CTIA
The Wireless Association®

Expanding the Wireless Frontier

Michael F. Altschul
Senior Vice President &
General Counsel

Via email to: privacyrfc2012@ntia.doc.gov

April 2, 2012

National Telecommunications and
Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, N.W., Room 4725
Washington, D.C. 20230

Re: **Multistakeholder Process to Develop Consumer Data Privacy Codes of Conduct, Docket No. 120214135-2135-01**

I. Introduction

CTIA - The Wireless Association® ("CTIA")[1] submits these comments in response to the National Telecommunications and Information Administration's ("NTIA") February 29, 2012 request for public comment on its proposed multistakeholder process. As described in the *Notice,* the goal of this process is to develop voluntary, consensus-driven codes of conduct which specify how the White House's draft Consumer Privacy Bill of Rights applies in "specific business contexts" such as consumer data privacy.[2]

The wireless ecosystem provides robust contributions to the national economy, significant productivity gains, and is a highly competitive market. The wireless marketplace continues its remarkable growth at a stunning rate, adding 20 million wireless subscribers per year, and in the still evolving market for wireless broadband applications, revenues are expected to grow from $15 Billion in 2011 to $58 Billion by 2014.[3] The mobile industry is justifiably proud of its record of developing and voluntarily adopting industry best practices

[1] CTIA - The Wireless Association® is the international organization of the wireless communications industry for both wireless carriers and manufacturers. Membership in the organization covers Commercial Mobile Radio Service ("CMRS") providers and manufacturers, including cellular, Advanced Wireless Service, 700 MHz, broadband PCS, and ESMR, as well as providers and manufacturers of wireless data services and products.

[2] Notice, 77 Fed.Reg. 13098 (March 5, 2012) ("*Notice*").

[3] Data from market research firm, Gartner. Erick Schonfeld, *Gartner Forecasts Mobile App Store Revenues Will Hit $15 Billion in 2011*, TechCrunch (Jan. 26, 2011), http://techcrunch.com/2011/01/26/mobile-app-store-15-billion-2011/.

and guidelines for wireless applications, which include, among others, CTIA's Best Practices and Guidelines for Location-Based Services ("LBS"), which apply to all LBS providers (including application developers, equipment providers and wireless carriers) and implement the customer notice and consent structure utilized by the FTC in its Fair Information Practice Principles. During the development of the LBS Best Practices, CTIA reached out to privacy experts, telecommunications companies, non-profit privacy groups and government agencies, and examined many privacy agreements from various LBS providers. CTIA appreciates NTIA's proposed use of CTIA's LBS Best Practices and other wireless industry initiatives to develop a consensus for voluntary industry codes of conduct and best practices for mobile applications and devices, as well as recent commitments by mobile device platform providers to promote transparency in mobile applications.[4] As the White House's February 23, 2012 *Privacy and Innovation Blueprint* ("*Blueprint*") recognizes, the wireless industry's model of voluntary self-regulation and successful implementation of best practices and guidelines can best respond to the consumer privacy needs of a changing technological environment, and provides the best path for a successful multistakeholder process leading to consensus-driven, voluntary consumer data privacy codes of conduct for mobile industry applications and devices.

II. Stakeholders Should Reach Initial Agreement on the Threshold Parameters for the Multistakeholder Process, including: (A) the scope of consumer data to be protected; (B) the privacy principle(s) that should inform possible additional voluntary codes of conduct; and (C) the best framework for an authorized safe harbor

If voluntary sets of industry best practices and codes of conduct are to be achieved during the multistakeholder process, ideally there should be initial agreement among stakeholders on (1) the scope of consumer data that needs to be protected; (2) what consumer privacy principles should be codified in a Consumer Privacy Bill of Rights; and (3) how an authorized safe harbor should be structured.

A. The Scope of Consumer Data to Be Protected Needs to be Defined.

For example, according to the *Blueprint*, the Consumer Data Privacy Bill of Rights is intended to apply to "commercial uses of personal data", or "any data, including aggregations of data, which is linkable to a specific individual."[5] Such data would include identifier data linked to a personal computer or to a smartphone when it is used to build a profile of the user, but is intended to be flexible enough to "capture the many kinds of data about consumers that commercial entities collect, use, and disclose."[6] This personal data would be very similar to

[4] Notice at 13099 & nn.15-16.b.

[5] *Blueprint*, at 10.

[6] *Id.*

the Federal Government's definition of "personally identifiable information."[7] Whether all stakeholders agree that this is the appropriate level and scope of consumer data protection requiring protection – or if some other scope is more appropriate, should be determined at an early stage of the process at the working group level.

B. The Scope of Any Consumer Data Bill of Rights Legislation is Uncertain.

Second, while the *Blueprint* recognizes that the "consumer data privacy framework in the United States is, in fact, strong," given basic privacy values, existing statutory and common law, as well as Federal Trade Commission ("FTC") enforcement, the Obama Administration is calling upon Congress to enact legislation adopting basic privacy principles that would apply to businesses which are not presently subject to federal law.[8] The Administration's proposed Consumer Privacy Bill of Rights outlines the "basic principles" the Administration believes should be reflected in "comprehensive federal privacy legislation."[9] The White House's proposed legislation seeks to ensure that Internet users have a right to the following seven principles in connection with the commercial uses of their personal data: individual control; transparency; respect for context; security; access and accuracy; focused collection; and accountability.

While these principles appear laudatory, the risk is that the imposition of inflexible regulatory burdens – in contrast to voluntary industry guidelines that allow companies to implement best practices in a manner appropriate to each company's technology and the needs of consumers as they adopt rapidly evolving technologies – may stifle technological innovation and discourage the introduction of innovative products and services that consumers desire. It is unclear whether there is consensus among stakeholders, let alone Congress, about whether all seven principles should be the subject of new Consumer Privacy Bill of Rights legislation. For example, the final privacy framework contained in the FTC's Final Privacy Report of March 26, 2012 recommends that Congress "consider enacting targeted legislation to provide greater

---

[7] *Id.*, n. 12 (quoting Peter R. Orszag, Memorandum for the Heads of Executive Departments and Agencies, Guidance for Agency Use of Third-Party Website and Applications, at 8 (Appendix), June 25, 2010 ("The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk than an individual can be identified.")

[8] Existing federal privacy statutes, among others, include: The Gramm-Leach-Bliley Act; The Health Insurance Portability and Accountability Act; The Fair Credit Reporting Act; The Children's Online Privacy Protection Act; The Telephone Consumer Protection Act; and the Fair and Accurate Credit Transactions Act.

[9] Press Release, *Fact Sheet: Plan to Protect Privacy in the Internet Age by Adopting a Consumer Privacy Bill of Rights*, White House, Office of the Press Secretary, Feb. 23, 2012.

transparency for, and consumer control over, the practices of *information brokers*."[10] Though it is not entirely clear what provisions such FTC-recommended legislation would include, it apparently would not address all seven principles of the proposed Consumer Privacy Bill of Rights.

Given this background, it is not surprising that even White House Officials recognize that serious political challenges exist to accomplishing privacy legislation.[11] In his March 29, 2012 congressional testimony, NTIA Administrator Strickling emphasizes that Consumer Privacy Bill of Rights legislation is necessary for new codes of conduct implementing those rights to be effective.[12] And substantively, apart from the legislative environment, while the NTIA Notice found generally "broad agreement" among commenters that "transparency" is a key element to protecting consumers' privacy,[13] no similar broad consensus has been announced among commenters as to any of the other seven principles on the proposed Consumer Privacy Bill of Rights. Accordingly, CTIA agrees with NTIA that it is appropriate to prioritize a narrower "definable area where consumers and businesses will receive the greatest benefit in a reasonable timeframe."[14] CTIA supports this incremental approach as being a reasonably achievable goal to the multistakeholder process, particularly where the process builds upon

---

[10] FTC Report, *Protecting Consumer Privacy in an Era of Rapid Change - Recommendations for Businesses and Policymakers* (March 2012) at iv. (Emphasis added)("FTC Final Report").

[11] Communications Daily, "Administration Urges Congress to Pass Data Privacy Laws" (March 16, 2012) (quoting Danny Weitzner, Policy Director of the White House Office of Science and Technology Policy as stating on March 15, 2012: "It is no secret to anyone that the political challenges of achieving privacy legislation are substantial...but it is our intention not to wait to implement these principles.")

[12] As Administrator Strickling testified, "[u]nder the Administration's recommended framework, companies would face a choice: Follow the general principles of the statutory Consumer Privacy Bill of Rights, or commit to following a code of conduct that spells out how those rights apply to their businesses. If this code of conduct sufficiently implements the Consumer Privacy Bill of Rights in the context in which a company (or group of companies) plans to use it, the FTC should forbear from enforcing the Consumer Privacy Bill of Rights against it, so long as the company lives up to its commitment. The latter course would provide greater certainty for companies and stronger incentives for all stakeholders to work toward consensus on codes of conduct, *but it requires Congress to act.*" Testimony of Lawrence E. Strickling, Assistant Secretary for Communications and Information, National Telecommunications and Information Administration, U.S. Department of Commerce; Hearing on "Privacy and Innovation: Does the President's Proposal Tip the Scale?"; Subcommittee on Commerce, Manufacturing and Trade, Committee on Energy and Commerce, United States House of Representatives (March 29, 2012), located at: http://www.ntia.doc.gov/speechtestimony/2012/testimony-assistant-secretary-strickling-privacy-and-innovation-does-president- ("Strickling Testimony")(emphasis added).

[13] Notice at 13099.

[14] *Id.*

existing industry best practices that have been developed by stakeholders such as CTIA, the Mobile Marketing Association, and Mobile Platform Providers. For those principles in the *Blueprint* for which voluntary consensus in a multistakeholder process may be more challenging, it may be a more efficient use of multistakeholder resources to defer work on those principles until they are codified in federal privacy legislation.

Finally, stakeholders in this process need to be prepared to confront consumer data privacy issues as they arise from new advances in technology or business models (whether mobile operating system platforms, HTML-5 or cloud computing). The multistakeholder process should develop these issues further. To be successful in establishing any voluntary new codes of conduct, the proposed multistakeholder process must consider an approach that (i) gives companies reasonable flexibility to implement guidelines; (ii) is technology-neutral, and neutral to various platforms and business models; (iii) fosters technological innovation that benefits consumers and the economy; (iv) recognizes the complex mobile ecosystem; and (v) minimizes unproductive burdens on businesses and consumers. Within such a framework, the mobile wireless industry can significantly contribute to the development of additional guidelines and codes of conduct within the multistakeholder process. The wireless industry has already undertaken voluntary best practices and guidelines, such as its Location-Based Guidelines, which can serve as a model for other technologies and business models. Among possible initiatives would be to develop additional, voluntary sets of best practices to supplement those industry best practices and guidelines that already exist. And establishment of an enforcement safe harbor for these practices or guidelines would encourage broad industry adoption of any new voluntary guidelines and best practices.

C. If a Company Agrees to Comply with Any Voluntary Code of Conduct and Guidelines, It Must Be Granted a Safe Harbor from any Enforcement.

Companies that voluntarily commit to self-governance programs should be rewarded with a safe harbor from enforcement proceedings for their compliance. This incentive will encourage broader participation by providing legal certainty to any company that voluntarily agrees to follow an approved code of conduct. Industry should take responsibility initially for enforcing its own codes of conduct. But to make these voluntary codes of conduct legally enforceable, as called for by the *Privacy and Innovation Blueprint* ("*Blueprint*"), the Federal Trade Commission (FTC) should have primary governmental authority to enforce any violations of public commitments by a company under the FTC's Section 5 authority.[15] A safe harbor regime will ensure consistency and encourage stakeholders to participate in the codes of conduct. Also, as the *Blueprint* recommends, because national uniformity is "crucial" to preserving the incentives for participation in the multistakeholder process,[16] Congress should preempt any State laws that may be inconsistent with any Consumer Privacy Bill of Rights that

[15] State Attorneys General, in coordination with the FTC, may also have authority under state consumer protection laws of general applicability.

[16] *Blueprint* at 37.

Congress may enact.[17] The FTC has considerable experience investigating and prosecuting deceptive practices, including violations of public commitments to a privacy policy or code of conduct, and it also has extensive experience with the operation of a safe harbor.

III. Stakeholders Should Draw from Existing Mobile Industry Codes of Conduct as a Starting Point for Any New Voluntary Codes of Conduct.

The wireless industry has responded to rapidly evolving technology in the mobile ecosystem by developing and voluntarily adhering to guidelines based on the broadly accepted Fair Information Practice Principles ("FIPPs"). These voluntary industry guidelines, which include CTIA's Best Practices and Guidelines for Location Based Services, CTIA's Consumer Code for Wireless Service ("CTIA Consumer Code"), and efforts by other mobile industry associations such as the Mobile Marketing Association Mobile Privacy Guidelines,[18] have promoted sound privacy practices within the wireless industry while also ensuring that a competitive landscape can thrive.

Successful examples of voluntary wireless industry self-regulatory codes of conduct include the following:

- **CTIA Consumer Code for Wireless Service**
  CTIA's Consumer Code, http://files.ctia.org/pdf/The_Code.pdf, ("Consumer Code") was first established in 2003. It has evolved over the years, and now includes 11 requirements. The Consumer Code includes a provision for each signatory carrier to abide by a specific set of practices for the protection of customer privacy, including complying with applicable federal and state law, and making available to the public its privacy policy regarding information collected online. Finally, each signatory carrier must comply with the CTIA Best Practices and Guidelines for Location-Based Services. The FCC has recognized the Consumer Code by incorporating compliance with its requirements as a predicate for wireless carriers seeking designation as FCC-designated Eligible Telecommunications Carriers under the Universal Service Fund.
- **CTIA's Best Practices and Guidelines for Location-Based Services**
  The CTIA Best Practices for location-based services ("LBS"), were first released four years ago (http://files.ctia.org/pdf/CTIA_LBS_Best_Practices_Adopted_03_10.pdf). The guidelines are applicable to all LBS providers (application developers, equipment providers, as well as wireless carriers), are technology-neutral, implement the notice and consent structure utilized by the FTC in its Fair Information Practice Principles, and include other safeguards. Examples of LBS provider privacy policies that demonstrate these Best Practices are posted on the CTIA website. CTIA's development process included reaching out to privacy experts

[17] *Id.*

[18] Mobile Marketing Association's Global Code of Conduct for Mobile Marketing (July 15, 2008), http://mmaglobal.com/codeofconduct.pdf.

from over 90 entities, including telecommunications companies, non-profit privacy groups, and government agencies, and examined many privacy agreements from various LBS companies.

- **Self-Regulatory Principles for Online Behavioral Advertising**
  A broad segment of the Internet advertising industry has actively implemented a Self-Regulatory Program building upon a comprehensive set self-regulatory principles developed in 2009 by the Digital Advertising Alliance. *See*, http://www.aboutads.info/.
- **CTIA's Wireless Internet Guidelines for Carrier Content Classification**
  CTIA's Content Classification Guidelines provide that signatory wireless carriers will, among other things, commit to develop voluntary content classification standards for "Generally Accessible Carrier Content" and "Restricted Carrier Content", the latter which is accessible only to consumers 18 years or older, and is accessible only after access controls have been deployed, and content rating standards are defined.
  See, http://files.ctia.org/pdf/CTIA_Content_Classification_Guidelines.pdf.
- **App Content Classification and Ratings**
  Developed by CTIA and the ESRB, and announced in November, 2011, these guidelines extend the 2010 Wireless Internet Guidelines to create a mobile application rating system that is developer-friendly, but provides parents and consumers the information they require.
  See, http://www.ctia.org/consumer_info/service/index.cfm/AID/12076.
- **Joint Statement of Principles by Mobile Device Platform Providers**
  In February, 2012, mobile device platform providers announced their commitment to promote transparency for mobile applications by facilitating the ability of application providers to make application privacy policies available to consumers for review in mobile marketplaces before downloading the application, and to establish a means for consumers to report apps that are not abiding by privacy standards under applicable law. These commitments can also serve as a baseline starting point for consensus-building in the multistakeholder process. See Joint Statement of Principles,
  http://ag.ca.gov/cms_attachments/press/pdfs/n2630_signed_agreement.pdf.

While these voluntary mobile industry guidelines may serve as an excellent baseline starting point, as the NTIA Notice itself recognizes, mobile applications on mobile devices present distinct consumer data privacy issues, not the least of which is disclosure of relevant information about individual data practices on a small display screen.[19] To this end, the FTC announced recently that it is sponsoring a workshop on May 30, 2012 that will address how "mobile privacy disclosures...can be short, effective, and accessible to consumers on small screens." The FTC "hopes that the workshop will spur further industry self-regulation in this area."[20] The results of this workshop will undoubtedly be considered in the multistakeholder process.

---

[19] Notice at 13099.

[20] FTC Final Report at v.

In order to begin building consensus, stakeholders in Working Groups might begin as a starting point with the February 2011 Joint Statement of Principles by mobile platform providers, and the various CTIA voluntary guidelines and best practices for privacy, such as for location-based services. Also, the results of the recently announced FTC workshop focused on accessible mobile privacy disclosures to consumers using small screens may yield some ideas that could form the basis for agreement to voluntary guidelines or codes of conduct.

Today's mobile operating platforms have introduced thousands of new third party application developers to consumers, making application providers a key element of the mobile ecosystem. However, if application providers do not undertake their responsibilities for data collection, use and sharing, consumers may not benefit from the proposed codes of conduct. Given today's "open" platforms, wireless carriers and mobile platform providers are not expected to, nor can they, guarantee or assume responsibility for the good conduct of every application provider.

Second, in addition to the importance of including mobile applications providers and all elements of the wireless ecosystem in the stakeholder process, it will be just as important to "future proof" wireless industry best practices and guidelines. What may be appropriate self-regulatory practices for the wireless smartphone industry of today may be less relevant in the future depending upon the industry segment, technology model, and business plan of all technology companies handling consumer data. For example, the universe of mobile devices having Internet connectivity is rapidly expanding to include notebook computers, tablets and e-readers using multiple operating systems, web browsers, and both licensed and unlicensed spectrum. And today's technology of the mobile applications stores will likely yield to new technologies tomorrow: rather than downloaded "native" software apps on the handset, with HTML5 and cloud computing, the data access capabilities of mobile apps will focus on the Internet browser and data will be in the cloud rather than residing in the mobile device. Finally, machine-to-machine communication technologies are rapidly developing, some of which have no user interface at all, presenting very different technical issues when considering possible new consumer rights of individual control, transparency, and access, among others.

This rapidly evolving ecosystem makes it all the more vital that the wireless industry model of self-regulation be followed, with good faith participation by all stakeholders seeking to adapt privacy best practices to fit emerging technology. It is also of paramount importance that the participating stakeholders balance (1) reasonable consumer privacy expectations with (2) consumer demand for ease of use and ready access to rapidly evolving and innovative technology. The danger is that inflexible and overly prescriptive regulatory frameworks could frustrate the deployment of new technology and services to consumers. CTIA encourages NTIA and the FTC to seek to "future proof" their principles by adopting guidelines that are fully informed by new and emerging business models and their technological capabilities and limitations.

IV. Working Groups Should Be Inclusive, Transparent, and Efficient

CTIA agrees that the code of conduct development process should be (1) open to any interested participant (including industry, consumer groups, academia, law enforcement agencies, and international partners); (2) that the proceedings should be transparent once codes of conduct are developed; and (3) that participating stakeholders must be willing to work together in good faith to develop enforceable codes of conduct.

A. The NTIA-Convened Multistakeholder Process Is Not a Rulemaking

As NTIA recognizes, its "role in the privacy multistakeholder process will be to provide a forum for discussion and consensus-building among stakeholders."[21] If different stakeholder interests should disagree, NTIA's role will be to act as an honest broker, to assist parties in clarifying what their positions are and whether options for a compromise consensus exist, "rather than substituting its own judgment."[22] But since this will not be a rulemaking proceeding in which NTIA has been authorized by Congress to adopt rules or regulations, or to decide among competing stakeholder interests, NTIA has no delegated administrative authority to adopt new consumer data privacy rules.

B. Structuring Multistakeholder Discussions

NTIA has indicated that promptly after receiving comments from interested stakeholders, it will convene an initial meeting to adopt procedures for the multistakeholder process.[23] CTIA believes that consensus-building would most effectively occur by the formation of working groups or subgroups within a larger, highly inclusive multistakeholder process. This multistakeholder process could be subdivided and organized along the lines of industry, consumer groups, law enforcement agencies (*e.g.*, FTC, DOJ, State AGs), academia, and international partners. While broad participation should be encouraged, there should be some limited organizational activity to ensure that each working group consists of relevant industry participants.[24] Each working group would meet on a regular basis (as frequently as each working group's attendees agree, depending on the requirements of the particular topic) to be convened with the possible assistance of NTIA. Initially, each working group would meet to discuss threshold parameters for a code of conduct or guidelines, such as the scope of consumer data at

---

[21] Notice at 1.

[22] *Blueprint* at 27.

[23] Following the comment period closing on Monday, April 2, 2011, NTIA states it "will move promptly to select a substantive issue and convene an initial public meeting to begin developing a code of conduct. Part of the business of this initial meeting will be for stakeholders to reach agreement on the procedures they will use to work together." Strickling Testimony (March 29, 2012).

[24] For example, there should be some minimum foundational definitions established at the outset as to what qualifies as a "mobile application" or a "mobile device" so that there are reasonable limitations on, for example, those business entities eligible to participate in a mobile application industry working group. That will encourage an efficient and more productive working group process.

issue (see Section II. above) in order to develop a consensus on various provisions of a new code or codes of conduct. For the initial meetings of each working group, a sign-in sheet and a contact list of attendees should be created. Once a proposed code of conduct is prepared, it could be exchanged among the other working groups for comment. Thereafter, once a majority of participants are satisfied with a proposed draft code of conduct and are prepared to share it for broader review, NTIA could publish the draft for public review and seek comment on the proposed "consensus" of the code's provisions. At a later stage of the process, designated representatives of different working groups could meet to discuss and attempt to resolve any differences between the working groups on the consensus codes of conduct.

Effectively run working groups, with agendas, and participants willing to lead the discussion, with possible NTIA participation to help convene the meetings, will be important factors that can help to ensure a successful multistakeholder process.[25] NTIA may also benefit

---

[25] Certain common principles and features embodied in technical standard setting organization decision-making could apply to the multi-stakeholder processes envisioned by NTIA. For example, ANSI and many U.S.-based developers of voluntary consensus standards have used the terms "openness" to characterize a process that has certain important features. These same features are central to the policies of well-recognized regional and international standards bodies such as the International Telecommunication Union (ITU), International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), European Telecommunications Standards Institute (ETSI) and the WC3 Consortium.

These features are also endorsed in Annex 4 of the Second Triennial Review of the WTO/TBT Agreement. They include:

1. Transparency:

    - Essential information regarding activities is accessible to all interested parties;

    - Before any discussion on the substance of any code of conduct, NTIA shall hold an issue identification workshop specifically focused on process so that all stakeholders are able to further discuss their views regarding scope, timelines, and procedures for development of a code of conduct.

2. Inclusivity:

    - A Notice of Workshop should be issued by each working group inviting all like stakeholders (i.e. industry; government; consumer groups; academia, etc.);

    - Stakeholders will be given the opportunity to volunteer for a work group or groups --to the appropriate work group for which a stakeholder belongs-- that will work on the issues identified at the initial workshop;

    - WG email distribution lists should be set up to facilitate collaborative discussion of all interested parties outside of formal "meetings/calls".

3. Transparency:

- WG meetings (or calls) should be open to all interested parties qualifying for a respective WG;
- Meetings/calls should be announced at least 10 business days in advance;
- Meeting agendas, working papers, etc...should be posted online at least 5 business days before consideration;
- NTIA can serve as a "secretary," and if and when authorized by a 2/3 majority of members of a particular WG, can share meeting minutes to be posted online no later than 5 business days after the WG meets;
- Chatham House Rule should apply to WG meetings/calls. As such, once meeting minutes are authorized by a 2/3 majority to be taken by each WG, the minutes would only refer to "Industry Rep X" and "Consumer Rep Y" to ensure open dialogue. However, formal presentations for consideration must be attributed to those proposing.

4. Consensus:

- NTIA would act as the convener and facilitator, not the chair that determines the outcome;
- Consensus should be reflected in a group or "consensus body" that includes representatives from materially affected and interested parties;
- Consensus is only achieved once a very large majority (i.e. 75%) of those who are materially affected and who will be subject to the voluntary code of conduct agree;
- Objections must be debated until a majority of participating WG members are satisfied that the objections are wrong.

5. Impartiality:

- No one interest dominates the process or is favored over another;
- There should be broad-based public review and comment on any draft codes of conduct;
- Relatively short, self-imposed deadlines are necessary;
- Each working group needs to have a clear mission statement and purpose;
- Participants should provide a modest "statement of interest" prior to participating in a working group.

from the experience of other multistakeholder processes, such as its recent ICANN generic TLD multistakeholder process, to encourage broad participation in this consumer privacy multistakeholder process.[26]

Ultimately, because industry members will need to voluntarily commit to comply with an enforceable code of conduct, and it will be industry members who will be held accountable for any failure to comply with voluntary codes of conduct, industry must be able to reach consensus as a group (or combination of sub-groups) as to what codes of conduct it can reasonably accept. A safe harbor protection will be an indispensible element to incentivize a broad array of industry members to develop and commit to an enforceable privacy code of conduct.

Finally, the consensus building should, to the extent possible, be a "future proof process", developing a code of conduct for tomorrow's complex mobile ecosystem technology, not merely today's current technology. At the same time, the privacy code of conduct should encourage technological innovations that benefit consumers and the economy and minimize inefficient burdens on businesses and consumers.

V. Conclusion

A flexible regulatory approach has fostered the development of a competitive market featuring innovative mobile devices, platforms and applications, that provide American consumers a wide array options, including a broad choice of devices, operating systems, applications and service providers, and more broadband deployment and better value as compared to other more highly regulated global markets. CTIA strongly supports President Obama's decision to utilize this flexible, self-regulatory approach, as recommended in the White

---

6. Notice and consent:

- any recognized WG participant may timely object to NTIA that appropriate notice and consent was not respected during the code development process;

7. Coherence: the process must encourage coherence to avoid any overlapping or conflicting codes of conduct for the same service, application or product.

[26] In the ICANN gTLD process, many interested stakeholders seemed not to participate until relatively late in the process until after the "consensus" had already developed and as the new critical domain name application period opened in January, 2012. Consequently, there was a great deal of confusion among many stakeholders -- with resulting political pressure being brought upon Congress and in turn upon NTIA -- at a very late stage in the process, such as whether trademark owners would need to file defensive registrations. This was confirmed by the NTIA Administrator in a January 3, 2012 letter to ICANN expressing concern about "unintended consequences" and urging that the launch of new gTLDs be "phased in". See, NTIA letter at: http://www.ntia.doc.gov/files/ntia/publications/ntia_letter_on_gtld_program_jan_3_2012.pdf. To avoid this, broad participation should be encouraged at an early stage by all industry participants, with the assurance of a safe harbor from any enforcement, and an emphasis on voluntary industry standards developed through consensus.

House's February, 2012 *Blueprint* and NTIA's March 5, 2012 Notice for Multistakeholder Comment to develop new voluntary mobile industry guidelines to protect consumer privacy. As the White House and NTIA recognize, this self-regulatory model has already fostered proactive, voluntary self-governance efforts by the mobile industry to develop robust and adaptive guidelines responsive to consumer demands for greater protection of privacy.

CTIA recommends that working groups be formed among stakeholders along the lines of common interests to engage in consensus-building on possible additional privacy codes of conduct involving principles on which there is already substantial consensus. Existing industry guidelines, such as CTIA's Location-Based Guidelines and the Feb. 2011 Joint Statement of Principles by mobile platform providers, should provide a baseline starting point for consideration of any new guidelines. Also, working groups should initially evaluate and reach agreement on the scope of affected consumer data to which such guidelines will be applied, and the nature of a safe harbor framework that will foster voluntary and broad industry participation in the multistakeholder process.

CTIA looks forward to working with NTIA and the other stakeholders on this important initiative.

Respectfully submitted,

By: _____

Michael F. Altschul
Senior Vice President and
General Counsel
CTIA – The Wireless Association®
Expanding the Wireless Frontier
1400 Sixteenth Street, NW, Suite 600
Washington, DC 20036
(202) 785-0081
www.ctia.org