

GEROME MIKLAU

Curriculum Vitae

College of Information and Computer Sciences
University of Massachusetts
140 Governors Drive, Amherst, MA 01003
Ph. (413) 545-4032 Fax (413) 545-1249
miklau@cs.umass.edu
people.cs.umass.edu/miklau

Education

University of Washington, Seattle, WA
Ph.D., Computer Science, August 2005
Thesis: Integrity and Confidentiality in Distributed Data Exchange
M.S., Computer Science, December 2001

University of California, Berkeley
B.S. Mathematics, B.A. Rhetoric with Honors. December 1995

Professional Positions

9/2005 - present	University of Massachusetts <i>College of Information and Computer Sciences</i> Professor (2017 - present) Associate Professor (2011 - 2017) Assistant Professor (2005 - 2011)	Amherst, Massachusetts
7/2019 - present	Tumult Labs, Inc. Co-founder	Durham, NC
2/2017 - 6/2019	U.S. Census Bureau Research Data Scientist, Research and Methodology Directorate	Suitland, MD
9/2012 - 6/2013	INRIA Visiting Professor (during sabbatical).	Saclay, France
9/1999 - 8/2005	University of Washington Teaching Assistant / Research Assistant	Seattle, Washington
6/2003 - 9/2003	IBM, Almaden Research Center Research Intern, <i>Intelligent Information Systems Group</i>	San Jose, California
6/2002 - 8/2002	Lucent, Bell Laboratories Research Intern, <i>Internet Management Research Group</i>	Murray Hill, New Jersey
5/1996 - 8/1998	J. P. Morgan and Company Associate, <i>Fixed income derivatives trading</i>	New York, New York

Awards and Honors

ACM PODS Alberto O. Mendelzon Test-of-Time Award 2020 (Ten-Year Best Paper Award)
Fellow, Interdisciplinary Studies Institute, UMass Amherst (2015–2016)
Best Paper Award, International Conference on Database Theory (ICDT) 2013.
ACM PODS Alberto O. Mendelzon Test-of-Time Award 2012 (Ten-Year Best Paper Award)
Lilly Teaching Fellowship, 2011–2012
Best Student Paper Award, IEEE International Conference on Data Mining, 2009.
NSF CAREER Award, 2007.
ACM SIGMOD Dissertation Award, 2006.

Publications

Refereed Journal Publications

- [1] Ryan McKenna, Brett Mullins, Daniel Sheldon, and Gerome Miklau. Aim: An adaptive and iterative mechanism for differentially private synthetic data. In *To appear, Proceedings of the VLDB Conference (PVLDB)*, 2022.
- [2] Ryan McKenna, Gerome Miklau, and Dan Sheldon. Winning the nist contest: A scalable and general approach to differentially private synthetic data. In *Journal of Privacy and Confidentiality (JPC)*, 2021.
- [3] Ryan McKenna, Raj Kumar Maity, Arya Mazumdar, and Gerome Miklau. A workload-adaptive mechanism for linear queries under local differential privacy. In *Proceedings of the VLDB (PVLDB)*, 2020.
- [4] Ios Kotsogiannis, Yuchao Tao, Xi He, Maryam Fanaeepour, Ashwin Machanavajjhala, Michael Hay, and Gerome Miklau. Privatesql: A differentially private sql query engine. In *Proceedings of the VLDB (PVLDB)*, 2019.
- [5] Abolfazl Asudeh, H. V. Jagadish, Gerome Miklau, and Julia Stoyanovich. On obtaining stable rankings. In *Proceedings of the VLDB (PVLDB)*, 2019.
- [6] Ryan McKenna, Gerome Miklau, Michael Hay, and Ashwin Machanavajjhala. Optimizing error of high-dimensional statistical queries under differential privacy. In *Proceedings of the VLDB (PVLDB)*, 2018.
- [7] Yue Wang, Alexandra Meliou, and Gerome Miklau. RC-Index: Diversifying answers to range queries. *Proceedings of the VLDB (PVLDB)*, 2018.
- [8] Chao Li, Daniel Yang Li, Gerome Miklau, and Dan Suciu. A theory of pricing private data. *Communications of the ACM (Research Highlight)*, 2017.
- [9] Chao Li, Gerome Miklau, Michael Hay, Andrew McGregor, and Vibhor Rastogi. The matrix mechanism: optimizing linear counting queries under differential privacy. *VLDB Journal*, 2015.
- [10] Chao Li and Gerome Miklau. Lower bounds on the error of query sets under the differentially-private matrix mechanism. *Transactions on Computer Systems*, 2015.
- [11] Chao Li, Daniel Yang Li, Gerome Miklau, and Dan Suciu. A theory of pricing private data. In *Transactions on Database Systems (TODS)*, 2015.
- [12] Wentian Lu, Gerome Miklau, and Neil Immerman. Auditing a database under retention policies. *VLDB Journal*, 22(2):203–228, 2013.

- [13] Michael Hay, Gerome Miklau, David Jensen, Don Towsley, and Chao Li. Resisting structural re-identification in anonymized social networks. *VLDB Journal*, 2010.
- [14] Gerome Miklau and Dan Suciu. A formal analysis of information disclosure in data exchange. *Journal of Computer and System Sciences (JCSS)*, 73(3):507–534, 2007.
- [15] Gerome Miklau and Dan Suciu. Containment and equivalence for a fragment of XPath. *Journal of the ACM (JACM)*, 51(1):2–45, 2004.
- [16] Todd J. Green, Ashish Gupta, Gerome Miklau, Makoto Onizuka, and Dan Suciu. Processing XML streams with deterministic automata and stream indexes. *ACM Transactions on Database Systems (TODS)*, 29, 2004.

Other Journal Publications

- [1] Dan Zhang, Ryan McKenna, Ios Kotsogiannis, George Bissias, Michael Hay, Ashwin Machanavajjhala, and Gerome Miklau. Ektelo: A framework for defining differentially-private computations. *SIGMOD Record*, 2019.
- [2] Gerome Miklau and Dan Suciu. Enabling secure data exchange. *IEEE Data Engineering Bulletin, Special Issue on Security and Privacy*, 27(1):34–41, 2004.
- [3] Igor Tatarinov, Zachary Ives, Jayant Madhavan, Alon Halevy, Dan Suciu, Nilesh Dalvi, Xin (Luna) Dong, Yana Kadiyska, Gerome Miklau, and Peter Mork. The Piazza peer data management project. *SIGMOD Record*, 32(3):47–52, 2003.

Refereed Conference Publications

- [1] Ryan McKenna, Siddhant Pradhan, Dan Sheldon, and Gerome Miklau. Relaxed marginal consistency for differentially private query answering. In *Conference on Neural Information Processing Systems (NeurIPS)*, 2021.
- [2] Dan Zhang, Ali Sarvghad, and Gerome Miklau. Investigating visual analysis of differentially private data. In *IEEE Conference on Information Visualization (InfoVis)*, 2020.
- [3] David Pujol, Satya Kuppam, Ryan Mckenna, Michael Hay, Ashwin Machanavajjhala, and Gerome Miklau. Fair decision making using privacy-protected data. In *ACM Conference on Fairness, Accountability, and Transparency*, 2020.
- [4] Zhiqi Huang, Ryan McKenna, George Bissias, Gerome Miklau, Michael Hay, and Ashwin Machanavajjhala. PsynDb: Accurate and accessible private data generation. In *Demo, Proceedings of the VLDB (PVLDB)*, 2019.
- [5] Ryan McKenna, Dan Sheldon, and Gerome Miklau. Graphical-model based estimation and inference for differential privacy. *International Conference on Machine Learning (ICML)*, 2019.
- [6] Ios Kotsogiannis, Yuchao Tao, Ashwin Machanavajjhala, Gerome Miklau, and Michael Hay. Architecting a differentially private sql engine. In *Conference on Innovative Data Systems Research (CIDR)*, 2019.
- [7] Yifan Guan, Abolfazl Asudeh, Pranav Mayuram, H. V. Jagadish, Julia Stoyanovich, Gerome Miklau, and Gautam Das. Mithraranking: A system for responsible ranking design. In *Demo Program, Conference on Management of Data (SIGMOD)*, 2019.
- [8] Dan Zhang, Ryan McKenna, Ios Kotsogiannis, Michael Hay, Ashwin Machanavajjhala, and Gerome Miklau. Ektelo: A framework for defining differentially-private computations. In *Conference on Management of Data (SIGMOD)*, 2018.
- [9] Sameera Ghayyur, Yan Chen, Roberto Yus, Ashwin Machanavajjhala, Michael Hay, Gerome Miklau, and Sharad Mehrotra. Iot-detective: Analyzing iot data under differential privacy. In *Demo Program, Conference on Management of Data (SIGMOD)*, 2018.

- [10] Ke Yang, Julia Stoyanovich, Abolfazl Asudeh, Bill Howe, HV Jagadish, and Gerome Miklau. A nutritional label for rankings. In *Demo Program, Conference on Management of Data (SIGMOD)*, 2018.
- [11] Yan Chen, Ashwin Machanavajjhala, Michael Hay, and Gerome Miklau. Pegasus: Data-adaptive differentially private stream processing. In *Conference on Computer and Communications Security (CCS)*, 2017.
- [12] Garrett Bernstein, Ryan McKenna, Tao Sun, Daniel Sheldon, Michael Hay, and Gerome Miklau. Differentially private learning of undirected graphical models using collective graphical models. In *International Conference on Machine Learning (ICML)*, 2017.
- [13] Michael Hay, Liudmila Elagina, and Gerome Miklau. Differentially private rank aggregation. In *SIAM Conference on Data Management (SDM)*, 2017.
- [14] Ios Kotsogiannis, Ashwin Machanavajjhala, Michael Hay, Gerome Miklau, and Margaret Orr. Dias: Differentially private interactive algorithm selection using pythia. In *Demo Program, Conference on Management of Data (SIGMOD)*, 2017.
- [15] Bill Howe, Julia Stoyanovich, Serge Abiteboul, Gerome Miklau, Arnaud Sahuguet, and Gerhard Weikum. Fides: Towards a platform for responsible data science. In *Conference on Scientific and Statistical Database Management (SSDBM)*, 2017.
- [16] Ios Kotsogiannis, Ashwin Machanavajjhala, Michael Hay, and Gerome Miklau. Pythia: Data dependent differentially private algorithm selection. In *Conference on Management of Data (SIGMOD)*, 2017.
- [17] Yue Wang, Alexandra Meliou, and Gerome Miklau. Lifting the haze off the cloud: A consumer-centric market for database computation in the cloud. In *To appear, Proceedings of the VLDB Conference (PVLDB)*, 2017.
- [18] Michael Hay, Ashwin Machanavajjhala, Gerome Miklau, Yan Chen, and Dan Zhang. Principled evaluation of differentially private algorithms using DPBench. In *Conference on Management of Data (SIGMOD)*, 2016.
- [19] Michael Hay, Ashwin Machanavajjhala, Gerome Miklau, Yan Chen, Dan Zhang, and George Bissias. Exploring privacy-accuracy tradeoffs using DPComp. In *ACM Conference on Management of Data (SIGMOD) Demo Program*, 2016.
- [20] Vera Zaychik Moffitt, Julia Stoyanovich, Serge Abiteboul, and Gerome Miklau. Collaborative access control in webdamlog. In *Conference on Management of Data (SIGMOD)*, 2015.
- [21] Wentian Lu, Gerome Miklau, and Vani Gupta. Generating private synthetic databases for untrusted system evaluation. In *International Conference on Data Engineering (ICDE)*, 2014.
- [22] Wentian Lu and Gerome Miklau. Exponential random graph estimation under differential privacy. In *Conference on Knowledge Discovery and Data Mining (KDD)*, 2014.
- [23] Chao Li, Michael Hay, and Gerome Miklau. A data- and workload-aware algorithm for range queries under differential privacy. *Proceedings of the VLDB (PVLDB)*, 2014.
- [24] Serge Abiteboul, Emilien Antoine, Gerome Miklau, Julia Stoyanovich, and Jules Testard. Rule-based application development using webdamlog. In *SIGMOD Conference (Demo Program)*, pages 965–968, 2013.
- [25] Chao Li, Daniel Yang Li, Gerome Miklau, and Dan Suciu. A theory of pricing private data. In *International Conference on Database Theory (ICDT)*, 2013
Winner, Best Paper Award.
- [26] Chao Li and Gerome Miklau. Optimal error of query sets under the differentially-private matrix mechanism. In *International Conference on Database Theory (ICDT)*, 2013.

- [27] Chao Li and Gerome Miklau. An adaptive mechanism for accurate query answering under differential privacy. *Proceedings of the VLDB Endowment (PVLDB)*, 5(6):514–525, 2012.
- [28] Michael Wick, Andrew McCallum, and Gerome Miklau. Scalable probabilistic databases with factor graphs and MCMC. In *Proceedings of the VLDB Endowment (PVLDB)*, 2010.
- [29] Michael Hay, Vibhor Rastogi, Gerome Miklau, and Dan Suciu. Boosting the accuracy of differentially-private queries through consistency. In *Proceedings of the VLDB Endowment (PVLDB)*, 2010.
- [30] Chao Li, Michael Hay, Vibhor Rastogi, Gerome Miklau, and Andrew McGregor. Optimizing linear counting queries under differential privacy. In *Principles of Database Systems (PODS)*, pages 123–134, 2010
Winner, Test-of-Time Award 2020.
- [31] Daniel Gyllstrom, Sudarshan Vasudevan, Jim Kurose, and Gerome Miklau. Efficient recovery from false state in distributed routing algorithms. In *NETWORKING 2010, 9th International IFIP TC 6 Networking Conference*, pages 198–212, 2010.
- [32] Michael Hay, Chao Li, Gerome Miklau, and David Jensen. Accurate estimation of the degree distribution of private networks. In *International Conference on Data Mining (ICDM)*, 2009
Winner, Best Student Paper Award.
- [33] Abhinav Parate and Gerome Miklau. A framework for safely publishing communication traces. In *Conference on Information and Knowledge Management (CIKM)*, 2009.
- [34] Vibhor Rastogi, Michael Hay, Gerome Miklau, and Dan Suciu. Relationship privacy: output perturbation for queries with joins. In *Symposium on Principles of Database Systems (PODS)*, pages 107–116, 2009.
- [35] Wentian Lu and Gerome Miklau. Auditing a database under retention restrictions. In *International Conference on Data Engineering (ICDE)*, pages 42–53, 2009.
- [36] Michael Hay, Gerome Miklau, David Jensen, Don Towsley, and Philipp Weis. Resisting structural identification in anonymized social networks. In *Proceedings of the VLDB Endowment (VLDB)*, pages 102–114, 2008.
- [37] Hala Mostafa, Victor Lesser, and Gerome Miklau. Self-interested database managers playing the view maintenance game. In *Conference on Autonomous Agents and Multiagent Systems (AAMAS)*, pages 871–878, May 2008.
- [38] Wentian Lu and Gerome Miklau. Auditguard: A system for database auditing under retention restrictions. In *Proceedings of the VLDB Endowment (Demonstration Paper)*, pages 1484–1487, 2008.
- [39] Bruno Ribeiro, Weifeng Chen, Gerome Miklau, and Don Towsley. Analyzing privacy in enterprise trace anonymization. In *Network and Distributed System Security Symposium (NDSS)*, pages 1–14, 2008.
- [40] Gerome Miklau, Brian Neil Levine, and Patrick Stahlberg. Securing history: Privacy and accountability in database systems. In *Conference on Innovative Data Systems Research (CIDR)*, pages 387–396, 2007.
- [41] Patrick Stahlberg, Gerome Miklau, and Brian Neil Levine. Threats to privacy in the forensic analysis of database systems. In *ACM Conference on Management of Data (SIGMOD)*, pages 91–102, 2007.
- [42] Gerome Miklau and Dan Suciu. Implementing a tamper-evident database system. In *Asian Computing Science Conference, Data Management on the Web (ASIAN)*, pages 28–48, Nov 2005.

- [43] Nilesh Dalvi, Gerome Miklau, and Dan Suciu. Asymptotic conditional probabilities for conjunctive queries. In *Proceedings of the International Conference on Database Theory (ICDT)*, pages 289–305, 2005.
- [44] Gerome Miklau and Dan Suciu. A formal analysis of information disclosure in data exchange. In *ACM Conference on Management of Data (SIGMOD)*, pages 575–586, 2004.
- [45] Gerome Miklau and Dan Suciu. Controlling access to published data using cryptography. In *Proceedings of the VLDB Conference*, 2003.
- [46] Todd J. Green, Gerome Miklau, Makoto Onizuka, and Dan Suciu. Processing XML streams with deterministic automata. In *Proceedings of the 9th International Conference on Database Theory*, pages 173–189, 2003.
- [47] Gerome Miklau and Dan Suciu. Containment and equivalence for an XPath fragment. In *Symposium on Principles of Database Systems (PODS)*, pages 65–76, 2002
Winner, Test-of-Time Award 2012.

Book Chapters

- [1] Michael Hay, Gerome Miklau, and David Jensen. Analyzing private network data. In *Privacy-Aware Knowledge Discovery: Novel Applications and New Techniques*. CRC Press, 2010.
- [2] Brian Neil Levine and Gerome Miklau. Auditing and Forensic Analysis. In M. Tamer A-Zsu and Ling Liu, editors, *Encyclopedia of Database Systems*. Springer-Verlag, June 2009.

Refereed Workshop Publications

- [1] Yuchao Tao, Ryan McKenna, Michael Hay, Ashwin Machanavajjhala, and Gerome Miklau. Benchmarking differentially private synthetic data generation algorithms. In *Workshop on Privacy-Preserving Artificial Intelligence (PPAI)*, 2022.
- [2] Sam Haney, William Sexton, Ashwin Machanavajjhala, Michael Hay, and Gerome Miklau. Differentially private algorithms for 2020 census detailed dhc race and ethnicity. In *Workshop on Theory and Practice of Differential Privacy (TPDP)*, 2021.
- [3] Ryan Mckenna and Gerome Miklau. Lessons learned from the NIST differential privacy synthetic data competition. In *Workshop on Theory and Practice of Differential Privacy (TPDP)*, 2019.
- [4] Dan Zhang, Michael Hay, Gerome Miklau, and Brendan O’Connor. Challenges of visualizing differentially private data. In *Workshop on the Theory and Practice of Differential Privacy (TPDP)*, 2016.
- [5] Chao Li and Gerome Miklau. Pricing aggregate queries in a data marketplace. In *Workshop on the Web and Databases (WebDB)*, 2012.
- [6] Vani Gupta, Gerome Miklau, and Neoklis Polyzotis. Private database synthesis for outsourced system evaluation. In *Alberto Mendelson Workshop*, 2011.
- [7] Greg Druck, Gerome Miklau, and Andrew McCallum. *Learning to Predict the Quality of Contributions to Wikipedia*. AAAI Workshop on Wikipedia and Artificial Intelligence, 2008.
- [8] David Mimno, Andrew McCallum, and Gerome Miklau. Probabilistic representations for integrating unreliable data sources. In *Workshop on Information Integration on the Web (IIWeb)*, 2007.
- [9] Gerome Miklau and Dan Suciu. Managing integrity for data exchanged on the web. In *Workshop on the Web and Databases (WebDB)*, pages 13–18, 2005.

- [10] Gerome Miklau and Dan Suciu. Modeling integrity in data exchange. In *Secure Data Management Workshop*, pages 41–54, 2004.
- [11] Gerome Miklau and Dan Suciu. Cryptographically enforced conditional access for XML. Workshop on the Web and Databases (WebDB), June 2002.

Other Unrefereed Publications

- [1] Wentian Lu and Gerome Miklau. Log sanitization: Auditing a database under retention restrictions. Technical Report 22, University of Massachusetts Amherst, June 2008.
- [2] Abhinav Parate and Gerome Miklau. A framework for utility-driven network trace anonymization. Technical Report 2008-038, University of Massachusetts Amherst, 2008.
- [3] Michael Hay, Gerome Miklau, David Jensen, Philipp Weis, and Siddharth Srivastava. Anonymizing social networks. Technical Report 07-19, University of Massachusetts Amherst, 2007.
- [4] Gerome Miklau. *Confidentiality and Integrity in Distributed Data Exchange*. PhD thesis, University of Washington, 2005
Winner, SIGMOD Dissertation Award.

Tutorials

Differential Privacy Bootcamp for US Government Personnel

Ashwin Machanavajjhala, Michael Hay, Daniel Kifer.
National Academy of Sciences. June 2019.

Data, responsibly: fairness, neutrality and transparency in data analysis.

J. Stoyanovich, S. Abiteboul, and G. Miklau.
International Conference on Extending Database Technology (EDBT), 2016.

Differentially Private Batch Query Answering: Exploiting the Workload vs. Exploiting the Data
Invited Tutorial.

Rutgers University, DIMACS Workshop on Recent Work on Differential Privacy across Computer Science.
October 2012.

Differential privacy in data publication and analysis.

Y. Yang, Z. Zhang, G. Miklau, M. Winslett, and X. Xiao.
ACM SIGMOD Conference on Management of Data (SIGMOD), July 2012.

Privacy-aware Data Mining in Information Networks.

with Michael Hay, Kun Liu, Jian Pei, Evimaria Terzi
ACM SIGMOD Conference on Management of Data (SIGMOD), 2011.

Privacy-aware Data Mining in Information Networks.

with Kun Liu, Jian Pei, Evimaria Terzi
ACM Conference on Knowledge Discovery and Data Mining (KDD), 2010.

Funding

Miklau (PI), with Narges Mahyar (co-PI) and Ali Sarvghad (co-PI).

Principles and Algorithms for Visual Data Exploration Under Differential Privacy

NSF Secure and Trustworthy Computing, Nov 2021 – Nov 2024. \$1,191,000

Miklau (PI), Sheldon (co-PI).

Tunable Differentially Private Synthetic Data.

Oracle Corporation, Sep 2020 – Sep 2022. \$150,000.

Miklau (PI), with Ashwin Machanavajjhala (co-PI, Duke), Michael Hay (co-PI, Colgate).

System P: A Data Analytics Engine With Customizable Privacy and Optimized Utility

DARPA Brandeis Program, Oct 2015 – Apr 2020. \$2,746,504

(\$1.2 million for expenditures at UMass)

Miklau (PI), with Ashwin Machanavajjhala (co-PI, Duke), Michael Hay (co-PI, Colgate).

Re[DP]: Realistic Data Mining Under Differential Privacy

NSF Secure and Trustworthy Computing, Aug 2014 – Jul 2018. \$418,356.

Miklau (co-PI), with James Kurose (PI).

Protecting Privacy while Providing Utility in Published Network Mobility

NSF Networking Technology and Systems, Oct 2014 – Sep 2017. \$499,765

Miklau (PI)

Automated Assessment of Disclosure Risk (STTR)

Contract with Aptima Inc. for Air Force Research Lab, Oct 2013 – Jun 2014. \$49,997.

Miklau (co-PI), with Yanlei Diao, Evimaria Terzi (co-PI, Boston University).

A Platform for Data-Intensive Cybersecurity Monitoring.

Advanced Cyber Security Center, Aug, 2012 – Aug, 2013. \$50,000.

Miklau (co-PI), with Johannes Gehrke (PI, Cornell), John Abowd (co-PI, Cornell), and Jerry Reiter (co-PI, Duke).

Practical Privacy: Metrics and Methods for Protecting Record-level and Relational Data.

NSF Trustworthy Computing, Jul 15, 2010 – Jul 15, 2015. \$569,855. (CNS 1012748).

Miklau (PI), with David Jensen (co-PI), Donald Towsley (co-PI).

Dissemination and Analysis of Private Network Data.

NSF Trustworthy Computing, May 1, 2010 – May 1, 2013. \$875,359. (IIS 0964094).

Miklau (co-PI), with Brian Levine (PI), Mark Corner (co-PI), Kevin Fu (co-PI), David Jensen (co-PI).

A Student Research Education Program in Information Command and Analysis.

National Security Agency / Department of Defense. Sep 1, 2009 – Sep 1, 2010. \$100,015.

Miklau (co-PI), with Jeff Reed (PI, Virginia Tech), Wade Trappe (PI, Rutgers), and Arun Venkataramani (PI)

AUSTIN– An Initiative to Assure Software Radios have Trusted Interactions.

NSF Trustworthy Computing. Sep 1, 2009 – Sep 1, 2011, \$190,000.

Miklau (co-PI), with Brian Levine (PI), Ping Li (co-PI, John Jay College of Criminal Justice), Janis Wolak (co-PI, University of New Hampshire)

A Northeast Partnership for Developing the Information Assurance Workforce.

NSF Federal Cyber Service. Sep 15, 2008 – Sep, 15 2010, \$287,502.

Miklau (PI). *Securing history: privacy and accountability in database systems.*

NSF CAREER Program, Jan 1, 2007 – Jan 1, 2012. \$499,000.

Research Experience for Undergraduates (REU), Supplement to CAREER Award, \$12,000

Miklau (co-PI), with Donald Towsley (co-PI), Johannes Gehrke (PI, Cornell), John Abowd (co-PI, Cornell), Dan Suciu (co-PI, University of Washington)

Preserving Utility while Ensuring Privacy for Linked Data.
NSF Cybertrust. Sep 15, 2006 – Sep 15, 2010. \$344,850.

Selected Talks

Microsoft. *The state of the art in differentially private synthetic data.* Feb 2022.
Invited Talk.

Tufts University. *Fair Decision Making Using Privacy-Protected Data.* Oct 2021.
Invited Talk.

Oracle Corporation. *Algorithms and Metrics for Releasing Differentially Private Statistical Summaries.* Nov 2019.
Invited Talk.

Simons Institute. *Accuracy Disparities and Social Choices in the Deployment of Privacy Mechanisms.* Apr 2019.
Invited seminar talk.

University of Washington. *Systems support for designing differentially private algorithms.* Nov 2017.
Invited Talk.

SIGMOD New Researcher Symposium. *“Towards work-life balance.”* Jun 2016.
Invited talk.

Harvard University. *“Exploring Privacy-Accuracy Tradeoffs using DPComp.”* Feb 2016.
Privacy tools group.

Boston University. *“Private Analysis of Network Data”* May 2014.
Invited Talk, Charles River Workshop on Private Analysis of Social Networks.

Paris, France. *“Private Personal Data: Protection or Profit?”* June 2013.
4th Workshop on the Protection of Privacy (4e Atelier sur la Protection de la Vie Prive)
Plenary Talk.

Brown University. *“Private Personal Data: Protection or Profit?”* Oct 2013.
Database Seminar.

University of Edinburgh. *“Managing Sensitive Personal Data: Protection or Profit?”*. May 2013.

Paris Institute of Technology. *“Pricing Queries in a Data Market- place”*. March 2013.

Technicolor, Inc., Paris France. *“Using Inference to Improve the Accuracy of Differentially-Private Output”*.
Sept 27, 2012

IAB, Nuremburg Germany. *“The Matrix Mechanism: Optimizing Linear Counting Queries Under Differential Privacy”* Workshop on Confidentiality and Disclosure . June 30, 2011

Workshop on Privacy Aspects of Data Mining (PADM). *“The Privacy Challenges of Analyzing Networks”*.
Invited Keynote, Dec 14th, 2010.

University of Twente. *“Analyzing Private Network Data”*.
Database Seminar, Jun 4th, 2010.

INRIA/ENS Cachan. *“Optimizing Linear Counting Queries Under Differential Privacy”*.
LSV Group Seminar, Jun 2nd, 2010.

Cornell University. *“Optimizing Linear Counting Queries Under Differential Privacy”*.
Database Seminar, May 24th 2010.

Dagstuhl Center for Informatics. *“Securely Managing Historical Retention in Database Systems”*.
Seminar on Distributed Usage Control, Apr 2010.

“Analyzing Private Network Data”, 2009.

Multiple institutions including: Stanford, Purdue, Illinois, Wisconsin, UC Berkeley, UC San Diego.

Stanford University. *“Analyzing Private Network Data Using Output Perturbation.”*

First Workshop on Social Network Security (SocialNetSec’09), Sep 11th 2009.

University of Edinburgh, *“Securely Managing History in Database Systems”*.

Provenance in Secure and Advanced Computer Systems Workshop, May 13th 2009

Harvard University, *“Protecting Anonymity in Published Networks”*.

Computer Science Department Colloquium, Sep 25th 2008.

Massachusetts Institute of Technology, *“Managing Historical Retention in Database Systems”*.

New England Database Day, Feb 4th 2008.

Williams College, *“Privacy and the Public Use of Social Network Data”*.

Computer Science Department Colloquium, Sep 28th 2007.

Teaching

Information Systems, CMPSCI 445. **F06, F08, S09, F10, S12, S16, S17, S18, F19, S21**

Seminar on Equitable Algorithms and Systems, COMPSCI 692E. **F19**

Information Systems, Honors Section CMPSCI 445. **F06, S12, S16.**

Database Design and Implementation, CMPSCI 645. **S06, S08, S10, S14, F18.**

Practice and Applications of Data Management, CMPSCI 345. **F16**

Programming with Data Structures, CMPSCI 187. **S14, F15.**

Principles of Data Privacy, 691DP. **S11**

Hot Topics in Databases, 691TD. **S09.**

Database Systems Laboratory, CMPSCI 591Q. **F07.**

Reliability in Information Integration, 691RI. **S07.**

Hot Topics in Information Security, 691I. **F05.**

Students & Advising

Graduated Ph.D. Students

Ryan McKenna, Ph.D. 2022. Joining Google Research.

Dan Zhang, Ph.D. 2021. Currently at Megagon.

Yue Wang, Ph.D. 2018. Currently at Microsoft.

Wentian Lu, Ph.D. 2014. Currently at Google

Chao Li, Ph.D. 2013. Currently at Google.

(Department Dissertation Award winner.)

Michael Hay, Ph.D. 2010, Currently an Assistant Prof. at Colgate University.

(Department and ACM SIGKDD Dissertation Award winner, 2011)

Graduated Masters Students

Joie Wu, M.S. 2022.

Isaac Vawter, M.S. 2018.

Luidmila Elagina, M.S. 2016.

Abhinav Parate, M.S. 2011.

Patrick Stahlberg, M.S. 2007.

Current Ph.D. Students

Arisa Tajima, expected graduation 2024.
Brett Mullins, expected graduation 2025.

Service

Editorial Activities

Program Committee Track Chair, Conference on Management of Data (SIGMOD) 2020
Program Committee Group Leader, Conference on Management of Data (SIGMOD) 2018
Area Chair, International Conference on Data Engineering (ICDE) 2017.
Area Chair, International Conference on Data Mining (ICDM) 2016.
Associate Editor, Transactions on Knowledge and Data Engineering (TKDE), Feb 2012–2014.

Organizing Activities

Co-Chair, Advisory Board, OpenDP project developing open source privacy tools.
Member of Steering Committee, Conference on Fairness, Accountability, and Transparency
Member of Steering Committee, Theory and Practice of Differential Privacy Workshop
Organizer, Dagstuhl Seminar 16291: “Data, Responsibly”, July 17-22, 2016.
Co-Chair, DBSocial: First Workshop on Databases and Social Networks, 2011.
Co-Chair, Tutorial Program, Conference on Very Large Databases (VLDB), 2011.
Web Chair, ACM Conference on Management of Data (SIGMOD), 2009.
Session Chair, Conference on Management of Data (SIGMOD) 2016.
Session Chair, Conference on Management of Data (SIGMOD) 2009.
Session Chair, Theory and Principles of Provenance Workshop (TaPP) 2009.
Session Chair, Symposium on Principles of Database Systems (PODS) 2006.

Program Committees

PC Member, International Conference on Machine Learning (ICML) 2019, 2020.
PC Member, Symposium on Principles of Database Systems (PODS) 2006, 2017.
PC Member, Conference on Management of Data (SIGMOD) 2009, 2012, 2014, 2019.
PC Member, Proceedings of the VLDB Endowment (PVLDB) 2012, 2016
PC Member, Conference on Very Large Databases (VLDB) 2007, 2008, 2010.
PC Member, Workshop on Web and Databases (WebDB) 2006, 2008, 2009, 2010, 2015, 2016.
PC Member, Conference on Privacy in Statistical Databases (PSD) 2012, 2014, 2016.
PC Member, New England Database Summit (NEDB) 2012.
PC Member, Theory and Principles of Provenance Workshop (TaPP) 2009, 2010.
PC Member, Conference on Very Large Databases, PhD Workshop, 2009, 2015.
PC Member, Conference on Very Large Databases, Demo Program, 2009.
PC Member, Conf. on Information and Knowledge Management (CIKM) 2008.
PC Member, Conference on Computer and Communications Security (CCS) 2007.
PC Member, International Conference on Data Engineering (ICDE) 2007.
PC Member, Workshop on Web Information and Data Management (WIDM) 2007.
PC Member, Symposium on Databases and Programming Languages (DBPL) 2005.

Reviewing

Reviewer, Proceedings of the National Academy of Sciences.
Reviewer, Journal of Computer and System Sciences.
Reviewer, Journal of Computer Systems Science and Engineering.
Reviewer, Journal on Very Large Databases.
Reviewer, Transactions on Database Systems.
Reviewer, Transactions on Knowledge Discovery and Data.
Reviewer, Transactions of the Web.
Reviewer, Transactions on Information and System Security.

Award Committees & Panels

Award Committee Member, SIGMOD Dissertation Award Selection Committee (2009)
Panel Member, National Science Foundation. 2006, 2008, 2009, 2012, 2013, 2014, 2019.

Departmental Service

Chair, Graduate Admissions Committee, 2020-2021.
Member, Promotion and Tenure Personnel Committee, 2020-2021.
Member, Promotion and Tenure Personnel Committee, 2019-2020.
Organizer, EQUATE (Equity, Accountability, Trust, and Explainability) faculty interest group. 2018-2020.
Co-Chair, Graduate Admissions Committee, 2015-2016.
Organizer, EQUATE meetings. 2018-2020.
Member, Executive Committee, 2015-2016.
Member, Public Relations Committee, 2015-2016.
Member, Promotion and Tenure Committee (AFR sub-committee), 2013-2014.
Member, Public Relations Committee, 2013.
Chair, Five-College Bioinformatics Search Committee, 2010-2011.
Member, Personnel Committee, 2010-2011
Member, Executive Committee, 2010-2011.
Member, Graduate Program Committee, 2009-2010.
Member, Computing and Website Committee, 2008-2011.
Chair, Information Outreach Committee, 2007-2008.
Member, Executive Committee. 2008-2009.
Member, Computing Committee, 2008-2009.
Member, Executive Committee. 2007-2008.
Member, Outreach Committee. 2007-2008.
Member, Personnel Committee. 2006-2007.
Member, Graduate Admissions Committee. 2005-2006.
Member, Special Events & Colloquia Committee. 2005-2006.