October 15, 2014

Via privacyeng@nist.gov

Ms. Diane Honeycutt
Secretary
Computer Security Division
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

Dear Ms. Honeycutt:

The Internet Commerce Coalition (ICC) appreciates the opportunity to comment on the National Institute of Standards and Technology (NIST) draft Privacy Engineering Objectives and Risk Model, which were released for public comment on August 7, 2014. Our members include leading Internet service providers, e-commerce sites and technology trade associations.

Our Coalition has actively supported multi-stakeholder efforts to increase privacy protections in the United States. We share NIST's goal to examine and improve privacy engineering solutions. Indeed, many of our member companies either implement or contract for privacy engineering solutions as part of "privacy by design" or their internal information management programs. We urge NIST to reevaluate and adjust its initiative in order to move forward in a constructive manner.

The NIST Discussion Draft and Discussion Deck propose objectives and a risk model to "test" those objectives with an eye toward developing controls and metrics as part of a privacy engineering standard. However, there is no clear and broadly applicable statutory guidance or basis for developing standards to achieve particular policy outcomes. First, privacy policy objectives have not been defined for many sectors and data practices. Second, the privacy laws that cover specific regulated sectors and practices vary widely, and engineering practices based on those laws differ. Finally, there are very few, if any, current industry privacy engineering standards from which NIST can draw, unlike in the cybersecurity context. In all three regards, this project differs markedly from other NIST work, such as NIST Special Publication 800-53 ("Security and Privacy Controls for Federal Information Systems and Organizations"), which support the implementation of an existing law—the Federal Information Security Management Act of 2002 (FISMA).

The Framework for Improving Critical Infrastructure Cybersecurity (the "Cybersecurity Framework"), which took a year of intensive multi-stakeholder work to define, was able to build on a substantial body of consensus security standards. These do not exist the privacy context.

Similarly, the privacy harms outlined in the Discussion Deck released for comment are not based on any law; nor are they based on any underlying policy framework that has been endorsed by policymakers or used by the private sector. The asserted harms lack definition, and in many cases are highly theoretical. They also take no account of beneficial uses of data that may in some cases justify privacy risks. Because they fit plaintiff bar class action theories that have been largely rejected by the federal courts, inclusion of these harms in a NIST-IR would risk fueling another generation of frivolous class action lawsuits by giving them prominence in a federal policy statement.

The attenuated and theoretical harms in the Discussion Deck would be difficult for senior managers and engineers to understand. Furthermore, from an engineering perspective, designing to avoid this expansive and amorphous list of harms, while ignoring the beneficial uses of data, would be confusing and difficult to operationalize.

Finally, the objectives of Predictability and Manageability identified by NIST in the Discussion Deck are currently not established engineering goals, which would further detract from the utility of the NIST privacy engineering initiative.

Given the complexity of U.S privacy law and the fluidity of policy discussions currently underway in Congress and at the Federal Trade Commission, incorporating underlying policy decisions into a harms framework and choosing an engineering standard is not feasible. It is also further complicated by existing sectoral privacy laws that apply to certain industries and not others, as well as ongoing efforts by industry stakeholders under the auspices of the NTIA and in other *fora* to refine best practices and to invest in incorporating privacy and security controls in their products.

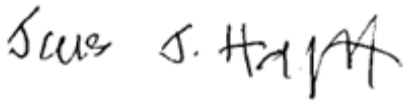
Until businesses and policymakers have determined whether there are further harms that privacy engineering standards should address, we believe it is inappropriate to develop a corresponding standard to harms not recognized in law. Once policies are in place that determine the proper balance between privacy concerns, innovation, and societal benefits, NIST may then have a role in facilitating standard-setting to help organizations implement those policy objectives. This effort would focus on practical operational steps that can be taken to safeguard privacy.

In the interim, we urge NIST to focus on cataloging in a policy-neutral way, existing, proven best-practices used to protect the privacy of individuals, drawing especially from industry sectors with existing legal paradigms. This would create a tool that is highly instructive for organizations seeking to improve privacy engineering and would make implementing privacy engineering solutions both cheaper and easier to implement. In following this path, NIST would

reorient the focus of its privacy engineering initiative from what *should be done* in privacy engineering to what *is being done* in the privacy engineering field by leading companies.

The ICC appreciates to the opportunity to comment on the NIST privacy engineering initiative.

Respectfully submitted,



Jim Halpert, General Counsel