KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

COMMENTS OF THE CENTER FOR DEMOCRACY & TECHNOLOGY

BEFORE THE NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION

IN THE MATTER OF

MULTISTAKEHOLDER PROCESS TO DEVELOP CONSUNER DATA PRIVACY CODES OF CONDUCT

Docket No. 120214135–2135–01, RIN 0660–XA27

APRIL 2, 2012

The Center for Democracy & Technology (CDT) appreciates the opportunity to respond to the questions posed in the National Telecommunications and Information Administration (NTIA) request for public comments (RFC). We believe the Privacy and Innovation Blueprint provides a strong foundation for this multistakeholder process and applaud the Department of Commerce's initiative. CDT has long supported a framework that gives industry segments the flexibility to develop privacy solutions that will benefit consumers, and we believe this process can move us toward this goal. We respectfully submit these comments.

RESPONSE TO QUESTIONS POSED BY THE NTIA

These comments are organized in two parts: substance and process. With regard to substance, we outline criteria for selecting privacy issues and highlight those we recommend for consideration. With regard to process, we encourage promoting participation among a wide range of stakeholders and offer advice for effective convening.

I. Substance: Selecting Privacy Issues

This part is in response to questions 1 and 2 from the RFC.

A. Criteria for Selecting Privacy Issues

The NTIA's multistakeholder process seeks to produce codes of conduct that, once created and voluntary adopted, will be binding upon companies. The RFC recognizes that the legitimacy of these codes will depend entirely upon consensus and the participation of relevant stakeholders.[1]

[1] *See* RFC at 1 ("[C]ompanies are unlikely to adopt a code about which they have serious reservations."); *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy,* The White House, February, 2012, http://www.whitehouse.gov/sites/default/files/privacy-final.pdf (Privacy and Innovation Blueprint) at 23–24, 37 (discussing importance of consensus in multistakeholder processes).

Accordingly, CDT urges the NTIA to focus initially on issues that (1) implicate a discrete, manageable set of corporate stakeholders, (2) are narrow in scope, and (3) are reasonably likely to yield consensus. Admittedly, these criteria foreclose on some important privacy issues. However, we believe this to be a wise tradeoff as NTIA fine-tunes the multistakeholder process.

For example, while we believe the data practices of mobile apps are among the most pressing privacy issues of the day, the difficulty of convening a quorum of mobile app developers presents a significant challenge for this process.[2] Accordingly, our suggestions include topics that implicate mobile platforms and carriers and are carefully scoped around transparency and device-level controls. (To be clear: we are not suggesting that the onus for protecting users' privacy vis-à-vis mobile apps falls to mobile platforms.[3] Instead, our suggestions reflect the belief that this process is best suited to address a smaller number of stakeholders.)

In sum, the NTIA can maximize the success of this process by deploying its convening power to maximum effect. We have seen the failure of many self-regulatory processes concerning consumer privacy.[4] The NTIA's efforts are likely to face some similar challenges. The NTIA's strengths lie in careful selection of issues and in providing a focused forum for discussion. (For more discussion on conducting the process, see *infra* Part II.) Early victories will lend legitimacy and empower the process to tackle more sweeping issues in the future.

B. Privacy Issues

As the RFC recognizes, the NTIA could address a wide array of privacy issues. Below, we offer a set of suggestions that fit with the criteria we outlined above. We emphasize issues that implicate small number of players. These suggestions include the retention of sensitive information (e.g., location and search data) and transparency/control issues for mobile devices.

1. Retention of Sensitive Information (e.g., location and search data)

Many companies collect and retain large amounts of sensitive data, such as search queries and precise location data. For example, consumers use search engines as a starting point to access

---

[2] The legitimacy of this process and the validity of any consensus will depend upon the need of participants. *See* Privacy and Innovation Blueprint at 26 ("[T]he deliberative process must meet the needs of its participants, who determine and abide by its outcome.").

[3] CDT and the Future of Privacy Forum (FPF) have released a draft version of best practices for mobile app developers. Best Practices for Mobile Applications Developers, CDT, December 21, 2011, https://www.cdt.org/blogs/2112best-practices-mobile-applications-developers. CDT has a long history of advocating for intermediary protections. We also strongly support frameworks that protect Internet intermediaries from liability. *See, e.g.,* Emma Llansó and Mark Stanley, *Shielding the Messengers: Section 230 and Free Speech Online*, CDT Blog, September 21, 2012, https://www.cdt.org/blogs/mark-stanley/219shielding-messengers-section-230-and-free-speech-online.

[4] *See, e.g.*, *Protecting Consumer Privacy in an Era of Rapid Change*, Federal Trade Commission Report, March 2012, http://www.ftc.gov/os/2012/03/120326privacyreport.pdf (FTC Report), at 11 ("[T]o date, self-regulation has not gone far enough."); Chris Hoofnagle, *Can Privacy Self-Regulation Work for Consumers?*, TAP Blog, January 26, 2011, www.techpolicy.com/CanPrivacySelf-RegulationWork-Hoofnagle.aspx (discussing the failure of the IRSG and NAI processes). The Digital Advertising Alliance (DAA) is poised to do better, but still has to resolve important issues surrounding collection of data in the contest of "Do Not Track." *See* Alexis Madrigal, *The Advertising Industry's Definition of 'Do Not Track' Doesn't Make Sense*, THE ATLANTIC, March 30, 2012, http://www.theatlantic.com/technology/archive/2012/03/the-advertising-industrys-definition-of-do-not-track-doesnt-make-sense/255285/.

health diagnoses, relationship advice, and many other sorts of sensitive information.[5] We have learned firsthand that even deidentified search logs can have serious privacy implications.[6] Similarly, precise location data can be highly revealing, even when it is not directly associated with other personal information.[7] In a broader vein, the Federal Trade Commission (FTC) recently recognized special privacy challenges presented by large platforms—such as Internet Service Providers, operating systems, browsers, and social media—that seek to comprehensively track consumers' online activities.[8]

Those that collect and retain search queries or precise location data, or otherwise have broad insight into consumers' online activities, have a responsibility to consumers to observe reasonable privacy practices and data retention periods. They should also employ thorough deidentification practices. These proceedings might provide an opportunity for these entities to create new best practices in these areas.

Relevant questions include:

- How long should precise location and search data be retained, and in what forms?
- What counts as precise location data?
- How long should identifying information be retained with search and location data?
- What controls and choices should be provided, and how should these vary depending on the sort of location or search data retained?
- How do these questions apply to large platforms (e.g., those highlighted by the FTC)?

2. Focused Mobile Privacy Issues

The RFC understandably emphasizes mobile privacy issues.[9] Because mobile phones are both powerful computing platforms *and* location-aware communication devices, they are at the

[5] The E.U.'s Article 29 Data Protection Working Party recently asked major search engines to reduce their data retention periods. Jeremy Kirk, *Europe warns Google, Microsoft, others about search data retention*, COMPUTERWORLD, May 27, 2010, http://www.computerworld.com/s/article/9177424/Europe_warns_Google_Microsoft_others_about_search_data_retention. *See also* Alissa Cooper, A Survey of Query Log Privacy-Enhancing Techniques from a Policy Perspective, ACM Trans. Web, 2, 4, Article 19 (October 2008) *available at* https://www.cdt.org/privacy/10012008acooper.pdf; *infra* note 6.

[6] Andrew Zangrilli, *Business Lessons from AOL's Search Data Mishap*, FindLaw, August 17, 2006, http://articles.technology.findlaw.com/2006/Aug/17/10204.html ("America Online's public disclosure of its users' search query data demonstrates the sensitive nature of search records and serves as a cautionary tale for businesses that collect and use their customers' search data. ").

[7] For example, for many, there is one location where they spend their daytime hours (at work) and one location where they spend their nighttime hours (at home). After a day or two of collecting just those two data points about a person, it becomes fairly obvious whom those data points describe. *See The Dawn of the Location Enabled Web*, CDT Policy Post, July 6, 2009, https://www.cdt.org/policy/dawn-location-enabled-web/

[8] FTC Report, 14. The FTC will be holding a workshop on this topic in the second half of 2012.

[9] The use of mobile devices is growing rapidly. *See, e.g.,* Cecilia Kang, *Smartphone sales to pass computers in 2012: Morgan Stanley analyst Meeker*, THE WASHINGTON POST, November 11, 2010, http://voices.washingtonpost.com/posttech/2010/11/smartphone_sales_to_pass_compu.html.

epicenter of many new privacy concerns.[10] However, a single code of conduct that implements the full Consumer Privacy Bill of Rights in the mobile app space, as contemplated by the RFC, would be a difficult undertaking. While issues related to apps' collection and use of data are important, as we discussed above, this process may not be best suited to create broad, app-based codes of conduct.

Instead, we present a more modest set of goals that includes convening mobile advertising networks and analytics providers (which often power a significant portion of apps' data collection) to discuss collection and use of sensitive data, as well as mobile platforms and carriers concerning more fundamental opportunities to heighten transparency and increase user control at the device level.

We suggest NTIA consider focusing on the following issue areas:

i. Use of Location by Ad Platforms, Analytics Providers, and other Third Parties

Mobile advertising and analytics services are likely to be effectively invisible third-party recipients of a consumer's mobile data. Indeed, for many apps, code provided by these entities initiates the bulk of an app's data collection.[11] While it is ultimately incumbent on app developers using such services to provide appropriate transparency and choice, relevant information can easily end up buried in a privacy policy (assuming a privacy policy is even provided[12]).

There's no question that location-based advertisements and analytics can be useful to consumers and valuable to companies and developers.[13] However, these services require grappling with the difficult questions of how granular collected data should be and how long it should be retained. Accordingly, we suggest giving special attention to the collection and use of sensitive information, like location data, by third-party advertising and analytics services. These proceedings might provide an opportunity for major mobile analytics and/or ad networks to discuss appropriate collection, use, and sharing policies for location data.

Relevant questions include:

- What practices constitute appropriate use for precise geolocation information collected by a mobile analytic or ad service acting as a third party?

---

[10] *See, e.g.,* Scott Thurm and Yukari Iwatani Kane, *Your Apps are Watching You*, THE WALL STREET JOURNAL, December 17, 2010, http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html; Alexis Madrigal, *What Does Your Phone Know About You? More Than You Think*, THE ATLANTIC, April 25, 2011, http://www.theatlantic.com/technology/archive/2011/04/what-does-your-phone-know-about-you-more-than-you-think/237786/; Julia Angwin and Jennifer Valentino-Devries, *Apple, Google Collect User Data*, THE WALL STREET JOURNAL, April 21, 2011, http://online.wsj.com/article/SB10001424052748703983704576277101723453610.html.

[11] PrivacyChoice, *Six privacy mistakes developers make*, http://www.privacychoice.org/resources/pitfalls (last accessed April 1, 2012) ("For most apps, the bulk of data collection happens when ad networks and analytics companies do their thing.").

[12] *See* Mark Hachman, *Most Mobile Apps Lack Privacy Policies: Study*, PC MAGAZINE, April 27, 2011, http://www.pcmag.com/article2/0,2817,2384363,00.asp.

[13] For a longer discussion on location-enabled mobile devices, *see* Statement of Justin Brookman, Before the Senate Judiciary Committee Subcommittee on Privacy, Technology, and the Law, *Protecting Mobile Privacy: Your Smartphones, Tablets, Cell phones, and Your Privacy*, May 10, 2011, https://www.cdt.org/files/pdfs/20110510_mobile_privacy.pdf.

- How should "Do Not Track"-type control mechanisms be applied to mobile third party services?

(*Note*: our questions concerning device-level transparency and control issues, discussed *infra* Part I.B.2.iii, are also relevant here.)

ii. Mobile Monitoring Software

The recent uproar over the Carrier IQ software prompted Rep. Edward Markey (D-MA) to release a draft bill that would require clear disclosure and express consent before monitoring software could be used on mobile devices.[14] The software in question tapped into a large and potentially revealing swath of diagnostic information from the mobile phone's operating system. For example, it could monitor what apps were used, whether an SMS was successfully sent, whether the screen was on or off, and the phone's location.[15] Phone carriers utilized the software primarily for diagnosis of hardware and network issues, collecting limited sets of data.[16]

Because Carrier IQ's software could have conceivably reported very revealing data like individual app usage, URLs, and the content of communications, this is an area ripe for voluntary codes of conduct. These proceedings might provide an opportunity for major wireless carriers and mobile platforms to address transparency concerns and outline appropriate collection and use limitations for monitoring software.

Relevant questions include:

- What level of transparency is appropriate for deployment of mobile monitoring software?
- What kinds of data might be collected without user choice and how may it be used?
- Should these standards differ for carriers, handset manufacturers, and mobile platforms?

iii. Transparency and Control on Mobile Platforms

Consumers frequently make privacy-related decisions (e.g., choosing which apps to install on an Android phone) based on information presented by a mobile operating system. While individual app privacy policies are very important,[17] "permission" requests may play an even more powerful role in informing consumers' choices. Consumers should also know if and how their device and application usage is being monitored (*see, e.g., supra* Part I.B.2.ii). This is an

[14] *See generally* Aaron Brauer-Rieke, *Bill Requires Permission for Mobile Monitoring Software*, CDT Blog, February 8, 2012, https://www.cdt.org/blogs/aaron-brauer-rieke/82bill-requires-permission-mobile-monitoring-software.

[15] For more technical details, *see* Posting of Trevor Eckhart, *What is Carrier IQ?*, *available at* http:// http://androidsecuritytest.com/features/logs-and-services/loggers/carrieriq/.

[16] Press Release, Sen. Franken Statement on Responses from Carrier IQ, Wireless Carriers, and Handset Manufacturers, December 15, 2011, http://www.franken.senate.gov/?p=press_release&id=1891.

[17] Best Practices for Mobile Applications Developers, CDT, December 21, 2011, https://www.cdt.org/blogs/2112best-practices-mobile-applications-developers.

especially salient point as background-running apps that utilize sensitive data, like precise geolocation, become more common.[18]

Consumers should be given the appropriate insight and choices, regardless of the entity collecting data or the purpose of the collection. As many have observed, mobile devices—especially smartphones—present special challenges due to their small size.[19] Since the mobile platforms (i.e., mobile operating systems) provide a foundational source of information about how device data is been used and accessed, it may be useful to convene mobile platforms to discuss improving transparency and control for mobile devices.

At this point, it's important to reiterate CDT's strong support of intermediary protections.[20] In the past, we have emphasized that a significant number of privacy issues are best addressed by app developers.[21] However, we believe a voluntary, transparent, multistakeholder forum can be an appropriate setting to address these particular intermediaries with the goal of developing best practices concerning device-level and OS-level transparency and control mechanisms. Mobile platforms recently expressed a willingness to engage in such an inquiry with the California Attorney General,[22] and this forum may be an appropriate and effective place to continue that discussion.

Relevant questions include:

- What options are available for mobile platforms and/or mobile operating systems to obscure location-based data? (e.g., reporting city/state instead of precise latitude and longitude)
- What kind of notifications and consent procedures should be deployed for different sorts of data requests?

---

[18] For example, the Electronic Frontier Foundation (EFF) recently discussed an "ambient social networking" app, Highlight, which persistently collects a user's location information for social networking purposes. Parker Higgins, *Highlighting a Privacy Problem: Apps Need to Respect User Rights From the Start*, EFF Deeplinks Blog, March 8, 2012, https://www.eff.org/deeplinks/2012/03/highlighting-privacy-problems-apps-need-respect-user-rights-start. Also, Groupon recently began using location information to offer users deals based on the time of day and their location. Dan Rowinski, *Groupon Changes Privacy Policy, Starts Tracking User Location*, ReadWriteWeb, July 11, 2011, http://www.readwriteweb.com/archives/groupon_changes_privacy_policy_starts_tracking_use.php. These are but two examples of apps that fall into this category.

[19] The FTC recently announced a workshop to discuss mobile disclosures on May 30, 2012. FTC Report at v. And, of course, privacy policies present significant difficulties even absent the special challenges introduced in the mobile context. *See, e.g.,* Aleecia McDonald and Lorrie Faith Cranor, *The Cost of Reading Privacy Policies, I/S: A Journal of Law and Policy for the Information Society* (2008 Privacy Year in Review issue), *available at* http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf (showing that for a consumer to reach a basic understanding of how his or her information is being collected and used, he or she would have to spend between 181 and 304 hours each year reading Web site privacy policies).

[20] *See, e.g.,* Intermediary Liability: Protecting Internet Platforms for Expression and Innovation, CDT Report, April 27, 2010, https://www.cdt.org/paper/intermediary-liability-protecting-internet-platforms-expression-and-innovation; Emma Llansó and Mark Stanley, *Shielding the Messengers: Section 230 and Free Speech Online*, CDT Blog, September 21, 2012, https://www.cdt.org/blogs/mark-stanley/219shielding-messengers-section-230-and-free-speech-online.

[21] *See, e.g., supra* note 13.

[22] *See* Press Release, *Attorney General Kamala D. Harris Secures Global Agreement to Strengthen Privacy Protections for Users of Mobile Applications*, Office of the California Attorney General, February, 22, 2012,http://oag.ca.gov/news/press_release?id=2630 (and attached agreement).

- What choices should be provided to users regarding collection and use of data by mobile platforms and handset manufacturers?

3. Other Privacy Issues

- *Data Broker Privacy and Access*

  In its final Privacy Report, FTC emphasized the need for greater transparency and control over the practices of data brokers. The Report recognized a "lack of transparency about the practices of information brokers, who often buy, compile, and sell a wealth of highly personal information about consumers but never interact directly with them."[23] The FTC recommended Congressional legislation, but also called upon data brokers to create a centralized resource to identify themselves to consumers and detail the access rights and other choices they provide.[24] Especially given its relatively small number of players, this space might be an area ripe for codes of conduct.

- *Commercial Cloud Provider Privacy*

  Cloud computing vendors are providing storage, connectivity, and processing power for an increasing number of web services. As these cloud services become a regular fixture in the IT infrastructure for consumer-facing web services, a new set of important privacy considerations arise. Traditionally, a single entity has been accountable for the privacy and protection of its customers' data. As the supply chain of IT resources extends, allocation of responsibility and accountability becomes more complicated and important.[25] Relevant considerations include the creation, retention, and use of ancillary data[26] and special data breach-like notification procedures.[27]

- *Computer Vision Privacy*

  Computer vision systems, such as facial recognition, are rapidly growing in sophistication.[28] Such systems are capable of tracking individuals over a wide area for

---

[23] FTC Report at v, ix.

[24] *Id.*

[25] For example, NIST has published a paper on cloud privacy and security concerns for public sector entities. Wayne Jansen and Timothy Grance, *Guidelines on Security and Privacy in Public Cloud Computing*, NIST Special Publication 800-144, www.nist.gov/customcf/get_pdf.cfm?pub_id=909494. The same sorts of issues are likely relevant to cloud services serving commercial entities.

[26] *See id.* at 20.

[27] Special notifications may be appropriate in this context. As the NIST paper contemplates: "[A] database of contact information stolen from a SaaS cloud provider, via a targeted phishing attack against one of its employees, was used in turn to launch successful targeted electronic mail attacks against consumers of the cloud service. The incident illustrates the need for cloud providers to protect and report promptly security breaches occurring not only in the data the cloud provider holds for its consumers, but also in the data it holds about its consumers, regardless of whether the data is held within or separately from the cloud infrastructure." *Id.*

[28] CDT recently published a report on facial recognition and privacy. Center for Democracy & Technology, *Seeing is ID'ing: Facial Recognition and Privacy*, December 6, 2011, https://www.cdt.org/report/seeing-iding-facial-recognition-and-privacy (report attached at https://www.cdt.org/files/pdfs/Facial_Recognition_and_Privacy-Center_for_Democracy_and_Technology-January_2012.pdf).

an extended period and serving individually-targeted advertising on networked screens. Some cameras are sensitive enough to detect certain health conditions through visual perception alone.[29] Importantly, advanced computer vision capabilities are being integrated into common consumer devices, such as smartphones, enabling widespread and potentially invasive use of the technology by the public.[30] While voluntary codes of conduct for the commercial use of facial recognition are in place with two trade associations, these codes apply only to the members of the trade association and only to relatively discrete uses of commercial facial recognition.[31] Important considerations include whether individuals have a choice in being tracked by a computer vision system over an extended period for commercial purposes, and transparency in the location and purpose of commercial computer visions systems.[32]

II. Process: Ensuring Fair, Effective Convenings

- **How can NTIA promote participation by a broad range of stakeholders, i.e., from industry, civil society, academia, law enforcement agencies, and international partners?**
- **How can NTIA best ensure the process is inclusive, given that participants will likely have different levels of resources available to support their participation?**

We applaud NTIA's commitment to involving a broad range of stakeholders. However, one of the primary barriers to participation by a diverse set of stakeholders will be resources. Many non-industry participants (as well as participants from small companies) will have limited resources to devote to this effort. Limited resources hamper entities' abilities to both travel to meetings and dedicate personnel to the process. By contrast, large companies may be able to devote one or multiple individuals to full-time work in the process. These participants will have the flexibility to read and draft language at a moment's notice, to craft and respond to detailed, technical emails, and to otherwise integrate themselves into the process, whereas other participants may not.

The work of large industry participants will expedite and be an asset to the process, but this can come at the cost of balanced participation by a diversity of stakeholders. Ensuring that small organizations with fewer staff and resources—including academics, law enforcement agencies, advocacy groups, and international partners—can participate fully in the process should be a priority.

To promote a full spectrum of participation, our suggestions include:

- In-person meetings should take place primarily in Washington, D.C., where a sizable number of non-industry participants are likely to be based. Taking into consideration organizations that do have to travel, a few longer, in-person meetings (e.g., a single three day convening) would be likely be more resource efficient than a greater number of short, in-person meetings (e.g., three separate one-day meetings).

[29] *Id.* at 2-3.

[30] *Id.* at 6.

[31] *Id.* at 11.

[32] *Id.* at 15.

- The facilitators of the process should act with a strong guiding hand. This will help the process in two ways. First, facilitators can help consolidate proposals, emails, and other conversations to help everyone stay abreast of the discussion. Second, facilitators can help maintain focus on the appropriate issues and prevent conversation from straying to irrelevant or tangential topics.

- **How can NTIA promote participation by a broad range of stakeholders, i.e., from industry, civil society, academia, law enforcement agencies, and international partners?**

  As suggested in the RFC, participants should include representatives from industry, civil society, academia, law enforcement agencies and other interested agencies (such as the FTC), and international partners. International partners will be able to offer a perspective on whether the codes of conduct will be sufficient to satisfy regulators in other countries, a perspective that may be of particular interest to industry participants.

  As discussed above, it is crucial that a balance of interests is represented in the convenings. What this "balance of interests" looks like might vary from topic to topic. We urge the NTIA to carefully consider participation on a topic-by-topic basis. (For more information on selection of appropriate topics, please see the discussion *supra*, Part I).

  Stakeholders with technical expertise, including those who can speak on behalf of industry, will be vital to the process. Industry representatives will be most helpful if they are able to explain how their respective companies' relevant technologies work and if they can answer specific questions to this effect. Consumer representatives will need enough technical expertise to evaluate the claims made by the industry representatives. Government and academic representatives should also be prepared to engage on a technical level.

  Finally, if a small number of industry stakeholders are dominant in a particular space, then it is absolutely essential to the relevance of the process that these stakeholders participate. For example, Apple and Google currently dominate the market for smart phones and tablet operating systems. To the extent codes of conduct are considered that might be relevant to mobile operating systems, the relevancy and legitimacy of these codes depends upon this participation.

- **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?**

  Prerequisites for participation are consistent with the principle of openness. While we remain concerned with promoting equal participation by organizations with limited resources, we believe that requiring a show of interest and commitment is appropriate. Organizations that are unable to muster the resources to put together a position paper will likely be unable to participate in the multistakeholder process in a meaningful way.

- **What balance should NTIA seek to achieve between in-person and virtual meetings?**

  Both virtual and in-person meetings have advantages. The best approach probably involves a combination. However, we strongly suggest that the process begin with a multi-day, in-person meeting and that a few such meetings are scheduled throughout each process. In-

person meetings facilitate engagement with and investment in the process to a degree that is unlikely to be achieved over the phone.

- **How should discussions during meetings be memorialized and published? Are verbatim transcripts or full recordings necessary, or would a more abbreviated record be appropriate?**

  We applaud the NTIA's commitment to a transparent process and emphasize the importance of providing *meaningful* notes and records. More abbreviated records would likely be far more useful to a broad range of participants than full transcripts. We are concerned that verbatim transcripts or full recordings would be difficult for lower-resourced participants to follow, hampering a meaningful dialogue. Instead, we suggest that the facilitators issue a short progress report after each multi-day meeting and, potentially, after each phone call.

  It might be useful to apply Chatham House Rules for some (but perhaps not all) portions of the process. Under Chatham House Rules, participants are free to use the information they acquire at a meeting but are not permitted to attribute that information to any individual or entity. Such rules would be respected not just by meeting participants but also within the official reports that would emerge from each meeting. These reports would therefore communicate the substantive discussions and decisions reached during each meeting but without attribution.

  Reports that summarize substantive decisions offer an additional advantage: they can be helpful for participants who have missed meetings or, because of a bad phone connection, language barriers, or for other reasons, could not follow the discussion. The use of such reports can also help prevent unnecessary discussion of already-resolved issues and can help ensure that all participants share a common understanding of where the process stands.

- **How can NTIA facilitate broad public review of codes of conduct during their development?**

  At a certain point in the process, draft codes of conduct should be made subject to a notice-and-comment period. Twenty days is an appropriate length of time for the notice-and-comment period. Once the period has ended, the codes of conduct should be modified based on the feedback received.

- **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?**

  It is important that the NTIA carefully scopes both the problem the group is trying to solve and the available solutions. History has shown that it is easy for participants to be drawn into legacy debates that are neither especially relevant nor especially constructive to the process. This problem is exacerbated when the topic for discussion is not narrowly scoped. As CDT wrote in a paper about the P3P process:

  > Pieces were added and then taken away. Professor [Lorrie] Cranor has aptly compared the process to out-of-control construction on a kitchen that at first only needs a small new

> appliance (a toaster) but ends up with a plan for new cabinets, floors and lighting. Controversial ideas for negotiation, automated data transfer and others were added. Fortunately, discussions about the complications introduced by these additions — as well as the significant work required just to finish the vocabulary alone — led the group to cut back on all of these ideas and to more or less return to the original plan. However, a lot of time and effort was wasted debating these large-scale additions to the specification.[33]

Earlier, we explained that strong facilitators can help ensure that discussion stays on track. Strong facilitators can also help ensure that the process proceeds efficiently. For example, while the facilitators should absolutely make sure that all voices are heard and that all stakeholders have the opportunity to meaningfully contribute, it will also be important for facilitators to intervene if stakeholders who have otherwise been silent throughout the process involve themselves at the very last minute in an effort to filibuster or derail consensus.

- **How did those groups define consensus? What factors were important in bringing such groups to consensus?**

  A group of consumer organizations, in a February 2011 statement, published a set of "Principles for [the] Multi-Stakeholder Process."[34] The statement's seventh principle offers a useful starting point for discussions of how consensus should be reached: "Decisions must be based on a fair and broad consensus among stakeholders rather than a majority vote by participants. The process should seek to resolve issues through open discussion, balance, mutual respect for different interests, and consensus."

  The process for achieving consensus at the World Wide Web Consortium (W3C) offers guidance for how a process that resolves issues in accordance with this principle might be conducted. At the W3C, "consensus" is achieved when "a substantial number of individuals in the [group] support the decision and nobody in the [group] registers a formal objection. Individuals in the [group] may abstain."[35] In this context, filing a "formal objection" is an option that is rarely exercised; when it is, the filing of such a formal objection is taken quite seriously. Indeed, to our knowledge, no formal objection has yet been filed by a member of the Tracking Protection Working Group, the W3C working group that is developing web standards for Do Not Track. The balance this system creates is one that errs in favor of consensus.

  Put more colloquially, the question asked is *not* "is this the best solution?" but rather "can we live with this?" We believe this approach promotes consensus by group members and the NTIA would be wise to adopt it.

---

[33] Ari Schwartz, *Looking Back at P3P: Lessons for the Future*, Center for Democracy & Technology, November 2009, https://www.cdt.org/files/pdfs/P3P_Retro_Final_0.pdf.

[34] World Privacy Forum, Consumer Action, Consumer Watchdog, Privacy Rights Clearinghouse, American Civil Liberties Union, Consumer Federation of America, Electronic Frontier Foundation, U.S. PIRG, Center for Digital Democracy, Consumers Union, National Consumer League, *Principles for Multistakeholder Process*, February 23, 2012, http://www.consumerfed.org/news/463.

[35] World Wide Web Consortium, *W3C Process Document: General Policies for W3C Groups*, http://www.w3.org/2005/10/Process-20051014/policies#Consensus (Last accessed March 20, 2012).

- **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?**

  It may be appropriate for NTIA to facilitate discussions among sub-groups of stakeholders. It is often easier for smaller groups to maintain focus, produce usable language, and reach compromise. However, in these cases, NTIA needs to notify other stakeholders, in real time, of both the fact it is facilitating such a discussion and who the participants are. Any "decisions" or "conclusions" reached by sub-groups must of course be brought to the full group for discussion and debate.

  Individual stakeholders may deploy tactics that are particularly disruptive to consensus, inadvertently or otherwise. For example, a stakeholder might remain silent throughout the majority of the process, only to voice substantial concerns just as the process is nearing conclusion. The NTIA should set firm ground rules and use strong moderation to help avoid such risks.

For more information, contact Aaron Brauer-Rieke (aaron@cdt.org, 202-407-8820) or Justin Brookman (justin@cdt.org, 202-407-8812).