April 2, 2012

Lawrence Strickling
Assistant Secretary of Commerce for Communications and Information
US Department of Commerce
National Telecommunications and Information Administration
1401 Constitution Avenue, Room 4725
Washington, DC 20230

Re: Multistakeholder Process To Develop Consumer Data Privacy Codes of Conduct

Dear Assistant Secretary of Commerce:

Mozilla submits the following comments in response to the March 5, 2012 call for public comments on a "Multistakeholder Process To Develop Consumer Data Privacy Codes of Conduct."

We applaud the Administration and the NTIA in seeking to establish open, transparent, multistakeholder processes for groups to develop consumer privacy codes of conduct.

The topics raised in the request for comments are pertinent to Mozilla on a number of levels. Our comments reflect contributions from both a number of engineers, developers and others at Mozilla who have worked to establish the Mozilla project as a multistakeholder process, of sorts, and also from people who have spent considerable time working with open standards groups. As with many of our efforts, we opened up the process within our community and asked for input from a broad range of participants, using a publicly available wiki page (see https://wiki.mozilla.org/Privacy/Policy/NTIA_RFC) to collect points of view and refine our messages.

Our comments are summarized as follows:

- Mozilla supports a process that is open and transparent while at the same time develops effective and meaningful codes of conduct. However, we don't think all areas of online privacy will be suitable for voluntary codes. We believe it will be vital for the Administration to use a well vetted and accepted criteria for determining its agenda.
- To foster consensus and transparency, the Administration should continue to promote openness and transparency at every stage of the process, including in technology, rapidly updating meeting minutes and decisions and lowering the barriers for interested stakeholders to participate.
- We encourage the Administration to commit to full openness: the most common reason for purportedly open/transparent processes to fail is that portions of the process end up being handled in a closed fashion and stakeholders lose trust in the process.

We are particularly appreciative of the process undertaken to engage the public throughout the past two years and through the Administration's ongoing efforts to solicit input from public and industry stakeholders before tackling various online privacy issues or launching into developing codes of conduct.

On behalf of Mozilla, we thank you for the opportunity to provide these comments. Please do not hesitate to contact us with any questions or for additional input.

Respectfully Submitted,

/s/

Alexander Fowler
Global Privacy and Public Policy Leader
Mozilla
650 Castro Street, Suite 300
Mountain View, CA 94041
(650) 903-0800, ext. 327

Mozilla's Comments to the NTIA on Developing Consumer Data Privacy Codes of Conduct via Multistakeholder Processes

I. Introduction

Mozilla is a global community of people working together since 1998 to build a better Internet. As a non-profit organization supporting an open source project, we are dedicated to promoting openness, innovation, and opportunity online.

Mozilla and its contributors make technologies for consumers and developers, including the Firefox web browser used by almost a half billion people worldwide. As a core principle, we believe that the Internet, as the most significant social and technological development of our time, is a precious public resource that must be improved and protected.

Openness, transparency, privacy and security are important considerations for Mozilla. They are embraced both in the process of creating products and services, as well as within the resulting products and services themselves. Mozilla's published Privacy Principles derive from a core belief that the user should have the ability to shape, maintain and control their web experience. We develop our products in the open and aim for transparency in every line of code and piece of content we produce. At the same time, we strive to ensure privacy and security innovations support consumers in their everyday activities whether they are sharing information, conducting commercial transactions, engaging in social activities, or browsing the web.

II. Issues suitable for multistakeholder processes and codes of conduct in privacy

One of the challenges in developing codes of conduct for online privacy is the pace of technological innovation and, in many cases, a lack of accountable institutions specialized in those areas of development. In the case of newly emerging technical capabilities and associated business practices, existing institutional and public stakeholders may not be well prepared, vested or focused to fully understand important nuances in how users are engaging with them, such that there aren't well defined partners to participate in developing and promulgating codes of conduct.

For instance, if we look at mobile apps, with privacy issues associated with notices, location, advertising and new types of personal data, it isn't clear today who the particular stakeholders would be to represent all the parties engaged in this vibrant and rapidly emerging area. Unlike the ongoing work by the advertising industry related to online behavioral advertising (OBA), where several influential trade associations represent the bulk of the industry, the corollary doesn't appear to exist for app developers.

Note the overall process related to OBA and privacy leaves a lot to be desired from an openness and transparency perspective. However, the trade associations have provided an important forum for their members to engage with other stakeholders on privacy.

For mobile apps, while there are major mobile trade associations like the GSMA, which brings together carriers and has a set of privacy principles, it's an open question as to whether it or any other group would have the convening power to mobilize the decentralized app industry to adhere to a code of conduct.

This led us to consider what conditions would need to be met for a particular privacy issue to be suitable for a multistakeholder process to generate a meaningful, voluntary and enforceable code of conduct. From our perspective, there appear to be five conditions necessary for determining if a code of conduct is suitable as a way to create a set of rules that can effectively protect consumer privacy, as opposed to other mechanisms like technology solutions or government regulation.

1. Trade associations and/or technical standards bodies have convening power to be accountable and represent the interests of leading companies and organizations in an emerging area of online privacy.
2. Consumer advocates and academics have sufficient technical and business understanding in the new online privacy concern.

3. User benefits to a technology, service or data type are demonstrable and users are motivated to use the technology or online service.
4. Heightened concerns for privacy and security represent a significant barrier for the industry to overcome.
5. There's a lack of existing regulation in the United States addressing that area.

Applying the above criteria and using the areas of interest outlined by the NTIA in its Federal Register notice, we came up with the following analysis:

Issue	Accountable Industry Groups	Engaged Public Interest Groups	Clear User Benefits	Heightened User Concerns	Unregulated in the U.S.
Mobile Apps	Low	Moderate	High	Low	Yes
Cloud Storage	Low	Low	High	Low	Yes
Identity Systems	Moderate	Moderate	High	Moderate	Yes
Online services for Kids 13 and Under	High	High	High	High	No (COPPA)
Online services for Teenagers	High	High	High	High	Yes
Collection of Personal Data via Multiple Technologies	Moderate	High	Moderate	Moderate	Yes

While we went back and forth internally over how to rate each dimension, and others will undoubtedly weigh things differently, we hope this analysis points out that codes of conduct are not going to be a one-size-fits all approach to online privacy. Nor will codes be easy to develop and promulgate without, in many cases, seeing changes across multiple stakeholders to gear up to tackle any one online privacy and security consideration.

From our analysis, we would end up ranking privacy considerations for online services directed at teenagers as an ideal area for a code, given the maturity and number of accountable industry and public interest groups already working on kids' privacy as a result of the Children's Online Privacy Protection Act. Likewise, looking to codes in the area of collecting personal data via multiple technologies (e.g., cookies, LSOs and cache) is another area where we see technology standards groups being well positioned and public interest groups having substantial experience working together with business and consumers to be a potentially good area for a code of conduct.

III. Mozilla supports a process that is open and transparent while at the same time develops effective and meaningful codes of conduct.

A. Open participation

To maintain an open, transparent process, first and foremost, it is critical to make available all relevant documents, drafts, ideas on process, guidelines, meeting plans, and meeting notes through the following suggested methods:

- Post information on an open, accessible web site, such as a wiki. See https://wiki.mozilla.org/ for example. This will promote transparency and participation.
- Hold open discussions on the web (e.g., webcast), via Internet Relay Chat (IRC) or by an open conference call for anyone to dial in to maximize inclusiveness. As additional options to holding meetings in person, these formats may enable those who lack resources to send delegates to in person meetings and still participate.
- Do not require prerequisites, such as position papers, to attend meetings. However, such optional papers can and should be submitted by posting them openly on the web, in an open format (preferably HTML) in a way people can easily view them on any web browser, and search engines can easily index.
- Communicate with stakeholders through an email list that is open for anyone to join.
- Foster broad community participation early and often.

B. Transparency

Technology

Mozilla believes that the technology used to promote the process can affect the transparency of the process as much as the procedural rules. Therefore, we would recommend that all documentation use open web standards like HTML

that can be implemented in multiple viewers and rendered in ways that are searchable and accessible at the lowest cost to stakeholders and the public.

Process

To facilitate a transparent process, we recommend that discussions during in-person meetings be documented in meeting minutes by voluntary minute-takers (as designated by the chair of the meeting). A technology that may be useful for this is Etherpad, where others in the meetings can also add to the minutes and make corrections as necessary in real-time.

Procedures stakeholders should follow to explain decisions

Stakeholders should publish their explanations of decisions on issues discussed on the web, preferably on an open wiki, and cite sources for their reasoning (using URLs). Stakeholders should also cite the minutes/notes of their meetings with other stakeholders to explain decisions they have reached in concert. There are several 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. We recommend a study of the W3C, IETF, WHATWG and microformats.org organizations. Many of the points those processes have come up with are summarized in this blog post by one of our contributors, Tantek Çelik. See http://tantek.com/2011/168/b1/practices-good-open-web-standards-development

C. Defining and incentivizing consensus

There are numerous factors in reaching consensus and they tend to differ based on the people involved and the issues at hand. For example, the W3C defines consensus roughly as a position which is either absent of objections, or has the least significant objections among several options. The NTIA can encourage consensus by requiring that all proposals be posted publicly and all discussions be posted publicly which will encourage stakeholders to think with a broader perspective than simply their own self-interests. Let sub-groups of stakeholders form organically rather than attempting to facilitate anything in particular. To keep the overall process transparent, make sure that all materials discussed are published openly on the web, and that meeting plans/attendees/minutes/notes are similarly published openly on the web.

D. Requirements for a multistakeholder process

Mozilla supports efforts to implement codes of conduct that would bring at least the level of technological and legal principles around privacy afforded to users of the web to the development of mobile apps. Therefore, the key requirements that a multistakeholder process will need to identify for privacy considerations to be addressed adequately are:

1. What are the privacy best practices that should influence the design of mobile apps and associated hosted services to provide user transparency and choice?
2. What are the legal or regulatory ramifications for failing to follow the codes of conduct?
3. How much will such codes of conduct continue to allow for innovation around novel uses of data that have user benefit?

IV. Current illustrative privacy practices

A. Privacy principles

Mozilla continues to implement a variety of consumer data privacy innovations in the creation of its products that we believe may help provide examples of potential areas for codes of conduct. We design our products with the following principles in mind (paraphrased from http://www.mozilla.org/en-US/privacy/):

- **No Surprises**
  Certain collection, use or disclosure of data sometimes unexpectedly suprises users. This means that, for unexpected collection, use and disclosure of data, we work hard to implement product-level notices and interactions that let users know and understand the data we collect and how we use it.

- **Real Choices, User Control and Sensible Settings**
  We give our users actionable and informed choices. We establish default settings that we try to align with user expectation as much as possible.
- **Limited Data**
  We collect and retain the least amount of information necessary for the feature or task.
- **Third Party Responsibilities**
  We make privacy a key factor in selecting and interacting with partners.

B. Three level privacy notifications

From a design perspective, we take into account a three-level approach to privacy notifications as we roll out and update our products:

1. In-product disclosures as the behavior of a feature or privacy notification
2. Settings that allow users to opt-in or opt-out of various collections, uses or disclosures of their data either separate from default or after they have made a privacy impacting choice
3. An understandable but sufficiently detailed Privacy Policy

C. Application privacy guidelines

Mozilla is in the process of launching an open HTML5 application marketplace (https://marketplace.mozilla.org). We are considering a range of privacy-related features including the following guidelines for application developers to improve the privacy of their applications:

- Design your app so that what you want to do with user data is what users think you are actually doing with it
- Give the user as much control over their data as you can
- Limit your data collection and use to only the data that you need
- Design your app to protect the security of your user's data in its collection, storage and use
- Respond to user questions and concerns about your privacy practices
- Avoid 'secret' updates
- Make your use of social or local features transparent and give (i) people a way to turn automatic sharing off and (ii) granular control over these features
- Obtain consent from users when necessary, especially for location and other sensitive information

D. Public resources from Mozilla on privacy and security

There are a number of examples of open, public-facing privacy and security work underway at Mozilla that may be of interest to the NTIA, including:

- Mozilla's Privacy Team Site (https://wiki.mozilla.org/Privacy)
- Privacy Reviews (https://wiki.mozilla.org/Privacy/Reviews)
- Security Reviews (https://wiki.mozilla.org/Security/Reviews)
- Data Safety at Mozilla (https://wiki.mozilla.org/Data_Safety)
- Privacy Roadmap (https://wiki.mozilla.org/Privacy/Features)
- Public Privacy Mailing List (https://lists.mozilla.org/listinfo/privacy)
- Mozilla Privacy & Data Safety Blog (http://blog.mozilla.com/privacy/)

V. Accountability

We believe that a clear accountability framework is necessary to help make a resulting code of conduct a meaningful exercise. Such an accountability framework should, at a minimum, involve:

- Clear, consistent rules around what constitute a violation of the code of conduct
- Balance user-centric innovation for uses of data with the need for more transparency and user control around their data

VI. Contact

Please direct questions and/or comments to:

Alex Fowler
Global Privacy and Public Policy Leader
Mozilla
650 Castro Street, Suite 300
Mountain View, CA 94041
(650) 903-0800, ext. 327