NATIONAL ACADEMIES *Sciences Engineering Medicine*

Workshop on Technology for Data Stewardship

A Forum on Cyber Resilience workshop

Data underpins the modern world, informing decisions, driving economies, enhancing health and wellbeing, and powering scientific discovery. Enabled by technology advances, data collection and analytics continue to scale up, posing challenges to data privacy and ownership. New technologies and processes are needed to protect data privacy, enforce regulations, and ensure responsible data use. The National Academies' Forum on Cyber Resilience invites you to join them online or in person in Washington, D.C. on **February 19, 2025**, for a workshop to explore current capabilities and future directions for data privacy and management technologies. Technologies to be discussed will include confidential computing, homomorphic encryption, multi-party computation, and secure hardware enclaves. This workshop builds on an October 2024 workshop organized by the German Academy of Science and Engineering (acatech) and the German Aerospace Center (DLR) which looked at data ownership and management in the EU.

WEDNESDAY, FEBRUARY 19, 2025

Purpose

- Characterize emerging needs for better data policies and controls.
- Explore current and emerging technical solutions for fine-grained control of data and what new options they afford.
- Survey current technology implementations and community efforts on secure computing standards.
- Highlight public and private investments and strategies to enable responsible data use and enhance privacy safeguards.

9:00am ET **Welcome**

9:05am ET **Panel Discussion: Characterizing the Need for Better Policies and Technologies for Data Management**

- **Moderator:** Nadya Bliss, Arizona State University, Forum Member
- Anita Nikolich, University of Illinois
- Sascha Meinrath, Pennsylvania State University
- Dylan Gilbert, NIST

10:30am ET **Break**

10:45am ET **Invited Talks: Current and Emerging Technical Solutions and Applications for Data Control and Management**

Multiparty Computation Brian LaMacchia, MPC Alliance, Forum Member

Homomorphic Encryption David Archer, Galois

12:15pm ET **Lunch**

1:15pm ET **Invited Talks: Current and Emerging Technical Solutions and Applications for Data Control and Management**

Confidential Computing John Manferdelli (*NAE*), *Cyber Forum Committee Chair*

Secure Enclaves Across CPU Architectures Eckhard Delfs, Qualcomm

2:45pm ET **Break**

3:00pm ET **Invited Talks: Current and Emerging Technical Solutions and Applications for Data Control and Management**

Enhancing Data Quality, Privacy, and Security in DLR Projects Oscar Ramirez Argudelo, DLR

3:45pm ET **Panel Discussion: Scaling Data Technologies for Real World Applications**

- **Moderator:** Nadya Bliss, Arizona State University, Forum Member
- Brian LaMacchia, MPC Alliance, Forum Member
- John Abowd, Cornell University
- Paul England (*NAE*), Forum Member

5:00pm ET **Meeting Summary**

John Manferdelli (*NAE*), *Cyber Forum Committee Chair*

5:30pm ET **MEETING ADJOURNS**

SPEAKER BIOGRAPHIES

Anita Nikolich is a Research Scientist and Director of Research Innovation at the School of Information Sciences at the University of Illinois at Urbana Champaign. She began her career as a cryptologist and has worked in multiple security leadership positions in both industry and government, including service as an NSF Program Director and co-founder of a cryptocurrency futures exchange.

Sascha Meinrath is the Palmer Chair in Telecommunications at Penn State and director of X-Lab, an innovative think tank focusing on the intersection of vanguard technologies and public policy. Professor Meinrath is a renowned technology policy expert and is internationally recognized for his work over the past two decades as a community internet pioneer, social entrepreneur, and angel investor. Prior to founding X-Lab, Meinrath was vice president of the New America Foundation, where he founded the Open Technology Institute in 2008 and built it into one of the largest public interest tech policy organizations in Washington, D.C. He also founded the Commotion Wireless Project, which works around the globe to strengthen communities by providing tools to build their own local communications infrastructures, and co-founded Measurement Lab, a global online platform for researchers to deploy Internet measurement tools that empower the public and key decision-makers with useful information about broadband connectivity. He serves as a board member for the American Indian Policy Institute, Brave New Software Foundation; Defending Rights and Dissent Foundation; Acorn Active Media Foundation; and Fourth Amendment Advisory Committee. He is also a member of the advisory councils for the Calyx Institute, FreedomBox Foundation, Loomio, and Whistleblower Aid.

Dylan Gilbert is the Privacy Engineering Program Lead in the Information Technology Lab at the National Institute of Standards and Technology, U.S. Department of Commerce. In this role, he advances the development of privacy risk management processes and integrating solutions for protecting individuals' privacy into current and emerging information technologies. Prior to joining NIST, he was Policy Counsel at Public Knowledge where he led and developed all aspects of the organization's privacy advocacy. This included engagement with civil society coalitions, federal and state lawmakers, and a broad cross-section of external stakeholders on issues ranging from consumer IoT security to the development of comprehensive federal privacy legislation. He spent the early part of his career as a working musician and freelance writer in his native southern California.

Brian LaMacchia is an applied cryptographer who is currently serving as the first Executive Director of the MPC Alliance, a consortium of over 50 companies and academic institutions formed to accelerate awareness, acceptance, and adoption of secure multi-party computation (MPC) technology. Brian retired from Microsoft Corporation in December 2022 after a 25+-year career with the company where he was Microsoft's Distinguished Engineer for Cryptography, head of the Security and Cryptography team within Microsoft Research, and co-founder and chair of the Microsoft Cryptography Review Board. He is an Adjunct Associate Professor in the School of Informatics and Computing at Indiana University-Bloomington, an Affiliate Faculty member of the Department of Computer Science and Engineering at the University of Washington, and an Advisor to Quantropi, Inc. Brian also currently serves as Treasurer of the International Association for Cryptologic Research (IACR) and as a Vice President of the Board of Directors of Seattle Opera. Brian received S.B., S.M., and Ph.D. degrees in Electrical Engineering and Computer Science from MIT in 1990, 1991, and 1996, respectively.

David Archer has over 30 years of research and development experience in system hardware and software architecture, secure computation, cryptography, and data-intensive systems. Currently, Dr. Archer leads projects in several DARPA programs, including the SafeWare program (cryptographic program obfuscation); the Brandeis program (privacy-preserving computation and databases); and the Transparent Computing program (analysis of computation by its provenance). Dr. Archer also heads research projects for IARPA and the Department of Homeland Security. At Galois, Dr. Archer leads the company's research work on secure multi-party computation, applied cryptography, information security, and data provenance. Dr. Archer holds a PhD in Computer Science from Portland State University, and an MS in Electrical Engineering and BS in Computer Engineering from the University of Illinois at Urbana-Champaign.

Eckhard Delfs received the Dipl.-Ing. degree in electrical engineering, specializing in communication electronics, from RWTH Aachen University of Technology, Aachen, Germany, in 1994. In 1995, he joined Ericsson Eurolab Germany as a System Designer, focusing on speech encoding algorithms, traffic simulations, and enhancing gateway channel capacity in mobile networks. In 2003, he joined the concept engineering group at Infineon, where he developed security concepts for mobile platforms, defined and reviewed security requirements, assessed third-party security IPs, and managed the EU-funded project OpenTC (Open-Trusted-Computing) for an Infineon subsidiary. His work also included performance optimizations of cryptographic algorithms using high-performance DSPs and prototyping a trusted execution environment. Since 2011, he has been with Intel Germany, serving as a Product Security Expert. His responsibilities included mentoring project teams, conducting threat modeling, and defining product segment-specific mitigations. He also presented security concepts to internal and external stakeholders. From 2020 to 2022, he was a Senior Expert for security topics in the Connected Mobility Solutions business unit at Elektrobit Automotive, where he served as the technical contact for UNECE R155 specifications, conducted code reviews, and analyzed test procedures from a cybersecurity perspective. In 2022, he joined Qualcomm Germany as a Principal Engineer in the product security engineering team. He is currently involved in task groups dealing with confidential computing topics at RISC-V International. Mr. Delfs holds seven patents.

John Manferdelli, (NAE), chair of the forum on cyber resilience is an independent consultant. Before that, he was, most recently, Confidential Computing, Incubation Project Leader in the Office of the CTO at VMware. Previously, he was Professor of the Practice and executive director of the Cybersecurity and Privacy Institute at Northeastern University. Immediately prior, Manferdelli was Engineering Director for Production Security Development at Google. Prior to Google, he was a senior principal engineer at Intel Corporation and co-PI (with David Wagner) for the Intel Science and Technology Center for Secure Computing at the University of California at Berkeley. He was also a member of the Information Science and Technology advisory group at DARPA and is a member of the Defense Science Board. Prior to Intel, J Manferdelli was a distinguished engineer at Microsoft and was an affiliate faculty member in computer science at the University of Washington. He was responsible for computer security, cryptography, and systems research, as well as research in quantum computing. At Microsoft, John also worked as a senior researcher, software architect, product unit manager, general manager at Microsoft and was responsible the development of the next-generation secure computing base technologies and the rights management capabilities currently integrated into Windows, for which he was the original architect. He joined Microsoft in February 1995 when it acquired his company, Natural Language Inc., based in Berkeley, California. At Natural Language, Manferdelli was the founder and, at various times, vice president of research and development and CEO. Other positions he has held include staff engineer at TRW Inc., computer scientist and mathematician at Lawrence Livermore National Laboratory, and principal investigator at Bell Labs. He was also an adjunct associate professor at Stevens Institute of Technology. Manferdelli's professional interests include cryptography and cryptographic mathematics, combinatorial mathematics, operating systems, and computer security. He is also a licensed Radio Amateur (AI6IT). Manferdelli has a bachelor's degree in physics from Cooper Union for the Advancement of Science and Art and a PhD in mathematics from the University of California, Berkeley.

Oscar Ramírez-Agudelo is a physicist with a Master's degree in Astronomy. He earned his Ph.D. in Astrophysics from the University of Amsterdam, Netherlands, in 2015. Currently, he is a researcher at the German Aerospace Center, leading the Data Quality and Privacy team within the Institute for AI Safety and Security. His research interests include predictive analysis, improving the safety and security of AI applications, and the spectroscopic study of massive stars.

John Abowd is the Edmund Ezra Day Professor Emeritus of Economics, Statistics and Data Science at Cornell University. From June 2016 until October 2022, he served as Chief Scientist and Associate Director for Research and Methodology at the U.S Census Bureau, where he led a directorate of five research centers each devoted to domains of investigation important to the future of social and economic statistics. He was the lead senior executive for the design and implementation of the 2020 Census Disclosure Avoidance System, the largest confidentiality protection system based on differential privacy ever implemented by a government agency. For this work he was awarded the 2022 EPIC Foundation Champion of Freedom Award. He served on the National Academy of Sciences Committee on National Statistics (2010-2016) and the American Economic Association's Committee on Economic Statistics (2013-2018). He currently serves as the President of the Society for Privacy and Confidentiality Research.

Paul England (NAE) retired from Microsoft in 2024 where he was a distinguished engineer and manager of a team of researchers and engineers in Microsoft Research. Paul led or contributed to many of the computer industry's hardware-based security innovations of the last 20 years. Most notable is the field of Trusted and Confidential Computing: a combination of novel cryptographic operations together with hardware/software environments for secure computation. Trusted Computing primitives are now a feature of most mobile, client, server and cloud computer systems, and the field remains an area of active research. Paul also contributed to the design of the first Trusted Platform Module and led the team that developed the current version. Paul became interested in cyber-resilient systems though his work with NIST in developing NIST SP 800-193 – Platform Firmware Resiliency Guidelines. Based on this, he subsequently worked with hardware partners and standards groups to develop architectures and hardware/software building blocks to enable secure and high assurance recovery of devices that have been compromised by malware or misconfiguration. Dr. England received his Ph.D. in condensed matter physics from Imperial College, London.