wiley

NIST's New Privacy Report: Taking a More Scientific Approach to Privacy
—

January 2017

On January 4, 2017, the National Institute of Standards and Technology (NIST) published <u>An Introduction to Privacy Engineering and Risk Management in Federal Systems</u> (Report). The Report introduces the concepts of systems engineering and risk management into privacy in an effort to develop more trustworthy federal systems. As the authors described in an accompanying <u>blog post</u>, the Report is one step in the process of moving privacy closer to science than art.

In taking a more scientific approach to privacy, as NIST has done in the security realm, the Report introduces a set of privacy engineering objectives to assist system engineers in implementing privacy policies and requirements. The objectives are **predictability** ("enabling reliable assumptions by individuals, owners, and operators about personal information and its processing by an information system"); **manageability** ("providing the capability for granular administration of personal information including alteration, deletion, and selective disclosure"); and **disassociability** ("enabling the processing of personal information or events without association to individuals or devices beyond the operational requirements of the system"). And, the privacy risk model introduced will allow agencies to conduct more consistent privacy risk assessments.

NIST attempted to create privacy processes that are repeatable and measurable.

Finally, the Report provides a general roadmap for NIST's privacy engineering and risk management guidance moving forward. As NIST has achieved thorough security guidance such as the *Risk Management Framework*, it plans to expand privacy guidance to

Authors
—

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Practice Areas
—

Privacy, Cyber & Data Governance

accomplish "privacy-positive outcomes" for federal systems.

As the title of the Report makes clear, this guidance is intended for federal agencies. However, as we have seen in the security arena, it is important for the private sector to be engaged and watchful in this process, as NIST's work is becoming increasingly influential, especially among regulators.