

Michael Carl Tschantz

Curriculum Vitae

Contact mct (at-sign) icsi.berkeley.edu
 www.icsi.berkeley.edu/~mct/

Education *Ph.D., Computer Science, May 2012*
 Carnegie Mellon University
 Pittsburgh, PA
 Dissertation: *Formalizing and Enforcing Purpose Restrictions*
 Advisors: Anupam Datta and Jeannette M. Wing
 Committee: Lorrie Faith Cranor, Joseph Y. Halpern, and Manuela M. Veloso

M.S., Computer Science, December 2010
 Carnegie Mellon University
 Pittsburgh, PA

Sc.B., Computer Science, May 2005
 Brown University
 Providence, RI
 Honors Thesis: *The Clarity of Languages for Access-Control Policies*
 Advisor: Shriram Krishnamurthi

Employment

2016/01 – present Senior Researcher
 International Computer Science Institute
 Berkeley, CA

2014/12 – 2015/12 Researcher
 International Computer Science Institute
 Berkeley, CA

2013/01 – 2014/12 Visiting Assistant Researcher
 School of Information, University of California, Berkeley
 Berkeley, CA

2011/09 – 2013/01 Post Doctoral Researcher
 Cylab, Carnegie Mellon University
 Moffett Field, CA

2008/06 – 2008/08 Research Assistant
 Microsoft Research India
 Bangalore, India

2007/06 – 2007/08 Research Assistant
 Software Engineering Institute, Carnegie Mellon University
 Pittsburgh, PA

2005/06 – 2005/08 Research Assistant
 Dept. of Computer Science, Brown University
 Providence, RI

2004/11 – 2005/05 Head Teaching Assistant for Intro to AI
Dept. of Computer Science, Brown University
Providence, RI

2004/06 – 2004/08 Research Assistant
Dept. of Computer Science, Brown University
Providence, RI

Publications

Conference Papers

Amit Datta, Anupam Datta, Jael Makagon, Deirdre K. Mulligan, and Michael Carl Tschantz. Discrimination in online advertising: A multidisciplinary inquiry. In Sorelle A. Friedler and Christo Wilson, editors, *Conference on Fairness, Accountability, and Transparency*, 2018.

Angelisa C. Plane, Elissa M. Redmiles, Michelle L. Mazurek, and Michael Carl Tschantz. Assessing user perceptions of online targeted advertising. In *USENIX Security*, August 2017.

Rachee Singh, Rishab Nithyanand, Sadia Afroz, Paul Pearce, Michael Carl Tschantz, Phillipa Gill, and Vern Paxson. Characterizing the nature and dynamics of Tor exit blocking. In *USENIX Security*, August 2017.

Brad Miller, Alex Kantchelian, Michael Carl Tschantz, Sadia Afroz, Rekha Bachwani, Riyaz Faizullahoy, Ling Huang, Vaishaal Shankar, Tony Wu, George Yiu, Anthony D. Joseph, and J. D. Tygar. Reviewer integration and performance measurement for malware detection. In *13th Conference on Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA)*. Springer, July 2016.

Michael Carl Tschantz, Sadia Afroz, Anonymous, and Vern Paxson. Sok: Towards grounding censorship circumvention in empiricism. In *IEEE Symposium on Security and Privacy*. IEEE Computer Society, 2016.

Michael Carl Tschantz, Amit Datta, Anupam Datta, and Jeannette M. Wing. A methodology for information flow experiments. In *Computer Security Foundations Symposium*. IEEE, 2015.

Amit Datta, Michael Carl Tschantz, and Anupam Datta. Automated experiments on ad privacy settings: A tale of opacity, choice, and discrimination. In *Proceedings on Privacy Enhancing Technologies (PoPETs)*, pages 92–112. De Gruyter Open, 2015.

Alex Kantchelian, Michael Carl Tschantz, Ling Huang, Peter L. Bartlett, Anthony D. Joseph, and J. D. Tygar. Large-margin convex polytope machine. In Z. Ghahramani, M. Welling, C. Cortes, N.D. Lawrence, and K.Q. Weinberger, editors, *Advances in Neural Information Processing Systems 27 (NIPS)*, pages 3248–3256. Curran Associates, Inc., 2014.

Michael Carl Tschantz, Anupam Datta, and Jeannette M. Wing. Purpose restrictions on information use. In *Proceedings of the 18th European Symposium on Research in Computer Security (ESORICS)*, volume 8134 of *Lecture Notes in Computer Science*, pages 610–627. Springer Berlin Heidelberg, 2013.

Michael Carl Tschantz, Anupam Datta, and Jeannette M. Wing. Formalizing and enforcing purpose restrictions in privacy policies. In *Proceedings of the IEEE Symposium on Security and Privacy*, pages 176–190, Los Alamitos, CA, USA, 2012. IEEE Computer Society.

Michael Carl Tschantz and Jeannette M. Wing. Extracting conditional confidentiality policies. In *SEFM '08: Proceedings of the Sixth IEEE International Conferences on Software Engineering and Formal Methods*, November 2008.

Michael Carl Tschantz and Shriram Krishnamurthi. Towards reasonability properties for access-control policy languages. In *SACMAT '06: Proceedings of the Eleventh ACM Symposium on Access Control Models and Technologies*, June 2006.

Kathi Fisler, Shriram Krishnamurthi, Leo A. Meyerovich, and Michael Carl Tschantz. Verification and change-impact analysis of access-control policies. In *ICSE '05: Proceedings of the 27th International Conference on Software Engineering*, pages 196–205, New York, NY, USA, 2005. ACM Press.

Michael Benisch, Amy Greenwald, Ioanna Grypari, Roger Lederman, Victor Naroditskiy, and Michael Carl Tschantz. Botticelli: A supply chain management agent. In *Third International Joint Conference on Autonomous Agents and Multiagent Systems AAMAS '04*, pages 1174–1181, New York, July 2004.

Michael Benisch, Amy Greenwald, Victor Naroditskiy, and Michael Carl Tschantz. A stochastic programming approach to scheduling in TAC SCM. In *ACM Electronic Commerce Conference ECC '04*, pages 152–160, New York, May 2004.

Workshop Papers

Alex Kantchelian, Michael Carl Tschantz, Sadia Afroz, Brad Miller, Vaishaal Shankar, Rekha Bachwani, Anthony D. Joseph, and J. D. Tygar. Better malware ground truth: Techniques for weighting anti-virus vendor labels. In *Proceedings of the 2015 ACM Workshop on Artificial Intelligence and Security (AISec)*. ACM, 2015.

Brad Miller, Alex Kantchelian, Sadia Afroz, Rekha Bachwani, Edwin Dauber, Ling Huang, Michael Carl Tschantz, Anthony D. Joseph, and J. D. Tygar. Adversarial active learning. In *Proceedings of the 2014 ACM Workshop on Artificial Intelligence and Security*, New York, NY, USA, 2014. ACM.

Alex Kantchelian, Sadia Afroz, Ling Huang, Aylin Caliskan Islam, Brad Miller, Michael Carl Tschantz, Rachel Greenstadt, Anthony D. Joseph, and J. D. Tygar. Approaches to adversarial drift. In *Proceedings of the 2013 ACM Workshop on Artificial Intelligence and Security*, pages 99–110, New York, NY, USA, 2013. ACM.

Michael Carl Tschantz and Aditya V. Nori. Measuring the loss of privacy from statistics. In *QA '09: Workshop on Quantitative Analysis of Software*, June 2009.

Sarah Bell, Michael Benisch, Maggie Benthall, Amy Greenwald, and Michael Carl Tschantz. Multi-period online optimization in TAC SCM: The supplier offer acceptance problem. In *Workshop on Trading Agent Design and Analysis*, New York, July 2004.

Technical Reports

Michael Carl Tschantz, Shayak Sen, and Anupam Datta. Differential privacy as a causal property. Technical Report arXiv:1710.05899, ArXiv, October 2017.

Michael Carl Tschantz, Serge Egelman, Jaeyoung Choi, Nicholas Weaver, and Gerald Friedland. The accuracy of the demographic inferences shown on Google's Ad Settings. Technical Report TR-16-003, International Computer Science Institute, Berkeley, CA, USA, October 2016.

Brad Miller, Alex Kantchelian, Michael Carl Tschantz, Sadia Afroz, Rekha Bachwani, Riyaz Faizullahoy, Ling Huang, Vaishaal Shankar, Tony Wu, George Yiu, Anthony D. Joseph, and J. D. Tygar. Back to the future: Malware detection with temporally consistent labels. Technical Report arXiv:1510.07338v1, ArXiv, October 2015.

Michael Carl Tschantz, Sadia Afroz, Vern Paxson, and J. D. Tygar. On modeling the costs of censorship. Technical Report arXiv:1409.3211v1, ArXiv, September 2014.

Amit Datta, Michael Carl Tschantz, and Anupam Datta. Automated experiments on ad privacy settings: A tale of opacity, choice, and discrimination. Technical Report arXiv:1408.6491v1, ArXiv, August 2014.

Michael Carl Tschantz, Amit Datta, Anupam Datta, and Jeannette M. Wing. A methodology for information flow experiments. Technical Report arXiv:1405.2376v1, ArXiv, May 2014.

Michael Carl Tschantz, Anupam Datta, and Jeannette M. Wing. Information flow investigations. Technical Report CMU-CS-13-118, School of Computer Science, Carnegie Mellon University, June 2013.

Michael Carl Tschantz, Anupam Datta, and Jeannette M. Wing. Purpose restrictions on information use. Technical Report CMU-CyLab-13-005 and CMU-CS-13-116, Carnegie Mellon University, June 2013.

Michael Carl Tschantz. *Formalizing and Enforcing Purpose Restrictions*. PhD thesis, Computer Science Department, School of Computer Science, Carnegie Mellon University, May 2012.

Michael Carl Tschantz, Anupam Datta, and Jeannette M. Wing. Formalizing and enforcing purpose restrictions in privacy policies (full version). Technical Report CMU-CS-12-106, School of Computer Science, Carnegie Mellon University, March 2012.

Michael Carl Tschantz, Anupam Datta, and Jeannette M. Wing. On the semantics of purpose requirements in privacy policies. Technical Report CMU-CS-11-102, School of Computer Science, Carnegie Mellon University, February 2011. Also available at <http://arxiv.org/abs/1102.4326>.

Michael Carl Tschantz, Dilsun Kaynar, and Anupam Datta. Formal verification of differential privacy for interactive systems. Technical Report arXiv:1101.2819v1 [cs.CR], ArXiv, January 2011.

Michael Carl Tschantz and Jeannette M. Wing. Formal methods for privacy. Technical Report CMU-CS-09-154, School of Computer Science, Carnegie Mellon University, September 2009.

Michael Carl Tschantz, Anupam Datta, and Dilsun Kaynar. Differential privacy for probabilistic systems. Technical Report CMU-CyLab-09-008, CyLab, Carnegie Mellon University, 2009.

Michael Carl Tschantz and Jeannette M. Wing. Extracting conditional confidentiality policies. Technical Report CMU-CS-08-127, School of Computer Science, Carnegie Mellon University, May 2008.

Michael Carl Tschantz and Jeannette M. Wing. Confidentiality policies and their extraction from programs. Technical Report CMU-CS-07-108, School of Computer Science, Carnegie Mellon University, February 2007.

Deepak Garg and Michael Carl Tschantz. From indexed lax logic to intuitionistic logic. Technical Report CMU-CS-07-167, School of Computer Science, Carnegie Mellon University, January 2008.

Michael Carl Tschantz and Shriram Krishnamurthi. Towards reasonability properties for access-control policy languages with extended XACML analysis. Technical Report CS-06-04, Computer Science Department, Brown University, April 2006.

Michael Matthew Greenberg, Casey Marks, Leo Alexander Meyerovich, and Michael Carl Tschantz. The soundness and completeness of margrave with respect to a subset of XACML. Technical Report CS-05-05, Computer Science Department, Brown University, April 2005.

Miscellaneous Papers

Michael Carl Tschantz, Dilsun Kaynar, and Anupam Datta. Formal verification of differential privacy for interactive systems (extended abstract). *Electron. Notes Theor. Comput. Sci.*, 276:61–79, September 2011. Presented at the 27th Annual Conference on Mathematical Foundations of Programming Semantics, Invited Paper.

Michael Carl Tschantz and Jeannette M. Wing. Formal methods for privacy. In *Proceedings of the 2nd World Congress on Formal Methods*, pages 1–15, Berlin, Heidelberg, 2009. Springer-Verlag.

Michael Carl Tschantz. The clarity of languages for access-control policies. Undergraduate Honors Thesis, Department of Computer Science, Brown University, May 2005.

Michael Benisch, Amy Greenwald, Ioanna Grypari, Roger Lederman, Victor Naroditskiy, and Michael Carl Tschantz. Botticelli: A supply chain management agent designed to optimize under uncertainty. *SIGecon Exchanges*, 4:29–37, 2004.

Posters

Conferences

Amit Datta, Anupam Datta, Lay Kuan Loh, Michael Carl Tschantz, and Zheng Zong. “Poster: Evaluating the effectiveness of privacy tools using Information Flow Experiments” at IEEE Symposium on Security and Privacy 2016/05.

Amit Datta, Anupam Datta, Suman Jana, and Michael Carl Tschantz. “Poster: Information Flow Experiments to study News Personalization” at IEEE Symposium on Security and Privacy 2015/05.

Michael Carl Tschantz, Anupam Datta, and Jeannette M. Wing. “Poster: The Semantics of Purpose Requirements in Privacy Policies” at IEEE Symposium on Security and Privacy 2011/05.

Panels

Workshops

9th Workshop on Security and Human Behavior (SHB), 2016/05

5th International Workshop on Data Usage Management, An IEEE CS Security & Privacy Workshop, 2014/05

2nd International Workshop on Accountability: Science, Technology and Policy, MIT Computer Science and Artificial Intelligence Laboratory, 2014/01

Workshop on Semantic Computing for Security and Privacy held in conjunction with The 5th IEEE International Conference on Semantic Computing, 2011/09

Talks

“Discrimination in Online Personalization: A Multidisciplinary Inquiry”, Civil Rights Division, United States Department of Justice, 2018/01/18.

“Machine Learning and Discrimination: Effects on Privacy and Security”, Berkeley Information Privacy Law Association, 2017/11/20.

“Discrimination in Online Personalization: A Multidisciplinary Inquiry”, hosted speaker, Unlocking the Black Box Conference, Yale Law School, 2016/02/02.

“Automated Experiments on Ad Privacy Settings”, PrivacyCon, Federal Trade Commission, Washington, D.C., 2016/01/14.

“Privacy and Composition (Part 2)”, invited speaker, Privacy by Design Workshop #3, Computing Community Consortium, Computing Research Association, Pittsburgh, PA, 2015/09/01

“AdFisher: Information Flow Experiments on Ad Privacy Settings”, hosted speaker, Max Planck Institute for Software Systems, 2015/07/22

“Automated Experiments on Ad Privacy Settings: A Tale of Opacity, Choice, and Discrimination”, invited speaker, CSL Student Conference, Coordinated Science Laboratory, University of Illinois at Urbana-Champaign, 2015/02/27

“Privacy Principles, Properties, and Mechanisms”, requested presentation by conference call, NPRF WG, National Coordination Office for Networking and Information Technology R&D, 2015/02/13

“Privacy Principles, Properties, and Mechanisms”, invited speaker, Privacy by Design Workshop #1, Computing Community Consortium, Computing Research Association, Berkeley, CA, 2015/02/05

“Privacy through Accountability: Information Flow Experiments”, Fairness, Accountability, and Transparency in Machine Learning; NIPS 2014 Workshop; Montreal, Canada; 2014/12/12

Program Committees

Conferences

IEEE Computer Security Foundations Symposium (CSF), 2014, 2016, 2018

International World Wide Web Conference (WWW), 2016, 2018

Privacy Enhancing Technologies Symposium (PETS), 2016–18

The Conference on Fairness, Accountability, and Transparency (FAT*), 2018

Workshops

8th USENIX Workshop on Free and Open Communications on the Internet (FOCI), 2018

Workshop on Data and Algorithmic Transparency (DAT), 2016

Workshop on Foundations of Computer Security held in conjunction with CSF, 2016

The 2nd&3rd IEEE International Workshop on Privacy Engineering (IWPE'16&17), co-located with IEEE S&P, 2016–17

The 8th&9th ACM Workshop on Artificial Intelligence and Security (AISec) held in conjunction with ACM CCS, 2015–17

Workshop on Privacy in the Electronic Society (WPES) held in conjunction with ACM CCS, 2014

The Fifth International Workshop on Data Usage Management (DUMA 2014) held in conjunction with IEEE S&P, 2014

The Second International Workshop on Network Forensics, Security and Privacy (NFSP-13) held in conjunction with IEEE ICDCS, 2013

Reviewing, Subreviewing

Journals

ACM Transactions on Information and System Security

ACM Transactions on Internet Technology

ACM Transactions on Intelligent Systems and Technology

ACM Transactions on Programming Languages and Systems

ACM Transactions on Software Engineering and Methodology

ACM Transactions on the Web

IEEE Transactions on Dependable and Secure Computing

Journal of the American Medical Informatics Association

MDPI Games

Theoretical Computer Science, Elsevier

VLDB Journal

Conferences

ACM Conference on Computer and Communications Security (CCS)

ACM Symposium on Information, Computer and Communications Security (ASIACCS)

Asian Computing Science Conference (ASIAN)

European Symposium on Research in Computer Security (ESORICS)

IFIP International Conference on Formal Techniques for Distributed Objects, Components and Systems (FORTE)

IEEE Computer Security Foundations Symposium (CSF)

IEEE Symposium on Security and Privacy (IEEE S&P, "Oakland")

International Conference on Computer Aided Verification (CAV)

International Conference on Foundations of Software Science and Computation Structures (FoS-SaCS)

International Conference on Information Systems Security (ICISS)

Mathematical Foundations of Programming Semantics (MFPS)

Privacy Enhancing Technologies Symposium (PETS)

USENIX Security

January 18, 2018