

Before the  
**DEPARTMENT OF COMMERCE**  
**NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY**  
Gaithersburg, MD 20899

In the Matter of )  
 )  
Privacy Engineering Objectives and Risk Model; )  
Second Privacy Engineering Workshop )  
 )

**COMMENTS OF THE CONSUMER ELECTRONICS ASSOCIATION**

The Consumer Electronics Association (“CEA”)<sup>1</sup> respectfully submits these comments on the National Institute of Standards and Technology’s (“NIST”) efforts to develop its Privacy Engineering Objectives and Risk Model. CEA enthusiastically supports efforts to strengthen consumer trust and improve relationships between consumers and technology companies, and thus respects NIST’s initiative to develop resources to help system users, owners, developers, and designers analyze privacy risks.<sup>2</sup> As explained below, CEA urges NIST to first focus its efforts on collecting, cataloging, and making available a comprehensive survey of the diverse methods by which organizations currently manage privacy risks.

CEA member companies are at the forefront of advanced consumer technologies that increasingly rely on data to provide value to end-users.<sup>3</sup> As such, CEA member companies

---

<sup>1</sup> CEA is the principal U.S. trade association of the consumer electronics and information technologies industries. CEA’s more than 2,000 member companies lead the consumer electronics industry in the development, manufacturing and distribution of audio, video, mobile electronics, communications, information technology, multimedia, and accessory products, as well as related services, that are sold through consumer channels. Ranging from giant multi-national corporations to specialty niche companies, CEA members cumulatively generate more than \$208 billion in annual factory sales and employ tens of thousands of people in the United States.

<sup>2</sup> See *2nd Privacy Engineering Workshop*, NIST, <http://www.nist.gov/itl/csd/privacy-engineering-workshop-september-15-16-2014.cfm> (last visited Oct. 14, 2014).

<sup>3</sup> See, e.g., Comments of the Consumer Electronics Association before the Federal Trade Commission on the Privacy and Security Implications of the Internet of Things (filed June 10, 2013), [http://www.ftc.gov/sites/default/files/documents/public\\_comments/2013/07/00027-86193.pdf](http://www.ftc.gov/sites/default/files/documents/public_comments/2013/07/00027-86193.pdf); Comments of the Consumer Electronics Association before the Federal Trade Commission on Spring Privacy Series: Consumer

understand the critical importance of protecting users' privacy and have strong incentives to do so: Consumers will not readily use new technologies that do not protect the privacy of their personal information. Our members are committed to safeguarding their customers' data, and many have comprehensive programs in place to ensure compliance with applicable federal and state laws, as well as with self-regulatory guidelines governing the protection of personal information.

CEA member companies also understand the importance of standards-setting organizations such as NIST. CEA itself plays an integral role in growing the CE industry by developing essential industry standards; as a standards-setting body, CEA is a vital connection between companies, retailers and consumers.

With this background in mind, CEA urges NIST to begin any privacy activities by cataloging the ways in which organizations manage privacy risks. It could do so by using a comprehensive survey of current privacy risk models and organizational objectives.<sup>4</sup> This survey would reveal similarities in organizations' approaches to privacy risk management, advance stakeholders' understanding of risk mitigation solutions, help identify common practices, and lay the groundwork for further discussion, as needed.

The survey's results also could provide a roadmap and important resource for organizations with fewer resources or less sophistication with respect to privacy issues, and help them to find and adopt common practices and risk analysis models.

---

Generated and Controlled Health Data (filed June 9, 2014),  
[http://www.ftc.gov/system/files/documents/public\\_comments/2014/06/00012-90404.pdf](http://www.ftc.gov/system/files/documents/public_comments/2014/06/00012-90404.pdf).

<sup>4</sup> NIST can look to similar efforts by other organizations. For example, last year the Internet Architecture Board published an informational memo, "Privacy Considerations for Internet Protocols," that analyzes privacy risks as applied to Internet protocol development. Internet Architecture Board, *Privacy Considerations for Internet Protocols* (July 2013), <http://tools.ietf.org/pdf/rfc6973.pdf>. In addition, other federal and state government organizations are analyzing how to mitigate privacy risks. Cataloging these methodologies would allow NIST to avoid conducting duplicative, and potentially conflicting, work.

NIST action to develop privacy engineering objectives and risk models without first comparing existing privacy solutions would be problematic. Privacy is a complex issue that spans multiple disciplines and changes over time to conform to social norms. For example, certain fundamental Fair Information Practice Principles (“FIPPs”), which serve as the framework for all privacy laws, face questions about their continuing workability in the emerging era of big data and the Internet of Things. It would be premature to consider a new privacy framework in this proceeding before stakeholders, policymakers, and society at large have had an opportunity to explore further the application of the FIPPs to big data and the Internet of Things, among other challenging issues.

Finally, stakeholder discussion at the Second Privacy Engineering Workshop illustrated that there are threshold problems inherent in a unified model that would be applicable to all organizations. For example, certain definitions in a privacy risk model could conflict with sector-specific legal requirements. Additionally, attempting to quantify risks to allow for objective comparison across organizations does not reflect the complicated, multi-faceted, and context-specific nature of privacy.

\* \* \*

CEA appreciates this opportunity to comment and looks forward to continuing its work with NIST to increase consumer trust and improve relationships between consumers and technology companies.

Respectfully submitted,

**CONSUMER ELECTRONICS ASSOCIATION**

**/s/ Julie M. Kearney**

Julie M. Kearney  
Vice President, Regulatory Affairs  
Alexander B. Reynolds  
Senior Manager & Regulatory Counsel

1919 South Eads Street  
Arlington, VA 22202  
(703) 907-7644

October 15, 2014