MEDIA ADVISORY

Contact: Jim Ormond
ACM Media Relations
212-626-0505
ormond@hq.acm.org

Technology Policy Experts Argue That It Is Time to Rethink Data Privacy Protections

Report Asserts That Controls Over Information Privacy Have Become Increasingly Ineffective

New York, NY, July 25, 2024 – The Association for Computing Machinery's global Technology Policy Council (TPC) has released "TechBrief: Data Privacy Protection." It is the latest in a series of TechBriefs—short technical bulletins that present scientifically grounded perspectives on the impact and policy implications of specific technological developments in computing.

"TechBrief: Data Privacy Protection" highlights the key challenge that proliferating data collection, advanced algorithms, and powerful computers have made it easy to piece together information about individuals' private lives from public information as controls over information privacy become increasingly ineffective.

The key policy implications highlighted in the TechBrief are:

- Proliferating data collection, use, and publication present rapidly accumulating risks of private information disclosure that require regulation to mitigate.
- Traditional approaches to anonymization, de-identification, and disclosure control fail to protect information at its current scale and are entirely unable to deal with new ways of utilizing information, such as generative AI.
- Inherently imperfect legal and technical solutions must balance individuals' and stakeholders' needs for data privacy and accuracy.

"Few people realize that, in just the last decade, new technologies such as generative AI have made old approaches to ensuring data privacy obsolete," explained co-author of the new TechBrief Micah Altman, Research Scientist, Center for Research on Equitable and Open Scholarship at the Massachusetts Institute of Technology. "First and foremost, the goal of this new ACM TechBrief is to make industry leaders, policymakers, and the public aware of this problem. From a technical standpoint, we call for a new set of best practices in our field to manage privacy risks. We also emphasize that privacy regulation must keep pace with privacy protection technologies."

In recent years, individual data privacy has become increasingly challenging. The TechBrief notes that when massive public data sources are being retrieved and analyzed, one way of protecting individual privacy has been to aggregate the data. But due to technical advances, too many independent analyses, even if highly aggregated, can reveal the underlying personal information. As an example, the TechBrief notes that a user of a mobile app may find private information about their employment, exercise habits, or even health at risk. Among the other important recommendations outlined in this TechBrief, the authors explain what modern privacy-enhancing technologies are and call for them to be widely implemented.

Key conclusions outlined in the TechBrief include:

- To effectively protect privacy, controls must systematically address every stage of the data life cycle from collection to publication to disposal.
- Effective data protection requires combining conservative threat assumptions, rigorous technical methods that limit inferences, and complementary non-technical controls on data use.
- Wherever reliable anonymization is needed, data policies should prefer the use of new privacy-enhancing technologies.
- Regulation of data processing should reflect the need for multiple data access strategies to support a range of uses, the need to explicitly manage cumulative privacy loss for individuals, and transparency about protective methods, privacy guarantees, and the accuracy of analytical results.

“As ACM’s Technology Policy Council is focused on educating lawmakers about issues at the intersection of technology and policy, this TechBrief calls for recognizing and addressing the realities of the current data environment,” added Stuart Shapiro, Chair of the TechBriefs Committee and Principal Cyber Security and Privacy Engineer at the MITRE Corporation. “Currently, the existing underpinnings of data protection law fail to account for the growing vulnerability of private data. While no law or regulation can completely ensure privacy and security, there are steps that can be taken. For example, we call on lawmakers to mandate transparent and accountable data processing that accounts for cumulative privacy risks. We hope that by issuing this TechBrief we can begin a dialogue with stakeholders at all levels that will lead to concrete changes to the status quo.”

ACM’s TechBriefs are designed to complement ACM’s activities in the policy arena and to inform policymakers, the public, and others about the nature and implications of information technologies. As with all TechBriefs, “TechBrief*:* Data Privacy Protection” includes an overview of the major policy implications of the technology, key statistics to put the issues in context, a narrative introduction to educate the public, and key conclusions.

“TechBrief: Data Privacy Protection” draws on collaborative research with Aaron Bembenek, Mark Bun, Aaron Fluitt, Marco Gaboardi, James Honaker, David R. O’Brien, Thomas Steinke, Salil Vadhan, Salome Viljoen, and Alex Wood. Stephen Chong, Professor of Computer Science, Harvard University, also reviewed the document and provided valuable feedback.

Earlier TechBriefs have covered topics such as automated vehicles, trusted AI, the data trust deficit, safer algorithmic systems, generative AI, climate change, facial recognition, smart cities, quantum simulation, and election auditing. Topics under consideration for future issues include media disinformation, technology abuse, accessibility and more.

About the ACM Technology Policy Council

ACM's global Technology Policy Council sets the agenda for global initiatives to address evolving technology policy issues and coordinates the activities of ACM's regional technology policy committees in the US and Europe. It serves as the central convening point for ACM's interactions with government organizations, the computing community, and the public in all matters of public policy related to computing and information technology. The Council's members are drawn from ACM's global membership.

About ACM

ACM, the Association for Computing Machinery, is the world's largest educational and scientific computing society, uniting computing educators, researchers, and professionals to inspire dialogue, share resources, and address the field's challenges. ACM strengthens the computing profession's collective voice through strong leadership, promotion of the highest standards, and recognition of technical excellence. ACM supports the professional growth of its members by providing opportunities for life-long learning, career development, and professional networking.

###