Submission to the National
Institute of Standards and Technology relating to Internal Report 8062
"Privacy Risk Management for Federal Information Systems"

Submitted via email to ***privacyeng@nist.gov***

July 30, 2015

I. Introduction

The undersigned associations appreciate this opportunity to provide comments to the National Institute of Standards and Technology (NIST) on draft Internal Report 8062—"Privacy Risk Management for Federal Information Systems" (the "draft NISTIR"). Our organizations, representing leading dynamic and innovative companies across numerous sectors, see great value in the collaborative work between NIST and industry. We have had the opportunity to engage with NIST and provide written input to NIST on a variety of initiatives. We write today to express some strong concerns about the direction of the draft NISTIR, in particular, the unintended consequences that could result from this initiative.

We appreciate NIST's recognition of the importance of privacy engineering and the use of technological approaches to minimize privacy risks and to implement a "privacy by design" approach. Many of our member companies incorporate privacy engineering as part of the processes they have implemented and continually refine as part of their information governance programs.

In the draft NISTIR, NIST puts forward a privacy risk management framework ("PRMF") with privacy engineering objectives and a privacy risk model. The draft NISTIR is intended to offer a methodology to federal agencies to enable them to identify and calculate privacy risks in their systems. As stated in the draft NISTIR multiple times, the methodology aims to provide a "repeatable and measurable method for addressing privacy risk in federal information systems."[1]

In this submission, we provide NIST with the following comments: (a) as written, the draft NISTIR extends beyond its intended scope of being limited to federal information systems and its potential applicability to the private sector is concerning; (b) the catalog of privacy problems set forth in the draft NISTIR includes subjective "problems" that result in premature policy-making on privacy; (c) the risk management methodology cannot produce repeatable and measurable results because it relies on subjective determinations; and (d) the draft NISTIR omits an integral component of privacy risk assessments, namely a discussion of the benefits of taking a certain data action.

A. Scope of the NISTIR

The draft NISTIR extends beyond its intended scope of being limited to federal information systems. While the draft NISTIR describes a privacy risk management framework for federal information systems, we note that references within the document appear aimed at the private sector. For example, within Appendix D (the Privacy Risk Assessment Methodology or "PRAM") there is a discussion of "business impact factors" which includes references to revenue loss and regulatory fines—factors that are associated with the private sector. As another example, Appendix F, which lists "problems for individuals" includes references to "differential pricing" and "redlining" – again, concepts associated with the private sector and not with government actors. Inclusion by NIST of these concepts suggests that the Privacy Risk Management Framework is intended to apply to the private sector. Such application would not be appropriate, and we urge NIST to refine the NISTIR, including the Appendices, to clarify that the scope is limited to Federal agencies. Even if these references were to be removed, however, considering the additional problematic issues we have identified below, we remain concerned that the methodology would be viewed by stakeholders (e.g., policymakers at the Federal, state or international level) as appropriate for applicability to the private sector.

B. Privacy "Problems"

The catalog of privacy problems contained in the draft NISTIR includes subjective "problems" effectively resulting in premature policy-level determinations by NIST with respect

[1] *See* draft NISTIR at 3.

to privacy. The six processes of the Privacy Risk Management Framework (PRMF) are characterized in the NISTIR as follows: (a) frame business objectives; (b) frame organizational privacy governance; (c) assess system design; (d) assess privacy risk; (e) design privacy controls; and (f) monitor change.

The "assess privacy risk" is further refined with the following explanatory equation: *Privacy Risk = Likelihood of a problematic data action X Impact of a problematic data action.* "Likelihood" is assessed as the probability that a data action will become problematic for a representative or typical individual—and to assess such "likelihood" users of the PRMF are directed to Appendix F, which provides a list of "problems" for individuals.

By attempting to define the "problems," to be used as part of the engineering methodology, NIST is effectively outlining policy objectives in the privacy realm. Policy discussions are currently underway in self-regulatory and governmental policy-making bodies, including Congress, state legislatures, the Federal Trade Commission and the National Telecommunications and Information Administration (NTIA). By populating the PRMF with privacy "problems," the NIST methodology is no longer an engineering tool, but rather, a vehicle for policy making.

C. Subjectivity of privacy problems and their likelihood will not result in repeatable and measurable results

While Appendix F includes a number of problems widely accepted as ones that can cause harm—such as economic loss, other "problems" listed are highly subjective and ill defined. For example, the "problems" characterized as "power imbalance" or "loss of trust" are ones that individuals would not experience uniformly. Indeed, policy makers are continuously examining privacy-related policy issues, and in the absence of underlying policy goals well-defined by a large and varied group of stakeholders, it is premature for NIST to provide the "problems" as inputs to the methodology. The subjective nature of these "problems" would not achieve an intended result of the methodology, which is to provide "repeatable" results. Only well-defined and non-subjective results relating to privacy impacting data actions would be appropriate for inclusion in a methodology designed to achieve repeatable results.

Additionally, by requiring users of the methodology to determine on a scale of 1-10 the "estimated expected rate of occurrence for each"[1] potential problem for individuals will insert an element of subjectivity even into those "problems" that could otherwise be viewed as objective.

[1] *See* draft NISTIR at 48.

D. Discussion of Benefits

Although an examination of the benefits of a data action is a critical component of conducting a privacy risk assessment, the draft NISTIR omits a discussion of such benefits. One of the fundamental operations of any risk management framework—whether it is related to privacy or another discipline—is assessing the possible risks in light of the benefits that can result from taking the data action. The PRMF does not include a discussion of benefits and the importance of measuring benefits against risk. Also, neither the equation noted above, nor the mathematical statement of the privacy risk model set forth in Appendix C of the NISTIR, contain any inputs relating to benefits.

> **"Yet accounting for *risks* is only part of a balanced value equation. Decision-makers must also assess, prioritize, and to the extent possible, quantify a project's *benefits* in order to understand whether assuming the risk is ethical, fair, legitimate and cost-effective.[1]"**

As noted above by the Future of Privacy Forum ("FPF"), it is critical to assess both benefits as well as risks in any value equation relating to privacy. We further note that an evaluation of costs and benefits of implementing privacy protections is an essential component of any privacy impact assessment (PIA).[2] Because the PRMF is intended to expand the utility of PIAs, a cost-benefit analysis component must be included in the methodology. It is unclear if NIST intends to address a benefits discussion at a later stage, however, considering that any assessment must include both risks and benefits at the same time (rather than individual assessments), we urge NIST to include an evaluation of costs and benefits as part of the value equation. While the "frame business objectives" prong of the PRMF calls for an agency to frame the "business objectives" of the system, these "objectives" would not sufficiently articulate benefits, and nor would they include how data actions might result in benefits beyond those that can be characterized as business "objectives."

* * *

The undersigned associations (see page 5) appreciate this opportunity to provide input to NIST on the draft NISTIR. We look forward to continuing to provide input to NIST and to continue engaging on these important issues.

[1] Jules Polonetsky, Omer Tene & Joe Jerome, *Benefit-Risk Analysis for Big Data Projects,* Future of Privacy Forum, September 2014 ("FPF paper"), available at http://www.futureofprivacy.org/wpcontent/uploads/FPF_DataBenefitAnalysis_FINAL.pdf at 1.

[2] FPF paper at 2.

Application Developers Alliance

Computer & Communications Industry Association

Computing Technology Industry Association (CompTIA)

CTIA-The Wireless Association

Electronic Transactions Association

Information Technology Industry Council

Internet Association

Internet Commerce Coalition

National Cable & Telecommunications Association

Retail Industry Leaders Association

Software & Information Industry Association

USTelecom Association