Association for Computing Machinery (ACM)
US Public Policy Council of ACM (USACM)

1828 L Street NW, Suite 800
Washington, DC 20036
Main Phone: 212-626-0541
acmpo@acm.org

RESPONSE TO REQUEST FOR PUBLIC COMMENTS
Multistakeholder Process to Develop Consumer Data Privacy Codes of Conduct
77 FR 13098
DOCUMENT NUMBER 2012-5220
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION

RESPONSE FILED BY:
U.S. PUBLIC POLICY COUNCIL OF THE ASSOCIATION FOR COMPUTING MACHINERY

On behalf of the U.S. Public Policy Council (USACM) of the Association for Computing Machinery (ACM) we are submitting the following response to the Request for Public Comment on a Multistakeholder process to develop Consumer Data Privacy Codes of Conduct.

With over 100,000 members, the Association for Computing Machinery (ACM) is the world's oldest and largest educational and scientific computing society. The ACM U.S. Public Policy Council (USACM) serves as the focal point for ACM's interaction with U.S. government organizations, the computing community, and the U.S. public in all matters of U.S. public policy related to information technology. Our comments are informed by our collective experience in computing research and practice. Should you have any questions or need additional information, please contact Cameron Wilson, our Director of Public Policy, at 212-626-0541 or at cameron.wilson@acm.org

We strongly concur with the need for a transparent process for developing the enforceable codes of conduct that would help implement the Consumer Privacy Bill of Rights ("Bill of Rights"). Trust in how these codes are developed and enforced will go a long way to foster trust in the Bill of Rights and in consumers' ability to use the information infrastructure. As the Department of Commerce and the National Telecommunications and Information Administration understand, trust in the information infrastructure has benefits for the economy and other components of society that can accomplish more through using that infrastructure.

While these codes of conduct would be used domestically, the nature of online commerce and activity means that they will have impact beyond U.S. borders. It will be important to ensure that the multistakeholder process ("process") has the expertise and flexibility to account for this international dimension.

Issues to Address for Privacy

NTIA outlines issues in the Request for Comment it would like to address through a privacy multistakeholder process, and we agree that the issues listed (mobile apps, location-based services, cloud computing services, trusted identity, etc.) all deserve attention in that process. The process should emphasize not only Fair Information Practice Principles (FIPPs), but assessments of the privacy risks that pertain to each of these technologies and applications. In our comments on the Department of Commerce and Federal Trade Commission reports on privacy, we describe in additional detail how these goals could be accomplished, and we refer you to those comments.[1,2]

[1] http://usacm.acm.org/images/documents/Commerce_Department_Online_Privacy_Comments_USACM.pdf
[2] http://usacm.acm.org/images/documents/FTCprivacyResponseFinal.pdf

The Multistakeholder Process

Regardless of whoever participates directly in the process, other entities, as well as the general public, will need to have access to the activities and written output of the process. Such material should be made available online in digitally signed, open standard, machine-readable formats that allow for analysis and reuse of the data. This is good transparency practice, which can help generate trust in the process.

While transparency will significantly contribute to the perceived legitimacy of the outcomes of this effort, the whole effort must afford potential and actual participants practical due process. This is not an area where reliance on an exclusive group of experts, however outstanding, is likely to produce products that gain acceptance.

Specific questions to address:

2. Please comment on what factors should be considered in selecting issues for the privacy multistakeholder process.

As indicated above, we believe that all of the issues listed in the Request for Comment have merit. However, as a practical matter, for any given topic or issue, the broader the scope (i.e., the wider the impact), the more difficult it will likely be to produce consensus on a code of conduct. When identifying codes to develop through this process, there will typically be a tradeoff between potential impact and ease of development. For example, a code covering notices for mobile devices would be relatively narrow in impact but also relatively straightforward to develop. A code covering cloud computing would have wider impact but also be more difficult to develop. Achieving the appropriate balance between impact and ease of development may prove difficult when selecting areas for developing codes of conduct.

Therefore, we recommend that specific items for consideration in this process be focused on common functionality or risks. For instance, looking at cloud computing separately from mobile devices could fail to address specific challenges that appear in both contexts. Organizing the process around FIPPs or types of exposures consumers face (e.g., data breaches, third party use, identity theft) would also allow the process to cope more readily with rapid changes in technology.

4. Which stakeholders should participate? What kinds of expertise or perspectives should participants have?

Consistent with our role as a computing society, we want to stress that technical expertise and interests must be a part of the multistakeholder process. Moreover, such expertise should include individuals and organizations that can offer independent technical assessments and perspectives.

8. Which technologies could facilitate discussions among stakeholders before, during, and after in-person meetings?

This process presents a significant opportunity to utilize technologies to support rapid work and to reduce the burden of participation on all parties. We do not support designation of one technology or suite of technologies; there are numerous technologies that are readily available at low or no cost that may be employed. In fact, at a slighter higher cost in administration, multiple processes could be utilized to address participants' differing situations. However, a focus on technologies must not obscure the goal of providing processes that, overall, meet the basic due process requirements that other bodies have found build trust in

their products. We suggest consulting with the Internet Engineering Task force (IETF) and American National Standards Institute (ANSI) leadership for Information and Communications Technologies Standardization (ATIS, INCITS and TIA) for both technologies and procedures that work in similar contexts.

13. Are there lessons from existing consensus-based, multistakeholder processes in the realms of Internet policy or technical standard-setting that could be applied to the privacy multistakeholder process? If so, what are they? How do they apply?

Existing entities that might serve as good models for the process include the IETF (www.ietf.org), and bodies using consensus-focused procedures such as ANSI (www.ansi.org) or the International Organization for Standardization (ISO) (www.iso.ch). In general, such organizations make use of topical committees/working groups to perform initial development of artifacts prior to wider consideration. USACM adopts this kind of practice when developing policy documents like the comments we are submitting. Given the broad range of potential issues, the process might benefit from a similar structure, thereby enabling work on multiple issues to proceed in parallel.

Instead of several distinct processes, with this practice there would be one overarching process that considers the work of several application-specific processes. As many different technologies, functions, applications, and processes interact in the information infrastructure, it would be reasonable to have some way of considering the whole system before approving something that is specific to a particular application or service.