wiley

NEWSLETTER

NIST Examining Privacy Engineering Best Practices

November 2014

The National Institute of Standards and Technology (NIST), a non-regulatory entity within the Department of Commerce, has been examining privacy engineering in parallel to its ongoing work on the Framework for Improving Critical Infrastructure Cybersecurity, which was released in February 2014. The Framework's accompanying Roadmap for Improving Critical Infrastructure Cybersecurity identified the need for more privacy technical standards to support the privacy methodology, giving rise to NIST's privacy engineering efforts.

NIST conducted its first Privacy Engineering Workshop April 9-10, 2014, which 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 held its second Workshop on September 15-16, 2014, which focused on gathering comments and feedback on the draft privacy engineering concepts contained in its Privacy Engineering Discussion Deck. These privacy engineering discussions will continue, and will likely result in written guidelines for privacy engineering best practices, similar in form to those set forth in the Cybersecurity Framework.

The private sector has expressed some concern about the effort, which some see as venturing into unsettled policy questions. For example, a broad coalition of private sector associations, including the United States Chamber of Commerce and the National Retail Federation, notes that NIST seems inclined to "define privacy harms" and select among "privacy engineering objectives." These groups believe that NIST can play a valuable role as a convener to catalog existing approaches, but "[t]he current initiative, however, sets out to define objectives as to which consensus does not yet exist, which is a

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

marked departure from NIST's usual practice."

Recent data security and privacy enforcement activities by the Federal Trade Commission and the Federal Communications Commission demonstrate the debate over whether existing guidance is adequate to put the private sector on notice of what is expected. A NIST privacy document or approach might be used to fill that void. Like the Cybersecurity Framework, NIST's privacy engineering process could eventually be used as a basis for regulation, standards or expectations by federal and state agencies and courts when assessing liability for privacy breaches. Industry should monitor the NIST privacy engineering process, to the extent the private sector wants to ensure it remains a purely voluntary, non-binding approach.