2308.12876*, 2023.

Sofya Raskhodnikova and Adam Smith. Private analysis of graph data. In Ming-Yang Kao, editor, *Encyclopedia of Algorithms*, pages 1–6. Springer Berlin Heidelberg, Berlin, Heidelberg, 2014. ISBN 978-3-642-27848-8. doi: 10.1007/978-3-642-27848-8_549-1. URL http://dx.doi.org/10.1007/978-3-642-27848-8_549-1.

Zachary Ratliff and Salil Vadhan. A framework for differential privacy against timing attacks. In *Proceedings of the 31st ACM SIGSAC Conference on Computer and Communications Security (CCS '24)*. ACM, 2024. Received a CCS '24 Distinguished Artifact Award. Preliminary version presented as a poster at TPDP '24 and posted as arXiv:2409.05623 [cs.CR].

Ryan Rogers, Aaron Roth, Jonathan Ullman, and Salil Vadhan. Privacy odometers and filters: Pay-as-you-go composition. In *Proceedings of the 30th International Conference on Neural Information Processing Systems*, NIPS'16, pages 1929–1937, USA, 2016. Curran Associates Inc. ISBN 978-1-5108-3881-9. URL http://dl.acm.org/citation.cfm?id=3157096.3157312.

Kenneth Rosen. *Discrete Mathematics and its Applications*. McGraw Hill Education, 7th edition, 2012. URL https://www.mheducation.com/highered/product/discrete-mathematics-applications-rosen/M9780073383095.html.

Sheldon M. Ross. *A First Course in Probability*. Fifth edition, 1998.

Tim Roughgarden. *Algorithms Illuminated: Omnibus Edition*. CUP, 2022.

Steven Ruggles and David van Riper. The role of chance in the census bureau database reconstruction experiment. *Population Research and Policy Review*, 41:781–788, 2022.

Jayshree Sarathy. From algorithmic to institutional logics: The politics of differential privacy, 2022.

Reza Shokri, Marco Stronati, Congzheng Song, and Vitaly Shmatikov. Membership inference attacks against machine learning models. In *2017 IEEE Symposium on Security and Privacy, SP 2017, San Jose, CA, USA, May 22-26, 2017*, pages 3–18. IEEE Computer Society, 2017. ISBN 978-1-5090-5533-3. doi: 10.1109/SP.2017.41. URL https://doi.org/10.1109/SP.2017.41.

Ryan Singel. Netflix cancels recommendation contest after privacy lawsuit. *Wired*, 12 March 2010. URL https://www.wired.com/2010/03/netflix-cancels-contest/.

Mary Anne Smart, Dhruv Sood, and Kristen Vaccaro. Understanding risks of privacy theater with differential privacy. *Proceedings of the ACM on Human-Computer Interaction*, 6(CSCW2):1–24, 2022.

Mary Anne Smart, Priyanka Nanayakkara, Rachel Cummings, Gabriel Kaptchuk, and Elissa Redmiles. Models matter: Setting accurate privacy expectations for local and central differential privacy. *arXiv preprint arXiv:2408.08475*, 2024.

A. Smith, A. Thakurta, and J. Upadhyay. Is interaction necessary for distributed private learning? In *2017 IEEE Symposium on Security and Privacy (SP)*, pages 58–77, May 2017. doi: 10.1109/SP.2017.35.

Adam Smith and Jonathan Ullman. Privacy in statistics and machine learning. https://dpcourse.github.io/, 2025.

Daniel J. Solove. A taxonomy of privacy. *University of Pennsylvania Law Review*, (154):477, 2006.

Daniel Solow. *How to Read and Do Proofs: An Introduction to Mathematical Thought Processes*. Wiley, 6th edition, 2013. URL https://www.wiley.com/en-us/How+to+Read+and+Do+Proofs%3A+An+Introduction+to+Mathematical+Thought+Processes%2C+6th+Edition-p-9781118164020.

S. Song, K. Chaudhuri, and A. D. Sarwate. Stochastic gradient descent with differentially private updates. In *2013 IEEE Global Conference on Signal and Information Processing*, pages 245–248, Dec 2013. doi: 10.1109/GlobalSIP.2013.6736861.

Mark F. St. John, Grit Denker, Peeter Laud, Karsten Martiny, and Alisa Pankova. Decision Support for Sharing Data Using Differential Privacy. *IEEE Transactions on Visualization and Computer Graphics*, pages 26–35, 2021.

Ryan Steed, Terrance Liu, Zhiwei Steven Wu, and Alessandro Acquisti. Policy impacts of statistical uncertainty and privacy. *Science*, 377(6609):928–931, 2022.

Latanya Sweeney. Weaving technology and policy together to maintain confidentiality. *The Journal of Law, Medicine & Ethics*, 25(2-3):98–110, 1997. doi: 10.1111/j.1748-720X.1997.tb01885.x. URL https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1748-720X.1997.tb01885.x.

Latanya Sweeney. Simple demographics often identify people uniquely. Technical report, Technical report, Carnegie Mellon University, 2000. URL https://dataprivacylab.org/projects/identifiability/.

Latanya Sweeney. K-anonymity: A model for protecting privacy. *Int. J. Uncertain. Fuzziness Knowl.-Based Syst.*, 10(5):557–570, October 2002. ISSN 0218-4885. doi: 10.1142/S0218488502001648. URL http://dx.doi.org/10.1142/S0218488502001648.

Latanya Sweeney, Akua Abu, and Julia Winn. Identifying participants in the personal genome project by name. Whitepaper 1021-1, Harvard University Data Privacy Lab, 13 April 2013. URL https://dataprivacylab.org/projects/pgp/.

Jun Tang, Aleksandra Korolova, Xiaolong Bai, Xueqiang Wang, and XiaoFeng Wang. Privacy loss in apple's implementation of differential privacy on macos 10.12. *CoRR*, abs/1709.02753, 2017. URL http://arxiv.org/abs/1709.02753.

Adam Tanner. Harvard professor re-identifies anonymous volunteers in DNA study. *Forbes*, 25 April 2013. URL https://www.forbes.com/sites/adamtanner/2013/04/25/harvard-professor-re-identifies-anonymous-volunteers-in-dna-study/#7bfba06192c9.

Pratiksha Thaker, Mihai Budiu, Parikshit Gopalan, Udi Wieder, and Matei Zaharia. Overlook: Differentially Private Exploratory Visualization for Big Data. *arXiv preprint arXiv:2006.12018*, 2020.

Salil Vadhan and Wanrong Zhang. Concurrent composition theorems for differential privacy. In *Proceedings of the 55th Annual ACM Symposium on Theory of Computing (STOC '23)*, pages 507–519, 20–23 June 2023. doi: 10.1145/3564246.3585241. URL https://doi.org/10.1145/3564246.3585241. Preliminary versions posted as arXiv:2207.08335 [cs.DS] and presented as a poster at TPDP '22.

Salil P. Vadhan. The complexity of differential privacy. In Yehuda Lindell, editor, *Tutorials on the Foundations of Cryptography — Dedicated to Oded Goldreich*, pages 347–450. Springer, 2017. ISBN 978-3-319-57047-1. doi: 10.1007/978-3-319-57048-8_7. URL https://doi.org/10.1007/978-3-319-57048-8_7.

Giuseppe Vietri, Cedric Archambeau, Sergul Aydore, William Brown, Michael Kearns, Aaron Roth, Ankit Siva, Shuai Tang, and Zhiwei Steven Wu. Private synthetic data for multitask learning and marginal queries. In *Proceedings of the 36th International Conference on Neural Information Processing Systems*, NIPS '22, Red Hook, NY, USA, 2022. Curran Associates Inc. ISBN 9781713871088.

Oliver Williams and Frank Mcsherry. Probabilistic inference and differential privacy. In J. D. Lafferty, C. K. I. Williams, J. Shawe-Taylor, R. S. Zemel, and A. Culotta, editors, *Advances in Neural Information Processing Systems 23*, pages 2451–2459. Curran Associates, Inc., 2010. URL http://papers.nips.cc/paper/3897-probabilistic-inference-and-differential-privacy.pdf.

Langdon Winner. Do artifacts have politics? *Daedalus*, 109(1):121–136, 1980.

Alexandra Wood, Micah Altman, Aaron Bembenek, Mark Bun, Marco Gaboardi, James Honaker, Kobbi Nissim, David R O'Brien, Thomas Steinke, and Salil Vadhan. Differential privacy: A primer for a non-technical audience. *Vand. J. Ent. & Tech. L.*, 21:209, 2018a.

Alexandra Wood, Micah Altman, Aaron Bembenek, Mark Bun, Marco Gaboardi, James Honaker, Kobbi Nissim, David R. O'Brien, Thomas Steinke, and Salil Vadhan. Differential privacy: A primer for a non-technical audience. *Vanderbilt Journal of Entertainment & Technology Law*, 21(1):209–275, 2018b. URL http://www.jetlaw.org/journal-archives/volume-21/volume-21-issue-1/differential-privacy-a-primer-for-a-non-technical-audience/. Preliminary version workshopped at PLSC 2017.

Alexandra Wood, Micah Altman, Kobbi Nissim, and Salil Vadhan. Designing access with differential privacy. In Shawn Cole, Iqbal Dhaliwal, Anja Sautmann, and Lars Vilhuber, editors, *Using Administrative Data for Research and Evidence-based Policy — A Handbook*, chapter 6, pages 173–242. Abdul Latif Jameel Poverty Action Lab (J-PAL), Cambridge, MA, 2020. ISBN 978-1736021606. URL https://admindatahandbook.mit.edu/book/v1.0/diffpriv.html.

Aiping Xiong, Tianhao Wang, Ninghui Li, and Somesh Jha. Towards effective differential privacy communication for users' data sharing decision and comprehension. In *2020 IEEE Symposium on Security and Privacy (SP)*, pages 392–410. IEEE, 2020.

Aiping Xiong, Chuhao Wu, Tianhao Wang, Robert W Proctor, Jeremiah Blocki, Ninghui Li, and Somesh Jha. Exploring use of explanative illustrations to communicate differential privacy models. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, volume 67, pages 226–232. SAGE Publications Sage CA: Los Angeles, CA, 2023.

Sajjad Zarifzadeh, Philippe Liu, and Reza Shokri. Low-cost high-power membership inference attacks. In *Forty-first International Conference on Machine Learning, ICML 2024, Vienna, Austria, July 21-27, 2024*. OpenReview.net, 2024. URL https://openreview.net/forum?id=sT7UJh5CTc.

Chiyuan Zhang, Samy Bengio, Moritz Hardt, Benjamin Recht, and Oriol Vinyals. Understanding deep learning requires rethinking generalization. In *5th International Conference on Learning Representations, ICLR 2017, Toulon, France, April 24-26, 2017, Conference Track Proceedings*. OpenReview.net, 2017. URL https://openreview.net/forum?id=Sy8gdB9xx.

Danfeng Zhang and Daniel Kifer. Lightdp: Towards automating differential privacy proofs. *SIGPLAN Notices*, 52(1):888–901, January 2017. ISSN 0362-1340. doi: 10.1145/3093333.3009884. URL http://doi.acm.org/10.1145/3093333.3009884.

Amitai Ziv. Israel's 'anonymous' statistics surveys aren't so anonymous. *Haaretz*, 7 January 2013. URL https://www.haaretz.com/surveys-not-as-anonymous-as-respondents-think-1.5288950.