RE: “Developing a Privacy Framework”: Comments in Response to NIST Request
From: Janine Hiller, Professor, Virginia Tech

These broad comments are submitted individually, not on behalf of any other entity or person; they are based on a background of privacy law and policy work, and specific analysis of how the NIST Privacy Framework might be useful, yet in need of further development, for promoting implementation of privacy standards across multiple domains. More detailed research and analysis, and an evolution of thought about the NIST Privacy Framework, is found in the articles cited at the end of these comments.

Particular strengths of the proposed NIST Privacy Framework are that it begins to create a systematic way for organizations to implement protections for privacy, and that it places some responsibility on the system operator, through risk management, to protect privacy and avoid harms. It rightly recognizes that harms occur not only from the unauthorized use of information, but equally from the authorized use of information in an unexpected or contextually different way. An operational system of responsibility is important, rather than placing the onus only on the individual to take steps to monitor information use in complex systems to protect individual privacy. These strengths, however, can be the source of harms if not constructed and implemented with care. By focusing on organizational risk rather than risk to the individual, the Framework attenuates the essence of personal privacy, and it places a high level of trust in an organization to protect individual privacy when the interests of these parties may not always align. By creating a system of privacy risk management for system operators, the Framework must nevertheless include steps to avoid the potential to become a “check the box” exercise in which operators make decisions that, even unintentionally, are an ex post exercise resting on confirmation bias. Brief examples follow.

In the healthcare big data and predictive analytics area, it is virtually impossible for a patient to control and manage the use of their data, and yet when health information is not protected there are particular harms to the patient/doctor relationship and to the trust that is essential to gain positive health outcomes. The NIST Privacy Framework would require significant modification, a proactive approach to determining privacy needs and an increased focus on the patient rather than the organization, in order to be helpful in the healthcare arena.

Within the “smart city” context, in which large amounts of personal information are collected in order to protect citizens and efficiently manage necessary resources. The impact of the multiple uses of the information and the potential for combining the information across applications have broad and significant implications for citizen privacy. For the NIST Privacy Framework to effectively protect citizens it should be designed to emphasize the socio-technical nature of privacy protection rather than the more static engineering approach to privacy protection. This requires an emphasis on citizen engagement and an iterative process within the system itself.

The fundamental triad of predictability, manageability, and dissasociability within the Privacy Framework is different from the three-pronged confidentiality, integrity, and availability in the Cybersecurity Framework. The three cybersecurity principles were long recognized within the security and policy industry and already in use at many levels. The three privacy principles are entirely new, and therefore do not have a history of acceptance. Predictability is especially important as a fundamental concept, and yet its meaning is unclear, and risk management processes to achieve the result are not complete. It is important that privacy officers and privacy advocates be part of the systematic operational loop that will proactively recognize and analyze the ways that new and expansive uses of data can result in privacy harms and unacceptable privacy risk, so that the predictability principle will avoid the “death by a thousand cuts” that could incrementally defeat individual privacy.

Janine Hiller, "Healthy Predictions: Questions for Data Analytics in Health Care," 53 Am. Bus. L.J. 251 (2016). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2735137

Janine S. Hiller & Jordan M. Blanke, "Smart Cities, Big Data, and the Resilience of Privacy," 68 Hastings L.J. 309 (2017) http://www.hastingslawjournal.org/smart-cities-big-data-and-the-resilience-of-privacy/

Jordan Blanke & Janine Hiller, *Predictability for Privacy in Data Driven Government*, 20 Minn. J.L. Sci. & Tech. 32 (2018), available at: https://scholarship.law.umn.edu/mjlst/vol20/iss1/3