BILLING CODE 3510–60–P

DEPARTMENT OF COMMERCE

National Telecommunications and Information Administration

[Docket No. 120214135-2135-01]

RIN 0660-XA27

Multistakeholder Process to Develop Consumer Data Privacy Codes of Conduct

AGENCY: National Telecommunications and Information Administration, U.S. Department of Commerce.

ACTION: Request for Public Comments.

SUMMARY: The National Telecommunications and Information Administration (NTIA) is requesting comment on substantive consumer data privacy issues that warrant the development of legally enforceable codes of conduct, as well as procedures to foster the development of these codes. NTIA invites public comment on these issues from all stakeholders with an interest in consumer data privacy, including the commercial, academic and civil society sectors, and from federal and state enforcement agencies.

DATES: Comments are due on or before 5:00 p.m. Eastern Daylight Savings Time on **[insert 20 days after publication in the *Federal Register*]**.

ADDRESSES: Written comments may be submitted by e-mail to privacyrfc2012@ntia.doc.gov. Comments submitted by e-mail should be machine-searchable and should not be copy-protected. Written comments also may be submitted by mail to 1401 Constitution Avenue, NW, Room 4725, Washington, DC 20230. Responders should include the name of the person or organization filing the comment, as well as a page number, on each page of their submissions. All comments received are a part of the public record and will generally be posted to http://www.ntia.doc.gov/category/internet-policy-task-force without change. All personal identifying information (for example, name, address, etc.) voluntarily submitted by the commenter may be publicly accessible. Do not submit Confidential Business Information or otherwise sensitive or protected information. NTIA will accept anonymous comments (enter "N/A" in the required fields if you wish to remain anonymous).

FOR FURTHER INFORMATION CONTACT: Aaron Burstein, National Telecommunications and Information Administration, U.S. Department of Commerce, 1401 Constitution Avenue, NW, Room 4725, Washington, DC 20230; telephone (202) 482-1055; e-mail aburstein@ntia.doc.gov. Please direct media inquiries to NTIA's Office of Public Affairs, (202) 482-7002.

SUPPLEMENTARY INFORMATION:

Background

The Executive Office of the President released *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (the "Privacy and Innovation Blueprint") on February 23, 2012. Two central elements of the Privacy and Innovation Blueprint are: (1) a Consumer Privacy Bill of Rights, which is a set of

principles the Administration believes should govern the handling of personal data in commercial sectors that are not subject to existing Federal privacy statutes; and (2) a multistakeholder process, which NTIA will convene, to develop legally enforceable codes of conduct that specify how the Consumer Privacy Bill of Rights applies in specific business contexts.

These discussions will be open to participation by all interested stakeholders, transparent, and consensus-driven.[1] Open participation is necessary to ensure that codes of conduct reflect input from the broad array of stakeholders that have interests in putting the Consumer Privacy Bill of Rights into practice. Any person or organization may choose to participate, no one is under an obligation to participate once discussions have started, and NTIA anticipates that there will be opportunities to join a process once it is underway. Transparency is necessary to allow those who do not participate in the process to understand how participants reached their decisions. Consensus of a broad set of stakeholders, achieved through a transparent process, will lend legitimacy to the code of conduct. At the same time, consensus will encourage companies to adopt codes of conduct; the decision to adopt a code of conduct is voluntary, and companies are unlikely to adopt a code about which they have serious reservations.[2]

The privacy multistakeholder process is voluntary. A code of conduct will not be binding on a company unless and until that company affirmatively commits to follow it. NTIA expects that a company's public commitment to follow a code of conduct will be legally enforceable, provided

[1] Privacy and Innovation Blueprint at 2, *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf (proposing a privacy multistakeholder process that consists of "open, transparent forums in which stakeholders who share an interest in specific markets or business contexts will work toward consensus on appropriate, legally enforceable codes of conduct"); *id.* at 23-25, 37 (discussing importance of consensus in multistakeholder processes that develop Internet policy and standards).

[2] *See* Privacy and Innovation Blueprint at 23-24, 37 (discussing importance of consensus in multistakeholder processes).

the company is subject to the Federal Trade Commission's jurisdiction.[3] Enforceable codes of conduct based on the principles set forth in the Consumer Privacy Bill of Rights will provide consumers clear, understandable baseline protections and give businesses greater certainty about how agreed upon privacy principles apply to them. Companies will build consumer trust by engaging directly with consumers and other stakeholders during the process and adopting a code of conduct that stakeholders develop through this process.[4] Moreover, in any enforcement action based on conduct covered by a code, the FTC would likely consider a company's adherence to such a code favorably.[5]

NTIA's role in the privacy multistakeholder process will be to provide a forum for discussion and consensus-building among stakeholders. In situations in which stakeholders disagree over how best to interpret the Consumer Privacy Bill of Rights, NTIA's role, as explained in the Privacy and Innovation Blueprint, "will be to help the parties reach clarity on what their positions are and whether there are options for compromise toward consensus, rather than substituting its own judgment."[6] Furthermore, stakeholder groups convened to develop codes of conduct will not be advisory committees, as neither NTIA nor any other Federal agency or office will seek consensus advice or recommendations on policy issues from participants in these privacy multistakeholder processes.[7]

---

[3] Currently, the Federal Trade Commission (FTC) brings cases based on violations of a company's public commitments in its privacy statements under the FTC's authority to prevent deceptive acts or practices. *See* 15 U.S.C. § 45. A code of conduct developed through a multistakeholder process likely would be enforceable under this authority.

[4] Privacy and Innovation Blueprint at 24.

[5] *Id.*

[6] *Id.* at 27.

[7] *See id.* at 24 (stating that "the stakeholders themselves will control the process and its results" and "[t]here is no Federal regulation at the end of the process"). Because participants will not provide "advice or recommendations" as a group to the Federal Government, the multistakeholder processes discussed here should not be subject to the Federal Advisory Committee Act, 5. U.S.C. App. 2. *See id.* § 3(2) (defining "advisory committee" to include the

Request for Comment

Consumer Data Privacy Issues to Address Through Enforceable Codes of Conduct

NTIA plans to facilitate the development of enforceable codes of conduct that implement the full Consumer Privacy Bill of Rights. Initially, NTIA seeks to conduct a privacy multistakeholder process focused on a definable area where consumers and businesses will receive the greatest benefit in a reasonable timeframe. Areas of consumer data privacy in which stakeholders have begun to collaborate to develop practices, or to develop consensus around specific practices, could provide such a starting point. For example, commenters on the Department of Commerce's "Privacy and Innovation Green Paper"[8] were in broad agreement that transparency is a key element of protecting consumers' privacy. An initial privacy multistakeholder process could focus on the Privacy and Innovation Blueprint's call to give consumers "easily understandable and accessible information about privacy and security practices" in a particular business setting.[9] Future iterations of the process could build on this initial work toward a comprehensive, enforceable code of conduct for that setting.

To identify potential consumer data privacy topics that would benefit from a multistakeholder process as well as risks and concerns, NTIA seeks comment from stakeholders.

---

establishment or utilization of a group "in the interest of obtaining advice or recommendations for the President or one or more agencies or officers of the Federal Government," subject to certain exceptions).

[8] Department of Commerce, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework*, Dec. 16, 2010, http://www.ntia.doc.gov/reports/2010/IPTF_Privacy_GreenPaper_12162010.pdf.

[9] The full statement of the Transparency principle in the Consumer Privacy Bill of Rights is as follows:

> **Transparency: Consumers have a right to easily understandable and accessible information about privacy and security practices.** At times and in places that are most useful to enabling consumers to gain a meaningful understanding of privacy risks and the ability to exercise Individual Control, companies should provide clear descriptions of what personal data they collect, why they need the data, how they will use it, when they will delete the data or de-identify it from consumers, and whether and for what purposes they may share personal data with third parties.

Privacy and Innovation Blueprint at 14.

1. NTIA seeks comment on what issues should be addressed through the privacy multistakeholder process. Among a variety of alternatives, NTIA is considering convening an initial multistakeholder process to facilitate the implementation of the Transparency principle in the privacy notices for mobile device applications ("mobile apps"). Mobile apps are gaining in social and economic importance.[10] However, as several commenters on the Privacy and Innovation Green Paper noted, mobile devices pose distinct consumer data privacy issues, such as disclosing relevant information about personal data practices on a small display.[11] Moreover, practices surrounding the disclosure of consumer data privacy practices do not appear to have kept pace with these rapid developments in technology and business models. Recent studies found that 33 percent of the top 10 paid mobile apps for three major mobile phone operating systems (thus, a total of 30 paid apps were studied), and 66 percent of the top 10 free mobile apps for the same operating systems, have privacy policies,[12] while a broader study found that only 19 percent of free mobile apps have a link to a privacy policy.[13] With respect to apps directed at children, a recent FTC report found that parents generally cannot

[10] A recent report that summarizes current app economy data is Gartner, Inc., Gartner Says Worldwide Mobile Application Store Revenue Forecast to Surpass $15 Billion in 2011, Jan. 26, 2011, http://www.gartner.com/it/page.jsp?id=1529214;
Il-Horn Hann, Siva Viswanathan, and Byungwan Koh, The Facebook App Economy, Sept. 19, 2011, http://www.rhsmith.umd.edu/digits/pdfs_docs/research/2011/AppEconomyImpact091911.pdf (estimating that "employment impact of developers building apps on the Facebook Platform in the United States in 2011 is 182,744 full time jobs" and "the total employment value of Facebook's app economy is $12.19 billion").

[11] *See, e.g.*, Ann Cavoukian, Ph.D., Comment on the Privacy and Innovation Green Paper, at 5, Jan. 27, 2011; Center for Democracy & Technology Comment on the Privacy and Innovation Green Paper, at 10, Jan. 28, 2011; CTIA – The Wireless Association Comment on the Privacy and Innovation Green Paper, at 4, Jan. 28, 2011; TRUSTe Comment on the Privacy and Innovation Green Paper, at 8, Jan. 28, 2011.

[12] *See* Future of Privacy Forum, FPF Survey: Free Mobile Apps Better than Paid on Privacy Policies, Dec. 19, 2011, http://www.futureofprivacy.org/2011/12/19/fpf-survey-finds-free-mobile-apps-better-than-paid-on-privacy-policies/ (reporting on a study of paid apps conducted in May 2011 and a study of free apps conducted in December 2011).

[13] TRUSTe, More Consumers Say Privacy – Over Security – is Biggest Concern When Using Mobile Applications on Smartphones, Apr. 27, 2011 (reporting results of survey of top 340 free mobile apps conducted jointly with Harris Interactive), http://www.truste.com/blog/2011/04/27/survey-results-are-in-consumers-say-privacy-is-a-bigger-concern-than-security-on-smartphones/.

determine which app poses privacy risks to their children before downloading an app.[14] A common set of practices that implement the Transparency principle in the Consumer Privacy Bill of Rights could provide guidance to mobile apps developers, operating systems, and apps stores, as well as better inform consumers about how mobile apps use personal data. An NTIA-convened effort toward this end could build on initial efforts to develop codes of conduct and best practices for mobile apps and devices[15] and complement recent commitments by mobile device platform providers to promote transparency in the mobile arena.[16]

NTIA seeks comment on other potential topics, including:

- Other issues associated with mobile apps in general (*e.g.*, a code of conduct that implements the full Consumer Privacy Bill of Rights)
- Mobile apps that provide location-based services

[14] *See, e.g.,* FTC, *Mobile Apps for Kids: Current Privacy Disclosures are Dis*appo*inting* (staff report), at 17, *available at* http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf.

[15] *See, e.g.*, CTIA, Best Practices and Guidelines for Location Based Services, *available at* http://www.ctia.org/business_resources/wic/index.cfm/AID/11300 (last visited Jan. 18, 2012); Future of Privacy Forum and Center for Democracy & Technology, Best Practices for Mobile Applications Developers, *available at* http://www.futureofprivacy.org/wp-content/uploads/Apps-Best-Practices-v-beta.pdf (last visited Jan. 18, 2012); GSMA, Mobile and Privacy: Privacy Design Guidelines for Mobile Application Development, Feb. 2012, *available at* http://www.gsma.com/go/download/?file=gsmaprivacydesignguidelinesformobileapplicationdevelopmentv1.pdf; Mobile Marketing Association, Global Code of Conduct, July 15, 2008, *available at* http://mmaglobal.com/codeofconduct.pdf; PrivacyChoice, Mobile Policymaker, http://privacychoice.org/resources/policymaker (last visited Jan. 18, 2012). In addition, the Federal Trade Commission (FTC) has called for stakeholders to "identify the best means and place for conveying data practices in plain language and in easily accessible ways on the small screens of mobile devices." FTC, *Mobile Apps for Kids: Current Privacy Disclosures are Dis*appo*inting*, *supra* note 14, at 3. *See also* FTC, FTC Seeks Input to Revising its Guidance to Business About Disclosures in Online, May 26, 2011, *available at* http://www.ftc.gov/opa/2011/05/dotcom.shtm.

[16] *See* California Office of the Attorney General et al., Joint Statement of Principles, Feb. 22, 2012, http://ag.ca.gov/cms_attachments/press/pdfs/n2630_signed_agreement.pdf.

- Cloud computing services, *i.e.*, those that store data in architectures that provide on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service;[17] or specific cloud computing market segments
- Accountability mechanisms (to enable companies to demonstrate how they are implementing the Consumer Privacy Bill of Rights)
- Online services directed toward teenagers (individuals 13 or older and younger than 18)
- Online services directed toward children (individuals under 13 years old)[18]
- Trusted identity systems, such as those discussed in the *National Strategy for Trusted Identities in Cyberspace*[19]
- The use of multiple technologies, *e.g.*, browser cookies, local shared objects, and browser cache, to collect personal data

This list is not exhaustive, and NTIA welcomes comments on any of these topics as well as descriptions of other topics that commenters would like NTIA to consider for the privacy multistakeholder process.

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

Implementing the Multistakeholder Process

[17] *See* Peter Mell and Tim Gance, The NIST Definition of Cloud Computing, version 15, Oct. 7, 2009, http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc (characterizing cloud computing with these five characteristics).
[18] A privacy multistakeholder process could extend protections required of online services directed toward children under 13 years old under the Children's Online Privacy Protection Act of 1998 (COPPA), 15 U.S.C. §§ 6501-6506. The FTC's COPPA Rule can be found at 16 C.F.R. Part 312.
[19] Executive Office of the President, *National Strategy for Trusted Identities in Cyberspace: Enhancing Online Choice, Efficiency, Security, and Privacy*, Apr. 2011, http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf.

Commenters also may wish to provide their views on how stakeholder discussions of the proposed issue(s) should be structured to ensure openness, transparency, and consensus-building. Analogies to other Internet-related multistakeholder processes, whether they are concerned with policy or technical issues, could be especially valuable.[20] Possible subjects for comment include:

Open Participation

The Privacy and Innovation Blueprint calls for a code of conduct development process that is open to any interested participant. A broad array of perspectives and expertise will be necessary to ensure that the privacy multistakeholder process thoroughly addresses the issues before it. NTIA, as convener of the privacy multistakeholder process, will not set criteria that prospective participants must meet, such as their ability to represent specific industries or consumer interests. Nonetheless, there may be practical obstacles to such broad participation. For example, the time required to participate and the expense of attending in-person meetings may make it difficult for some stakeholders to participate. The following questions seek input on how NTIA can keep these barriers to a minimum and ensure that the privacy multistakeholder process is open, as a practical matter, to all interested stakeholders.

3. How can NTIA promote participation by a broad range of stakeholders, *i.e.*, from industry, civil society, academia, law enforcement agencies, and international partners?
4. Which stakeholders should participate? What kinds of expertise or perspectives should participants have?

[20] Potentially relevant examples mentioned in the Privacy and Innovation Blueprint include the Internet Corporation for Assigned Names and Numbers (ICANN), the Internet Engineering Task Force (IETF), and the World Wide Web Consortium (W3C). Privacy and Innovation Blueprint at 25. The Internet Governance Forum (IGF) is another potentially relevant multistakeholder forum for Internet policy development. *See* Internet Governance Forum, The Internet Governance Forum, http://www.intgovforum.org/cms/ (last visited Feb. 3, 2012). NTIA welcomes discussion of these and any other examples of multistakeholder policy development processes that commenters believe are relevant to developing privacy-related codes of conduct.

5. How can NTIA best ensure the process is inclusive, given that participants will likely have different levels of resources available to support their participation?
6. Are pre-requisites for participating in the privacy multistakeholder process consistent with the principle of openness? For example, what impact would a requirement to submit a brief position paper in advance of a stakeholder meeting have on participation?
7. What balance should NTIA seek to achieve between in-person and virtual meetings?

Transparency

Providing timely, relevant information in an accessible manner is crucial to effective transparency.[21] Transparency, in turn, will enable all stakeholders to understand how decisions within the privacy multistakeholder process are reached, whether they participate in the process or not.

8. Which technologies could facilitate discussions among stakeholders before, during, and after in-person meetings?
9. How should discussions during meetings be memorialized and published? Are verbatim transcripts or full recordings necessary, or would a more abbreviated record be appropriate?
10. How can NTIA facilitate broad public review of codes of conduct during their development?
11. What procedures should stakeholders follow to explain their decisions on issues discussed within the privacy multistakeholder process?

[21] *See* Memorandum for the Heads of Executive Departments and Agencies, Open Government Directive, Dec. 8, 2009, *available at* http://www.whitehouse.gov/open/documents/open-government-directive; Memorandum for the Heads of Executive Departments and Agencies, "Transparency and Open Government," Jan. 21, 2009, *available at* http://www.whitehouse.gov/the_press_office/TransparencyandOpenGovernment/.

12. What procedures should stakeholders follow to explain decisions they reach in concert with other stakeholders?

Building Consensus

Ideally, stakeholders who decide to help develop an enforceable code of conduct will do so with a "willingness to work in good faith toward reaching consensus on the code's provisions."[22] Consensus, however, does not have a single definition. The obstacles to consensus are also likely to vary, based in part on how consensus is defined. NTIA seeks comments on how other multistakeholder processes in the Internet policy and standards realms have defined and reached (or failed to reach) consensus.

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?
14. How did those groups define consensus? What factors were important in bringing such groups to consensus?
15. Are there multistakeholder efforts that have failed to achieve consensus? Why did these efforts fail to reach consensus? What policies or standards, if any, resulted from these efforts?
16. In what ways could NTIA encourage stakeholders to reach consensus? Under what circumstances should NTIA facilitate discussions among sub-groups of stakeholders to help them reach consensus? In these cases, what measures would be necessary to keep the overall process transparent?

[22] Privacy and Innovation Blueprint at 26.

Response to this Request for Public Comments is voluntary. Commenters are free to address any or all of the issues identified above, as well as provide information on other topics that they think are relevant to developing policies consistent with open, transparent, voluntary, consensus-based processes for developing consumer data privacy codes of conduct. Please note that the Government will not pay for response preparation or for the use of any information contained in the response.

Dated: _____.

_____

Lawrence E. Strickling,

Assistant Secretary for Communications and Information