NIST
National Institute of
Standards and Technology

National Strategy for Trusted Identities in Cyberspace (NSTIC) Privacy Workshop

June 27-28, 2011

Massachusetts Institute of Technology Media Lab
E14 Building, 6th Floor, 75 Amherst St, Cambridge, MA 02139

WORKSHOP OBJECTIVES

The purpose of the NSTIC Privacy Workshop is to offer opportunities to meet with stakeholders and to gather feedback on topics relating to privacy in the implementation of the NSTIC. The focus discussion at the workshop will be on the privacy-enhancing objectives of the Strategy, including overcoming the challenges of establishing user-centric privacy protections, and how to effectively implement them in the Identity Ecosystem Framework.

During the workshop, we will facilitate discussion and organize breakout meetings on topics related to the challenges of developing workable rules and guidelines for privacy protections as well as possible means of implementing these protections. These and other challenges that may arise in implementing privacy protections will be discussed at this workshop.

The Strategy’s first of four Guiding Principles calls for identity solutions to be privacy-enhancing and voluntary. As part of implementing the Strategy, the Identity Ecosystem Framework must offer individuals a better means of protecting their privacy by establishing clear rules and guidelines for the Identity Ecosystem, based on the Fair Information Practice Principles (FIPPs). The FIPPs are widely accepted as a solid framework for evaluating and mitigating privacy impacts. The Strategy begins the process of moving from the FIPPs to actionable and implementable privacy protections that could be part of the Identity Ecosystem Framework.

One objective of the workshop is for participants to discuss ways to continue translating these privacy protections into workable rules and guidelines specific to the Identity Ecosystem. The Strategy specifies a list of privacy protections that will be discussed at the workshop:

- Limit the collection and transmission of information to the minimum necessary to fulfill the transaction's purpose and related legal requirements;
- Limit the use of the individual's data that is collected and transmitted to specified purposes;
- Limit the retention of data to the time necessary for providing and administering the services to the individual end-user for which the data was collected, except as otherwise required by law;
- Provide concise, meaningful, timely, and easy-to-understand notice to end-users on how providers collect, use, disseminate, and maintain personal information;
- Minimize data aggregation and linkages across transactions;
- Provide appropriate mechanisms to allow individuals to access, correct, and delete personal information;
- Establish accuracy standards for data used in identity assurance solutions;
- Protect, transfer at the individual's request, and securely destroy information when terminating business operations or overall participation in the Identity Ecosystem;
- Be accountable for how information is actually used and provide mechanisms for compliance, audit, and verification; and
- Provide effective redress mechanisms for, and advocacy on behalf of, individuals who believe their data may have been misused.[1]

Additionally, developing clear policies will only be the first step to achieving enhanced privacy protections within the Identity Ecosystem. Participating service providers need to implement the policies in ways that provide a good user experience and enable individuals to realize meaningful benefit from those policies. Approaches may have an impact on system design architecture, user interfaces, and the development of specific, privacy-enhancing technologies. Privacy measures and policies need to be implemented as part of both the front-end and back-end processes of an organization. On the front-end, they should be clearly communicated, easy to understand, and easy for people to use. On the back-end, they should help provide accountability and measurable

[1] National Strategy for Trusted Identities in Cyberspace, p 30 (2011) at http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf

outcomes critical to assessing the success of the Identity Ecosystem as a whole, and as necessary features of the Identity Ecosystem Framework’s implementation.

The Strategy recognizes that privacy-enhancing technologies can play an important role in creating a user-centric identity model, but there may be hurdles to developing widespread use of such technologies. In addition to hurdles to adoption, the workshop will also consider additional challenges that may arise in designing or implementing privacy protections for the Identity Ecosystem and issues associated with implementing those privacy protections, such as increased operational complexity organizations must deal with in an environment of multiple international privacy frameworks and creating enforcement mechanisms for maintaining privacy protections.