



National Privacy Research Strategy outlines US privacy research agenda

Lorrie Cranor, FTC Chief Technologist

Jul 19, 2016

TAGS: [Data security](#) | [Privacy](#) | [Research](#)

The White House recently [released](#) the first ever United States “[National Privacy Research Strategy](#),” which identifies priorities for privacy research funded by the Federal government. While focused on government, the strategy is also intended to spur similar private sector efforts. I participated in the working group that developed the strategy and am excited to see it published.

The NPRS makes the case for why privacy research is important. It calls for funding for privacy research, coordination across government agencies, and mechanisms to facilitate the alignment of privacy research with real-world requirements. The NPRS outlines seven national privacy research priorities and provides a set of research questions in support of each priority.

Foster a multidisciplinary approach to privacy research and solutions. This priority recognizes that privacy research is multidisciplinary. Protecting consumer privacy requires technical research to understand privacy threats and develop tools to combat them, as well as social and behavioral science research to understand consumers’ privacy expectations and goals and the impact of privacy events on people. Multidisciplinary approaches are needed to understand when privacy protections are best implemented through technology, ethics and policy, or a combination of methods.

Understand and measure privacy desires and impacts. This priority addresses the need to both understand consumer privacy desires, and also to find ways to quantify the impact of privacy events. Research questions in the first area focus on understanding privacy desires, expectations, attitudes, beliefs, interests, and knowledge among different populations and how they impact behavior. Research questions in the second area focus on ways to define and measure privacy objectives and impacts.

Develop system design methods that incorporate privacy desires, requirements, and controls. This priority focuses on research into how to build systems that operationalize privacy. Research questions in support of this priority examine ways to use design patterns, cryptography, and other tools to implement privacy controls, as well as metrics to evaluate the effectiveness of these controls. In addition, this priority recognizes that there may be tradeoffs between privacy and system utility, and calls for research on how to maximize both.

Increase transparency of data collection, sharing, use, and retention. This priority focuses on research on improving privacy disclosures through the use of more effective language and formats, standardization, and automation. Additional research questions look at how to evaluate the effectiveness of transparency approaches, and where privacy disclosures should be supplemented with other types of protections.

Assure that information flows and use are consistent with privacy rules. This priority focuses on research to apply privacy rules to information and ensure that those rules are enforced as information is processed and flows within and between systems. For example, techniques are needed to allow data collectors to apply tags to data elements that will not only specify restriction on how those elements may be used, but also allow for automated enforcement of these restrictions.

Develop approaches for remediation and recovery. This priority focuses on developing and evaluating mechanisms to

facilitate remediation and recovery from data breaches and other privacy events.

Reduce privacy risks of analytical algorithms. The increasing use of predictive analytical algorithms combined with “big data” has led to a range of privacy concerns: algorithms may rely on inappropriate or inaccurate data, result in incorrect decisions, impact individual autonomy, and operate in contexts where there is no reasonable means of redress. This priority focuses on understanding the impact of analytical algorithms, how they may adversely impact some groups of people, and how to increase the transparency and accountability of these algorithms.

Many of the research questions discussed in the NPRS are similar to questions the FTC has asked as we consider privacy issues. We remain interested in questions that will further our work protecting consumers. Privacy research helps us to, among other things, identify potential areas for investigation and enforcement and fashion remedies.

At our first PrivacyCon event last January we showcased privacy research on topics such as data security, online tracking, consumer perceptions of privacy, privacy disclosures, big data, and the economics of privacy. We are currently seeking research submissions for our second PrivacyCon event, to be held January 12, 2017. We are especially interested in research on quantifying consumers’ privacy and security interests, attack trends and responses, transparency and control, and tools.

The author’s views are his or her own, and do not necessarily represent the views of the Commission or any Commissioner.

