Before the
National Institute of Standards and Technology
Washington, DC

In re Draft Privacy Engineering Objectives and Risk Model	October 15, 2014

COMMENTS OF
COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION

Pursuant to the request for comments[1] issued by the National Institute of Standards and Technology (NIST) prior to the Second Privacy Engineering Workshop, the Computer & Communications Industry Association (CCIA) submits the following comments.

CCIA represents large, medium and small companies in the high technology products and services sectors, including computer hardware and software, electronic commerce, telecommunications and Internet products and services. CCIA members employ more than 600,000 workers and generate annual revenues in excess of $465 billion.[2]

I. Introduction

CCIA appreciates the opportunity to file in this proceeding, and commends NIST for turning its expertise to the field of privacy engineering. NIST's mission, which is "to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards,

[1] *2nd Privacy Engineering Workshop*, *available at* http://www.nist.gov/itl/csd/privacy-engineering-workshop-september-15-16-2014.cfm.
[2] A list of CCIA members is available at http://www.ccianet.org/members.

and technology . . . ," is well-suited to the development and improvement of privacy engineering processes and practices.[3]

However, CCIA is concerned that the privacy engineering initiative, as currently envisioned, does not appropriately leverage NIST's traditional core competencies, including measurement science, rigorous traceability, and the development and use of standards.[4] Significant components of the initiative make both implicit and explicit policy determinations, which are neither within NIST's remit as a technological standards development organization, nor objectively measurable components of a technical risk model.

II. The proposed privacy engineering risk model makes unwarranted policy prescriptions.

NIST's proposed privacy engineering risk model sets out three overarching privacy engineering objectives, lists selected problematic data actions, and enumerates privacy harms. Each of these significant components of the risk model results from determinations about privacy policy goals formulated in the absence of a well-defined direction developed by a wide range of interested stakeholders.

At the initiative's heart are the following privacy engineering objectives: predictability, manageability, and confidentiality.[5] They were developed by NIST with an eye for avoiding the "creepy" factor, controlling for surprises, and promoting individual control and self-determination.[6] These objectives are not derived from any public policy framework developed by relevant policy-making bodies and are not the result of evidence-based research.

[3] *Mission, Vision, Core Competencies, and Core Values*, NIST, http://www.nist.gov/public_affairs/mission.cfm.
[4] *Id.*
[5] NIST, NIST PRIVACY ENGINEERING OBJECTIVES AND RISK MODEL DISCUSSION DRAFT (2014), *available at* http://www.nist.gov/itl/csd/upload/nist_privacy_engr_objectives_risk_model_discussion_draft.pdf.
[6] *Id* at 2.

Flowing from these unusually derived objectives are a variety of problematic data actions, which in turn are said to result in a catalogue of privacy harms to individuals, as determined by NIST. The enumerated privacy harms, derived from the work of a sole academic, include concepts like "loss of autonomy," "loss of liberty," "stigmatization," "power imbalance," and "loss of trust."[7] These harms in particular are subjective and intangible—characteristics that are fundamentally impossible to measure or effectively mitigate with standardized technical processes. These are not appropriate or sufficient characteristics for a workable risk-mitigation engineering model, especially one promulgated by an organization meant to help define national technical standards.

III. NIST should use its technical expertise in developing a risk management framework for privacy engineering.

Rather than incorporating premature policy determinations into an abstract, subjective risk model, we urge NIST to turn its attention to aiding the growth of privacy engineering through activities that leverage its considerable technical expertise. NIST would be particularly well-positioned to assess prevailing methods of managing information and mitigating privacy risks in those industries operating under current legal privacy regimes. Making such assessments and spurring further technical development has been within NIST's traditional ambit, and would allow NIST to build on previous work in the privacy and security engineering spaces.

To that end, the privacy engineering initiative's intentional omission of established risk models and processes in the security engineering space is a missed opportunity. An effective means of modeling and mitigating privacy risks is to measure the effectiveness of the security of

[7] *See* NIST, PRIVACY ENGINEERING OBJECTIVES AND RISK MODEL - DISCUSSION DECK (2014), *available at* http://www.nist.gov/itl/csd/upload/nist_privacy_engr_objectives_risk_model_discussion_deck.pdf.

an information system.[8] NIST has already done considerable work in data security, as evidenced by its Framework for Improving Critical Infrastructure Security ("Cybersecurity Framework").[9] The Cybersecurity Framework builds upon NIST's extensive prior efforts to assess and implement—in a policy-neutral way—the security and privacy controls available for federal information systems and the private sector,[10] an approach that should also be a natural starting point for models of private sector privacy engineering.

NIST's work to catalogue and assess standards in other emerging technical areas, including identity verification and cloud computing, can also provide a roadmap for the privacy engineering initiative. In identity verification, NIST developed a methodology for assigning authentication strength requirements for Smart Cards,[11] while the NIST Cloud Computing Security Reference Architecture provides a methodology for evaluating cloud-based services using a risk-management framework approach.[12] Both of these methodologies play to NIST's strengths, as they assess existing tools and processes and then widen their utility through standardized frameworks.

[8] *See* NIST, SP 800-53 REVISION 4, SECURITY AND PRIVACY CONTROLS FOR FEDERAL INFORMATION SYSTEMS AND ORGANIZATIONS xi (2013), *available at* http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

[9] NIST, FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY (2014), *available at* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

[10] *Id* 21-22. *See also* NIST, SP 800-53 REVISION 4 at ix.

[11] Ramaswamy Chandramouli, NIST, NISTIR 7849, A METHODOLOGY FOR DEVELOPING AUTHENTICATION ASSURANCE LEVEL TAXONOMY FOR SMART CARD-BASED IDENTITY VERIFICATION (2014), *available at* http://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7849.pdf.

[12] NIST, SP 500-299, NIST CLOUD COMPUTING SECURITY REFERENCE ARCHITECTURE, *available at* http://collaborate.nist.gov/twiki-cloud-computing/pub/CloudComputing/CloudSecurity/NIST_Security_Reference_Architecture_2013.05.15_v1.0.pdf

IV. Conclusion

CCIA encourages NIST's continued study of privacy engineering. Given NIST's considerable expertise in measurement science and the development of technical standards, and the absence of a consensus public policy direction from relevant entities, NIST should ensure that its approach to privacy engineering catalogues existing work in privacy and security risk mitigation, in both private and public sector organizations, without implicitly or explicitly prescribing policy.

October 15, 2014

Respectfully submitted,

Bijan Madhani
Public Policy & Regulatory Counsel
Computer & Communications Industry Association
900 Seventeenth Street NW, 11th Floor
Washington, D.C. 20006
(202) 783-0070