Curriculum Vitae: Sarah Ann Scheffler

CONTACT INFORMATION

Website: https://sarahscheffler.net
Email: sscheffl@cmu.edu
Phone: +1 412-438-8612

ACADEMIC POSITIONS HELD

Carnegie Mellon University (CMU)
Assistant Professor
CyLab (CMU Security and Privacy Institute, core faculty)
Engineering and Public Policy Department (CMU College of Engineering, 50% joint appointment)
Software and Societal Systems Department (CMU School of Computer Science, 50% joint appointment)
August 2024 - Present

Massachusetts Institute of Technology
Postdoctoral Associate
Internet Policy Research Initiative
September 2023 - August 2024

Princeton University
Postdoctoral Research Associate
Center for Information Technology Policy
September 2021 - August 2023

EDUCATION

Boston University
Ph.D. in Computer Science
Advisor: Prof. Mayank Varia
Thesis: Decrypting Legal Dilemmas
Computer Science Research Excellence Award
September 2016 - June 2021

Harvey Mudd College
B.S. joint in Computer Science and Mathematics
Departmental Honors in Computer Science
Graduated with Distinction
Concentration ("minor") in Political Science
September 2011 - May 2015

PEER-REVIEWED ARCHIVAL PUBLICATIONS

[1] Yanzi Lin, Cheng Zhang, Madelyne Xiao, Lorrie Faith Cranor, Sarah Scheffler.
What Adults Will (and Won't) Do to Prove Their Age: Empirical Evidence from a Deceptive Web Experiment.
USENIX Security 2026.
https://www.usenix.org/system/files/usenixsecurity26-lin-yanzi.pdf.
(Short tech report version: https://cs.cmu.edu/~sscheffl/AgeVerifFTC.)

[2] B. Hagag, W. L. Anderson, C. S. de Witt, S. Scheffler.
Architecture Matters for Multi-Agent Security.
International Conference on Machine Learning (ICML) 2026.
https://arxiv.org/pdf/2604.23459.

[3] S. Liu, S. Scheffler.
Adequately Tailoring Age Verification Regulations.
ACM Symposium on Computer Science and Law (ACM CS&Law) 2026.
https://arxiv.org/abs/2601.20241.

[4] M. Xiao, A. Sellars, S. Scheffler.
When Anti-Fraud Laws become a Barrier to Computer Security Research.
ACM Symposium on Computer Science and Law (ACM CS&Law) 2025.
https://arxiv.org/abs/2502.02767.

[5] S. Scheffler, J. Mayer.
Group Moderation under End-to-End Encryption.
ACM Symposium on Computer Science and Law (ACM CS&Law) 2024.
https://dl.acm.org/doi/abs/10.1145/3614407.3643704.

[6] S. Scheffler, A. Kulshrestha, J. Mayer.
Public Verification for Private Hash Matching.
IEEE Security & Privacy (IEEE S&P) 2023.
https://ia.cr/2023/029.

[7] S. Scheffler, J. Mayer.
Systematization of Knowledge: Content Moderation for End-to-End Encryption.
Privacy Enhancing Technologies Symposium (PETS) 2023.
https://arxiv.org/abs/2303.03979.

[8] A. Cohen, S. Scheffler, M. Varia.
Can the government compel decryption? Don't trust—verify.
In ACM Symposium on Computer Science and Law (ACM CS&Law) 2022.
https://arxiv.org/abs/2208.02905.

[9] S. Scheffler, E. Tromer, M. Varia.
Formalizing Human Ingenuity: A Quantitative Framework for Copyright Law's Substantial Similarity.
In ACM Symposium on Computer Science and Law (ACM CS&Law) 2022.
https://arxiv.org/pdf/2206.01230.

[10] Y. Gvili, J. Ha, S. Scheffler, M. Varia, Z. Yang, X. Zhang.
TurboIKOS: Improved Non-interactive Zero Knowledge with Sublinear Memory.
In Applied Cryptography and Network Security (ACNS) 2021. (Acceptance rate: 19.9%)
https://ia.cr/2021/478.

[11] Y. Gvili, S. Scheffler, M. Varia.
BooLigero: Improved Sublinear Zero Knowledge Proofs for Boolean Circuits.
In Financial Crypto (FC) 2021. (Acceptance rate: 24.2%)
https://ia.cr/2021/121.

[12] S. Scheffler M. Varia.
Protecting Cryptography against Compelled Self-Incrimination.
In USENIX Security 2021. (Acceptance rate: 18.7%)
https://ia.cr/2020/862.

[13] L. Alcock, S. Asif, J. Bosboom, J. Brunner, C. Chen, E. Demaine, R. Epstein, A. Hesterberg, L. Hirschfeld, W. Hu, J. Lynch, S. Scheffler, L. Zhang.
Arithmetic Expression Construction.
In International Symposium on Algorithms and Computation 2020. (Acceptance rate: 31.2%)
https://arxiv.org/abs/2011.11767.

[14] J. Ani, S. Asif, E. Demaine, Y. Diomidov, D. Hendrickson, J. Lynch, S. Scheffler, A. Suhl.
PSPACE-completeness of Pulling Blocks to Reach a Goal.
In the Journal of Information Processing 2020.
https://www.jstage.jst.go.jp/article/ipsjjip/28/0/28_929/_pdf.

[15] J. Milligan, S. Scheffler, A. Sellars, T. Tiwari, A. Trachtenberg, M. Varia.
Case Study: Disclosure of Indirect Device Fingerprinting in Privacy Policies.
In Socio-Technical Aspects of Security 2019.
https://arxiv.org/abs/1908.07965.

[16] J. Ani, S. Asif, E. Demaine, Y. Diomidov, D. Hendrickson, J. Lynch, S. Scheffler, A. Suhl.
PSPACE-completeness of Pulling Blocks to Reach a Goal.
In the Japan Conference on Discrete and Computational Geometry, Graphs, and Games 2019.
https://www.jstage.jst.go.jp/article/ipsjjip/28/0/28_929/_pdf.

[17] R. Canetti, A. Cohen, N. Dikkala, G. Ramnarayan, S. Scheffler, A. Smith.
From Soft Classifiers to Hard Decisions: How fair can we be?.
ACM Fairness, Accountability, and Transparency 2019. (Acceptance rate: 24%)
https://arxiv.org/abs/1810.02003.

[18] S. Scheffler, S. Smith, Y. Gilad, S. Goldberg.
The Unintended Consequences of Email Spam Prevention.
In International Conference on Passive and Active Network Measurement 2018. (Acceptance rate: 40%)
https://link.springer.com/chapter/10.1007/978-3-319-76481-8_12.

BOOK CHAPTERS

[19] T. Morrison, S. Scheffler, B. Pal, A. Viand.
Private Outsourced Translation for Medical Data.
Book chapter in "Protecting Privacy through Homomorphic Encryption" (2021), pp. 107-116.
https://link.springer.com/chapter/10.1007/978-3-030-77287-1_7.

PEER-REVIEWED NON-ARCHIVAL PAPERS NOT LISTED ABOVE

[20] S. Scheffler, G. Sullivan.
Human Rights Challenges and Directions for Hash-sharing Governance.
In Data for Policy Europe 2025.

[21] S. Liu, S. Scheffler.
Privacy-preserving Age Verification based on Improved Verifiable Credentials Framework.
In Workshop on Technology and Consumer Protection 2025.
https://conpro25.ieee-security.org/papers/liu-conpro25.pdf.

MANUSCRIPTS

[22] K. Merrill, A. Woo, W. Zheng, S. Scheffler.
Zero Knowledge Barcode Decoding with Application to Private Online Attribute Verification.
Preprint. August 2026.
https://ia.cr/2026/1567.

[23] Christian Schroeder de Witt et al.
Open Challenges in Multi-Agent Security: Towards Secure Systems of Interacting AI Agents.
Preprint. Apr 2026 (v2).
https://arxiv.org/abs/2505.02077.

[24] Y. Lin, C. Zhang, M. Xiao, L.F. Cranor, S. Scheffler.
User (Non-)Compliance with Age Verification: Preliminary Evidence from a Deceptive Web Experiment.
Tech report. Jan 2026.
https://www.cs.cmu.edu/~sscheffl/docs/2026/AgeVerif2026.pdf.

[25] S. Scheffler, S. Liu.
Exploring Privacy in ID-Based Age Verification Architectures.
Manuscript position paper for W3C/IAB Age Verification Workshop. Oct 2025.
https://datatracker.ietf.org/doc/slides-agews-paper-exploring-privacy-in-id-based-age-verification-architectures/.

[26] M. Xiao, P. Jain, M. Gorelick, S. Scheffler.
Synopsis: Secure and private trend inference from encrypted semantic embeddings.
Preprint. May 2025.
https://arxiv.org/abs/2505.23880.

[27] E. Gaumond, F. Fewer, S. Scheffler, M. Xiao, P. Déziel, M. Dupuis-Crane.
Ready for Prime Time? Are Age Assurance Systems Sophisticated Enough to Verify Users' Age Without Breaching their Privacy Rights?
Manuscript. Sep 2024.
https://www.cippic.ca/news/cippic-submision-on-age-assurance.

[28] T. Reynolds, S. Scheffler, D.J. Weitzner, A. Wu.
Mind the Gap: Securely modeling cyber risk based on security deviations from a peer group.
Manuscript. Feb 2024.
https://arxiv.org/abs/2402.04166.

[29] S. Scheffler, J. Ostling.
Dismantling False Assumptions about Autonomous Weapon Systems.
Manuscript. 2019.
Won 2nd place in the Student Paper Competition at the ACM CSLaw Student Paper Competition in 2019.
https://sarahscheffler.net/2019/Autonomous_Weapons_False_Assumptions.pdf.

[30] J. Hennessey, S. Scheffler, M. Varia.
On Resilient Password-Based Key Derivation Functions.
Preprint. 2018.
https://sarahscheffler.net/diskcrypt/draft-2018-bog.pdf.

ARTICLES AND BLOG POSTS

Communications of the ACM:
Age Verification Systems Will Be a Peronal Identifiable Information Nightmare (Jun 2024, https://cacm.acm.org/opinion/age-verification-systems-will-be-a-personal-identifiable-information-nightmare/)

The Conversation:
Artificial intelligence must know when to ask for human help (Mar 2019)

Cyber Alliance Blog:
(Fewer Than) Five Reasons the Tech Sector Isn't All That Different (Feb 2018)
Google Has Its Fingers In Many Pies, But Isn't Monopolizing Any Individual Pie (July 2018)
Computers are Poor Decision-Makers for Ill-Defined Problems (Aug 2018)
The Skeletons in My Closet Are Styrofoam But It's Really None Of Your Business (Sep 2018)

PANELS, INTERVIEWS AND PRESS QUOTES

- Speaker at three unlisted events under Chatham House Rules to discuss age verification in 2025–2026.
- Panelist at SIIA Digital NEXT event
(July 2026, https://www.linkedin.com/posts/siia_last-month-siia-was-pleased-to-co-host-a-activity-7491564134510247936-SB__)

- Panelist at State of the Net 2026 for Panel: "Verifying the Future: The Paxton Decision, Age Assurance, and the Next Phase of Online Safety" (Feb 2026, https://www.stateofthenet.org/sotn-26/)

- Panelist at Federal Trade Commission Age Verification Workshop for Panel 2: "From Biometrics to Behavioral Signals: Age Verification Tools" (Jan 2026, https://www.ftc.gov/news-events/events/2026/01/age-verification-workshop)

- Moderator at Transforming Cybersecurity (University of Pittsburgh Workshop) for Panel: "Perspectives on Risk" (Aug 2025, https://www.engineering.pitt.edu/contentassets/a07b5ba3dd1d451486d8083262b283bd/rba11-transforming_cybersecurit.pdf [sic])

- Quoted in "UK users are losing a key Apple security feature, raising questions about the future of privacy" by Clare Duffy, CNN (Feb 2025, https://www.cnn.com/2025/02/25/tech/apple-advanced-data-protection-uk-encryption/index.html)

- Work described on the Cyber Alliance Blog in "Could math change the law? What the 5th Amendment means in cryptography" (Mar 2021)

- Interviewed in "Security vs Privacy – Why should you have to choose on messaging apps?" (Mar 2021)

PUBLIC TALKS

Privacy Stories from our Everyday Lives – Data Privacy Day at the Carnegie Library of Pittsburgh (Jan. 2026, 2025).

INVITED TALKS

CSIRO Australia Cybersecurity Seminar (October, 2026)
CyLab Seminar (November, 2024)
Cornell Security Seminar (April, 2023)
EPFL SPRING Lab Seminar (November, 2022)
Stanford Security Lunch (November, 2022)
Microsoft Research Cryptography and Privacy Colloquium (November, 2022)
ACM CS/Law (November, 2022)
Rutgers Seminar for the REU Summer Program at DIMACS for Mathematics and Computer Science (June, 2022)
DIMACS Workshop on the Co-Development of Computer Science and Law (May, 2022)
CS+Law Research Presentations through Northwestern Univeristy (May, 2022)
USENIX Security (Aug. 2021)
Privacy Law Scholars Conference (June 2021)
Cryptic Commons Workshop (May 2021)
Georgetown Data Co-Ops Meeting (Mar. 2021)
Duke Privacy and Security Seminar (Mar. 2021)
Stanford Security Seminar (Feb. 2021)
Berkeley Cryptography Seminar (Jan. 2021)
Winter Security Seminar Series at Carnegie Mellon University (Jan. 2021)
Real World Crypto (Jan. 2021)
MIT Security Seminar (Dec. 2020)
Guest lecturer at ETH Zurich course "Approaches to Authentication and Security: Views from Law, Economics, and the Scientific Disciplines" (Nov. 2020)
Northeastern Privacy Scholars Workshop (Nov. 2020)
DIMACS Workshop on the Co-Development of Computer Science and Law (Nov. 2020)
Boston University Security Seminar (Oct. 2020)

Cybersecurity Law and Poicy Scholars Conference (planned Apr. 2020, two papers accepted for discussion, event postponed to Dec. 2020 due to COVID-19)
Bridging Privacy seminar at Berkman Klein Center for Internet and Society (Dec. 2019)
Cornell Crypto Seminar (Nov. 2019)
Carnegie Mellon University AI Seminar (Oct. 2019)
Boston University CyberAlliance Seminar (Dec. 2018)

COURSES TAUGHT AT CMU

Applied Methods for Technology-Policy Analysis (19-351; Spring 2026)
Privacy Policy, Law, and Technology (17-333 / 17-733 / 19-608 / 95-818; Fall 2026, Fall 2025)
Privacy by Design Workshop & Practicum (17-606 / 17-607; Fall 2024)
Current Topics in Privacy Seminar (17-702 / 19-602 / 95-862; Fall 2024)

PROGRAM AND ETHICS COMMITTEES

Program Committee Vice-Chair:
USENIX Security (2026)

Conference Program Committee member:
USENIX Security (2027, 2025, 2023)
ACM Computer Science and Law (2027–2024)
IEEE Euro Security & Privacy 2024
ACM Conference on Fairness, Accountability, and Transparency (ACM FAccT) 2023

Research Ethics Committee member:
USENIX Security (2025)

Workshop Program Committee member:
Privacy and Public Policy Conference 2027
New England Security Day 2024
Generative AI + Law 2023
Workshop on Foundations of Computer Security 2023, 2021

External Reviewer:
CHI 2026
CRYPTO 2025
IEEE Security & Privacy Magazine 2024
Eurocrypt 2024
USENIX Security 2022
IEEE Security & Privacy 2021
ISCA Symposium on Security and Privacy in Speech Communication 2021
Theory of Cryptography Conference 2020
Eurocrypt 2020
IEEE Security & Privacy 2020
ACM Conference on Fairness, Accountability, and Transparency 2020
IEEE Computer Security Foundations Symposium 2018
International Conference on Cryptology and Network Security 2017
International Conference on Information Theoretic Security 2016

Shadow Program Committee member:
IEEE S&P 2020

WORKSHOPS ORGANIZED

Privacy and Public Policy Conference (Planning committe chair: 2026; Discussion lead: 2024)
CMU CyLab Robotics Security and Privacy Workshop (Co-organizer: 2025)
ACM CS/Law Workshop for Junior Scholars (Co-chair: 2025, 2024)
Privacy Enhancing Technology for the Public Interest (Co-organizer: 2023, 2022)

HONORS, AWARDS, AND FELLOWSHIPS

Google Ph.D. Fellowship (supported my Ph.D. research 2019-2021)
Clare Boothe Luce Graduate Fellowship (supported my Ph.D. research 2017-2019)
Boston University Computer Science Research Excellence Award (2021)
RSA Conference Security Scholar (2020)
ACM CSLaw Student Paper Competition: 2nd Place (2019)
Clinic Team Award, HMC Computer Science Department (2015, awarded for an exceptional capstone project)
International Mathematical Competition in Modeling: Meritorious Winner (2014), Honorable Mention (2015)

HIGH SCHOOL OUTREACH

RACECAR Crash Course: From Oct. 2018 - Jan. 2019, volunteered as a teaching assistant for this program to prepare high school students for the Beaver Works Summer Institute RACECAR course in the summer.
Code Creative: From Jan. 2017 - Jan. 2018, was a mentor for Code Creative, a computer science education program for Boston-area high school students who do not have access to a computer science course at their schools. Was responsible for creating slides and labs, lecturing, organizing, and in-class tutoring. https://www.codecreative-ll.org/
Codebreakers: In summer 2016, as one of a team of three, created and taught a summer cybersecurity class for high school girls. Was responsible for creating the curriculum, creating class material and exercises, and leading classes. In 2017, 2018, and 2019, was a guest lecturer. https://www.bu.edu/lernet/cyber/

OTHER WORK EXPERIENCE

Assistant Staff MIT Lincoln Laboratory Sep. 2015 - June 2016

Worked in the Secure and Resilient Systems and Technology group within the Cybersecurity and Information Sciences division. Assisted in the implementation and testing of a library that adds confidentiality and integrity guarantees to the Accumulo database, protecting it against a malicious server or sysadmin.

Intern: Implementing Oblivious RAM MIT Lincoln Laboratory Summer 2015

Designed and implemented an Oblivious RAM for the Accumulo database in Java, to hide a querying client's access patterns from a malicious server as part of a larger project within the Secure and Resilient Systems and Technology group.

Capstone: Evaluating Latent Fingerprints MITRE Corporation and HMC Fall 2014 - Spring 2015

Worked on a team of four students to design, implement, and test a system that uses image processing and machine learning techniques to evaluate the suitability of crime scene fingerprint images for identification by Automated Fingerprint Identification Systems.

Summer Undergrad Research: Testing Cryptographic Entropy Sources NIST Summer 2014

Worked with Dr. Allen Roginsky in the Computer Security Division of the National Institute of Standards and Technology (NIST) to improve NIST's statistical tests for entropy sources in cryptographic random number generators. Also made adjustments to the process for generating large primes for cryptography.