# Summary of the Privacy Engineering Workshop at the National Institute of Standards and Technology

*April 9-10, 2014*

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) hosted a workshop on privacy engineering on April 9-10, 2014. The workshop focused on advancing privacy engineering as a basis for the development of technical standards, guidelines, and best practices for the protection of individuals' privacy and civil liberties. It was designed to explore the concepts of a privacy risk management model, privacy objectives, and privacy-enhancing system design and development.

Approximately 240 specialists in the legal, policy, and technical aspects of privacy participated in the workshop at NIST and another 100 attended via webcasts of plenary sessions. A varied array of companies, associations, civil societies, government agencies, and universities were represented among the attendees. The broad participation across sectors and disciplines illustrated both the complexity of the issue, and the demand for building consensus around common goals.

## Background

Under Executive Order 13636, Improving Critical Infrastructure Cybersecurity, NIST has produced the first version of a voluntary framework for reducing cybersecurity risk to critical infrastructure, which included a methodology for protecting individuals' privacy and civil liberties during the conduct of cybersecurity activities. Released in February 2014, the *Framework for Improving Critical Infrastructure Cybersecurity* was developed by collaborating extensively with critical infrastructure owners and operators, industry leaders, government partners, and other stakeholders. The accompanying *NIST Roadmap for Improving Critical Infrastructure Cybersecurity* identified the need for more privacy technical standards to support the privacy methodology.

Other initiatives in ITL, including the National Strategy for Trusted Identities in Cyberspace, Smart Grid and "big data" have also pointed to the need for outcome-driven privacy design and engineering practices.

While many sets of principles already exist that address the handling of individuals' personal information, including the foundational Fair Information Practice Principles (FIPPs), concerns persist about the future of privacy in the face of rapidly evolving technologies. Process-oriented principles are an important component of an overall privacy framework, but on their own they do not achieve consistent and measurable results in privacy protection. In the security field, risk management models, along with technical standards and best practices, are key components of improving security. Similarly, the safety risk management field also has well-developed models, technical standards and best practices. To date, the privacy field has lagged behind in the development of analogous components.

## Workshop Objectives

A key objective of the workshop was to explore the proposition that development of privacy framework components analogous to other engineering fields would enable the creation of reusable, standards-based tools and practices for developers. These tools and practices would facilitate the design and maintenance of systems and technologies with strong privacy postures. In particular, breakout sessions at the workshop focused on whether the development of privacy objectives that serve a similar purpose as the security objectives – confidentiality, integrity and availability – could provide the keystone for a privacy engineering framework.

## Key Outcomes

General themes that emerged from the workshop were:

*Communicating Across Disciplines*

- There is a material communication gap between organizations' policy teams and the system/technology developers and engineers.
- Privacy principles are difficult for engineers to implement; engineers require specific design requirements to implement privacy principles.
- There was support for the development of a NIST Interagency Report (NISTIR) on privacy engineering that would include common terminology and engineering framework components to help bridge the communication gap.
- Where possible, approaches in system design to protect privacy should be applicable internationally.

*Considerations for Privacy Engineering and Design*

- Reusable tools and practices that facilitate the creation and maintenance of systems with strong privacy postures would allow system owners and developers to address privacy risks in a measurable way within their overall risk management process.
- Some participants felt that overall risk management should be a fundamental driver of an organization's approach to privacy: solutions should be risk-based and affordable.
- There needs to be more development of tools for measuring the effectiveness of privacy practices.
- Managing individual consent is challenging, particularly in areas of data repurposing and data collection from devices or sensors in emerging technologies such as Big Data, the Internet of Things, wearable technologies, and image capture by unmanned aerial vehicles.
- Effective visual displays may help users better understand privacy considerations and options, and enhance their ability to make choices.
- Understanding the role of general privacy principles such as the FIPPs in privacy frameworks requires continuing work.
- Specific use cases can help the community gain a shared understanding of system design challenges, illustrate the impact on privacy in different contexts and identify potential privacy harms and mitigation strategies. These mitigation strategies may lead to common privacy objectives that can be used to guide the development of engineering practices.

## Next Steps

NIST's objective is to provide system owners, developers, and engineers with reusable, standards-based tools and privacy engineering practices that will help to evaluate the privacy posture of existing systems, enable the creation of new systems that mitigate the risk of privacy harm and address privacy risks in a measurable way within an organization's overall risk management process.

NIST will engage a broad community of stakeholders to facilitate this work. NIST will produce a report that identifies challenges in privacy engineering, and proposes a framework for understanding privacy risk and a methodology for designing privacy-enabled systems that would support outcome-driven privacy design and engineering practices. NIST will hold additional workshops and formal public comment periods to maximize input from a broad set of stakeholders.

As a next step, NIST will produce a document containing draft privacy objectives and underlying components for discussion at a second workshop. NIST will also consider use cases that can improve understanding of the issues. As the development of reusable tools and privacy engineering practices evolves, NIST may produce additional supporting materials.

Please send your email to privacyeng@nist.gov if you would like to receive notifications of upcoming workshops or other activities related to the NIST privacy engineering initiative.