PEPR '24: 2024 USENIX Conference on Privacy Engineering Practice and Respect

June 3–4, 2024, Santa Clara, CA, USA

Sponsored by USENIX, the Advanced Computing Systems Association

The **2024 USENIX Conference on Privacy Engineering Practice and Respect (PEPR '24)** will take place on June 3–4, 2024, at the Hyatt Regency Santa Clara in Santa Clara, CA, USA.

Important Dates

- Submissions deadline: **Monday, February 12, 2024**
- Notification to presenters: **Thursday, March 14, 2024**

Conference Organizers

Program Co-Chairs

Nuria Ruiz, *Outschool.com*
Lawrence You, *Google*

Program Committee

Jay Averitt, *Microsoft*
Greg Chappell, *Meta*
R. Jason Cronk, *Institute of Operational Privacy Design*
Damien Desfontaines, *Tumult Labs*
Apoorvaa Deshpande, *Snap*
Giles Douglas, *BetterOmics*
Cat Easdon, *Dynatrace*
Steven Englehardt, *DuckDuckGo*
Debra J Farber, *Privacy Advisor*
Nathaniel Fruchter, *Google*
Vaibhav Garg, *Comcast Cable*
Bhavani Shankar Garikapati, *Lyft*
Emily Greene, *Moveworks*
Hana Habib, *Carnegie Mellon University*
Michael Hay, *Tumult Labs and Colgate University*
Isaac Johnson, *Wikipedia*
Farzaneh Karegar, *Karlstad University*
Nandita Narla, *Doordash*
Madison Pickering, *University of Chicago*
Shivan Sahib, *Brave Software*
Behrooz Shafiee, *Stripe*
Daniel Simmons-Marengo, *Tumult Labs*
Peter Snyder, *Brave Software*
Mohammad Tahaei, *eBay*
Hal Triedman, *Wikipedia*
Ben Weinshel, *Apple*
Molly Weiss, *Google*
Primal Wijesekera, *University of California, Berkeley*
Simone Wu, *Google*
Tariq Yusuf, *Kalles Group*
Shikun Aerin Zhang, *TikTok*

Steering Committee

Lorrie Cranor, *Carnegie Mellon University*
Casey Henderson-Ross, *USENIX Association*
Lea Kissner, *Lacework*
Divya Sharma, *Google*
Blase Ur, *University of Chicago*

Overview

The 2024 Conference on Privacy Engineering Practice and Respect (PEPR '24) is a single-track conference focused on designing and building products and systems that enhance privacy and respect for both users and society. Our goal is to improve the state of the art and practice in designing for privacy and respect, as well as to foster a deeply knowledgeable community of privacy practitioners and researchers who collaborate toward that goal.

We view diversity as a key enabler of this goal. Effectively designing for privacy and respect is a challenge in and of itself; attempting this without a range of perspectives is harder still. Thus, we encourage and welcome participation from all employment sectors, racial and ethnic backgrounds, nationalities, genders, disability statuses, ages, and all those other differences which make us richer as humanity.

PEPR '24 is committed to fostering a respectful and collaborative environment. Please see the USENIX Event Code of Conduct at www.usenix.org/conferences/coc.

Call for Participation

PEPR '24 is soliciting proposals for 10- and 15-minute original talks, and 45-minute panels featuring discussions with 3–5 speakers. Additional time will be added for Q&A. The program committee will select talks that best illuminate topics in the fields of practical privacy engineering and building systems that respect their users. PEPR is tilted toward constructive solutions, but also includes the illumination of challenges. We're interested in talks from both practitioners and researchers about design proposals, research, deployed systems, case studies, and experience reports.

We are particularly interested in talks addressing the following themes:

Talks focused on building. Usability, crypto, and anonymization are all important, but these are only a small slice of what is needed to build for privacy and respect. PEPR is designed to take a comprehensive view, including topics like architecting large-scale systems for reliable and measurable data deletion, end-to-end consent (from the user all the way to infrastructure), data access and handling (how do you grant it, how do you understand it, how do you enforce it, how do you build a system for debugging with minimal data and access, etc.), how to do a privacy review (design, code, test), privacy red-teaming, incident management, root cause analysis and coming full-circle, how to run an engineering-focused privacy program, and many, many, many more. We encourage case studies demonstrating the integration of practical considerations while building in any of these areas. In addition, we encourage talks related to building for a variety of privacy use cases (e.g., compliance, consumer product innovation, user controls, data transparency and portability).

Talks focused on practice. PEPR focuses on designing for privacy and respect in real-world systems. Everything technical is more complex when it hits the real world, but privacy is more so because 1) there are a lot of humans and personal information involved; and 2) there are more regulatory and legal requirements than in many other technical fields. We encourage proposals that talk about the intersection of privacy and other fields as we build real-world systems (e.g., the intersection of privacy, applied ethics, safety, competition, and AI). Lastly, we see Privacy Engineering as a discipline and vital self-supporting community and encourage talks that foster community and career development.

Talks focused on applied research. We welcome proposals that focus on different aspects of privacy research that could help influence privacy designs in practice, as well as empirical studies that could be used by practitioners to make either better decisions or a stronger case for privacy engineering. Some examples include research related to privacy user interfaces, adoption/use of privacy-related tools or features, attitudes and preferences related to privacy, surveys of how frequently various technologies are deployed, rates of compliance/non-compliance, and more.

Talks focused on holistic systems and governance. Privacy Engineering has evolved so that it is integrated into system design and development as well as technical and organizational governance. We welcome talks that describe software infrastructure design/development, translations of policy or regulatory requirements into specifications, end-to-end data management, and implementing organizational governance rules via engineering. We also encourage talks that describe risks to individuals/public/organizations and means to assess, test, monitor, and mitigate them.

Talks may include demos, if appropriate. New talks on previously published materials are also welcome. **Please note that we do not accept product pitches or product demos.**

Submission Guidelines

Please submit talk proposals via the submission form linked from the Call for Participation web page.

Submissions require a proposed talk title, the names (and accompanying short bios) of the speakers, a short talk abstract (approximately 200 words), and a more detailed outline of the proposed talk/panel. Slides, videos, and supplemental materials are not required, and in fact not accepted, as part of this initial submission. Submissions will be reviewed by members of the program committee based on the proposal's relevance to PEPR, as well as the quality and novelty of the proposal.

Note that PEPR is a venue for talks and panels discussing advances in privacy engineering, not a publication venue. While submissions undergo a rigorous peer-review process, there are neither formal proceedings nor archival publications. The final talk, talk abstract, talk video, and the names and bios of the speakers will appear on the conference website. Because PEPR is a venue for presentations, not publications, submissions are not anonymous during the review process.

If you have any questions, please reach out to pepr24chairs@usenix.org.