FUTURE OF PRIVACY FORUM | W&L LAW | iapp international association of privacy professionals

CALL FOR PAPERS

A NATIONAL CHALLENGE: ADVANCING PRIVACY WHILE PRESERVING THE UTILITY OF DATA

With today's technology, people's lives are integrated with information systems across all sectors of society, including commercial, social, financial, and governmental. Individuals and organizations around the world rely on a wide range of technical, administrative and legal measures to collect, manage, and protect ever-growing quantities of data, and are increasingly aware of the need to address the privacy and security interests inherent in holding and using this information.

Addressing "privacy" increasingly involves discussions of ethics, philosophy, and psychology along with law, economics, and technology. Finding an approach to future privacy concerns that supports the benefits of technology without compromising individual rights is an increasingly complex challenge. Not only is technology continuously advancing, but individual attitudes, expectations, and participation vary greatly. New ideas and approaches to privacy must be identified and developed at the same pace and with the same focus as the technologies they address.

To contribute to this important discussion, the Future of Privacy Forum, Washington & Lee University School of Law, and the International Association of Privacy Professionals are collaborating to produce an on-line Roundtable Issue of the Washington & Lee Law Review during the 2016–2017 academic year. This Issue will focus on data and privacy topics relating to the **National Privacy Research Strategy** (NPRS), published by the National Science and Technology Council's Networking and Information Technology Research and Development Program in June 2016. This call seeks papers on the privacy impact of current and projected technological advancements, focusing on the transparency, sharing, and algorithmic implications of data collection and use.

The NPRS establishes objectives for Federally-funded privacy research, with the overarching goal to "produce knowledge and technology that will enable individuals, commercial entities, and the government to benefit from transformative technological advancements, enhance opportunities for innovation, and provide meaningful protections for personal information and individual privacy."

Many privacy practices are rooted in an understanding of the Fair Information Practice Principles (FIPPs). With more complex and connected devices, services, and personal interactions, and exponentially increased quantities of data involved, the challenges of adequate privacy controls expand in ways not easily addressed by vendors or understood by consumers. Proponents of sophisticated data analysis cite benefits across industries and systems based on algorithmic interpretation of large data sets; this analysis can support social goods and consumer benefits. A key argument in favor of "big data" is that analysis promotes rapid advancement of new knowledge and discovery.

In recent years, several well-publicized studies have shown that big data analysis can analyze patterns to identify discrimination and bias; to protect vulnerable populations and communities; and to identify trends in public services and education systems to support better public policy decisions. However, there have also been challenges raised by repeated security breaches, and equally concerning examples of privacy requirements ignored or minimized. Such incidents have raised serious doubts for many about the extent to which can privacy can remain a credible right for individuals when companies are using and deriving value from large data sets without sufficient transparency, notice, access, and control. Policy advocates and technical experts are divided on the question of how privacy priorities should be managed in relation to other values, with some arguing that it is impossible to sufficiently protect privacy rights in light of the large data sets held commercially or by government agencies.

In the context of the NPRS, policy analysts struggle over what steps researchers should take to protect individuals' privacy. Making data that have been collected by governments and corporate actors

accessible can raise security and privacy risks, since some such data may be highly sensitive. In addition, individuals may have had little choice to provide the data and may not be aware that such data may one day become widely distributed (or even public) and used for secondary purposes. The expanded collection and use of data holds great promise, but also brings risk. And the need for sound principles governing privacy policy development has never been greater.

To address these challenges, FPF, W&L, and IAPP are sponsoring this Call for Papers and hosting a Symposium on Privacy Research Prioritization. Authors from multiple disciplines including law, computer science, statistics, engineering, social science, ethics and business are invited to submit papers for presentation at a full-day program to take place in Washington, D.C. in April 2017.

Successful submissions may address issues such as the following:

- This Call requests in particular topics that address or support issues within three of the main priorities outlined in the NPRS:
- Increase the transparency of data collection, sharing, use, and retention (Priority 3.4)
- Assure that information flows and use are consistent with privacy rules (Priority 3.5)
- Reduce privacy risks of analytical algorithms (Priority 3.7)

Specific questions for each priority as outlined below are paraphrased or adapted from the NPRS.

- **Transparency.** Increased transparency includes consideration of data collection, sharing, use, and retention. Individual consumers face tremendous challenges in today's technology environment. While the collection of data in some contexts is clear, how much information on individuals is collected without their awareness, and potentially by parties with whom the consumer has no direct connection or relationship? To what extent does "notice and choice" remain a practical or reasonable system of interface with consumers when providing data? Even with known parties, how are the uses to which individual data may be put continuously expanding beyond that which may be reasonably anticipated or understood by those who provide their data initially? Can privacy policies be written, posted, or communicated with any measure of effectiveness to answer these challenges? Which existing tools or data analysis techniques support privacy protective use of datasets by researchers? Is there a conflict between the needs of researchers, current technology capabilities, and existing privacy standards? What is the current state of the art in technological methods and tools for ensuring safe data collection, use and retention? How do these methods and tools balance competing requirements such as privacy, utility, and efficiency?

- **Information Flows and Consistent Privacy Rules.** Individuals need to have confidence that there are rules in place that govern the collection and flow of personal data, and that the rules are followed. Can or should data be "tagged" to maintain the original relationship to the context and consent under which it was collected? Can methods similar to those used for tracking, assuring, and archiving the data and software components be used to assure privacy compliance? What analysis methods can be developed for various kinds of information flow properties and privacy policy language with both legal value and developmental uses for how systems and code operations on personal information? How can the change in status or value or sensitivity of data, as they are combined with other information, be taken into account and properly reflected within information processing systems? Can access control systems that incorporate usage-based and purpose-based constraints be adapted to the range of privacy issues now faced by system designers? Are there effective information disclosure controls, methods for de-identifying data, and means for assessing these de-identification methods? Can anonymous and pseudonymous computing, computing with obscured or encrypted data, and management of multiple identities be made efficient and practical?

- **Analytical Algorithms.** Algorithms are used ever more extensively by government and business. Some algorithms can directly affect decision-making about particular individuals. Some can be used in ways that individuals may not always be aware of, and may not always be obviously beneficial or clearly harmful. In what ways do analytical algorithms and systems adversely affect individuals or groups? What types of concerns should individuals have with respect to predictive algorithms, what information would they need to address them, and how can this information be effectively conveyed at an individual level? How can the accuracy of data used in making a decision or a prediction about an individual or groups be assessed? How can analytical algorithms be designed to minimize adverse effects on individuals or groups? What are the impacts of analytical algorithms on individuals' autonomy and agency or in what ways do analytical algorithms create a structure that determines, affects, or limits decisions by individuals? How can new technologies and algorithms, and combinations of technologies and algorithms, provide practical and theoretical privacy-preserving data analysis?

Requirements:

Optimally, papers will contain between 5,000—8,000 words but must not exceed 10,000 words. Papers must be submitted to (paperssubmissions@fpf.org) by February 24, 2017.