



April 2, 2012

Sent via electronic filing to [privacyrfc2012@ntia.doc.gov](mailto:privacyrfc2012@ntia.doc.gov)

National Institute of Standards and Technology  
Lawrence E. Strickling, Assistant Secretary for Communications and Information  
U.S. Department of Commerce  
1401 Constitution Avenue N.W., Room 4725  
Washington, DC 20230

RE: Docket No. 120214135-2135-01 – OTA’s comments in response to the request for comments regarding a multi-stakeholder process to develop voluntary yet enforceable Consumer Data Privacy Code(s) of Conduct

Dear Assistant Secretary Strickling,

Thank you for providing the Online Trust Alliance (OTA) the opportunity to submit comments on the White House Privacy Bill of Rights (“PBR”) and voluntary privacy Code of Conduct, (“Code”).<sup>1</sup>

OTA commends the efforts of the White House and Department of Commerce in the development of the Privacy Bill of Rights and the commitment to support a multi-stakeholder process to develop a voluntary privacy Code. Since OTA’s formation in 2004, we have advocated for voluntary best practices to enhance online trust and confidence including data privacy protections which we believe is essential to maintaining consumers’ trust in the digital economy. Confidence that user preferences are honored is the foundation of the internet and critical to the long-term growth and vitality of online services.

As stated by the President in the launch of the PBR, “even though we live in a world in which we share personal information more freely than in the past, we must reject the conclusion that privacy is an outmoded value.” As stewards of data OTA believes it is essential for industry to embrace this view as it innovates and develops new products and online services.

---

<sup>1</sup> As a member-based non-profit, OTA includes nearly 100 organizations representing the Internet ecosystem, with members including the public and private sector. OTA’s mission is to develop and advocate best practices and public policy to mitigate privacy, identity, and security threats. Our goal is to enhance online trust and confidence which is the cornerstone of the digital economy and all online services. <https://otalliance.org>

Self-regulation provides industry with an effective and *agile* vehicle to respond to new challenges, technologies and threats across the internet ecosystem. For the internet to prosper self-regulation with meaningful codes of conduct can be an ideal way to balance privacy, innovation and security. Industry and consumers can mutually benefit from the adherence to best practices and Codes designed to protect users' privacy and data while reinforcing the value users may receive from services which may collect data. Those entities who self-assert their support should be recognized as "North Stars", allowing them to differentiate their services based on their privacy practices and resulting value proposition

Bringing together representatives from industry, government, academia and advocacy to collaborate in the development of voluntary codes of conduct affords the opportunity to preserve consumer privacy and trust while assuring the vitality of internet services. It is important to acknowledge potential short-comings when such efforts are totally transparent and open to any interested party. The process risks becoming unnecessarily elongated while participants hedge or posture what they say due to the public nature of these efforts.

OTA has a long-history of supporting such efforts and codes of conduct including ISP best practices as well as publishing specific guidelines for countering malvertising, driving adoption of email authentication, enhancing security of email service providers and publishing data breach readiness guidelines.<sup>2, 3, 4, 5</sup> OTA believes consumers and industry is best suited with the adoption of a voluntary code versus added legislation and regulations which risks encumbering legitimate businesses and can stifle innovation.

Creating such code is preferable to legislation assuming it can be completed in a reasonable time period (less than 12 months). This position is based on the assumption that such codes are meaningful, actionable and measurable and quickly adopted. In the absence of such, legislation may be required. While such a code develops, the FTC must remain vigilant and continue its current efforts against bad actors and firms who violate existing regulations or fail to uphold their privacy and data use polices.

OTA supports the multi-stakeholder process proposed by the Administration. At the same time OTA believes industry driven initiatives can move forward more quickly, assuming parties are committed to making meaningful changes to advance consumer control of the privacy and data usage. Recent example includes the introduction of Domain-based Message Authentication, Reporting & Conformance (DMARC)<sup>6</sup>, and the efforts of the Digital Advertising Alliance (DAA).<sup>7</sup>

---

<sup>2</sup> Anti-Malvertising Guidelines - <https://otalliance.org/resources/malvertising.html>

<sup>3</sup> Security by Design Email Marketing Guidelines - <https://otalliance.org/resources/securitybydesign.html>

<sup>4</sup> Data Incident Planning Guide - <https://otalliance.org/resources/Incident.html>

<sup>5</sup> Email Authentication <https://otalliance.org/resources/authentication/index.html>

<sup>6</sup> "Domain-based Message Authentication, Reporting & Conformance", (DMARC) is a technical specification created by a group of organizations to help reduce the potential for email-based abuse.

<https://otalliance.org/resources/authentication/dmarc.html>

<sup>7</sup> DAA <http://www.aboutads.info/>

The DAAs, “self-regulatory program for online data collection” is an example of an industry driven initiative and a positive step towards this goal. Recently the DAA revised their principles to now include limitations on the collection of tracking data and prohibitions on the use or transfer of the data for employment, credit, insurance or health care eligibility purposes. This is a positive step and we now need to build upon these efforts to honor user preferences as they apply to all collection, use and sharing of any data as it applies to third parties data if so requested.

As outlined in the PBR and last week’s FTC release of the “Protecting Consumer Privacy in the Era of Rapid Change” report, OTA strongly supports the use and deployment of browser based “Do Not Track” (DNT), mechanisms as it applies to the collection and usage of third party data, when consistent with the context of the user's interactions with the service. An exception is required for data used for "internal operations" such as website analytics, fraud detection and other tailored exceptions. Such browser based mechanisms need to shift from their current state of being obscure to the common user, to becoming discoverable, persistent and universal, while providing relying websites visibility of the user’s choice.

In addition, it is recommended a DNT include a user defined allow mechanism, which on a site or advertiser basis, could override the global settings when a DNT is enabled. While such functionality may not immediately be available, it needs to be defined within scope to enrich choices and reward self-asserting companies. In addition it is recommended domain based DNT be supported to provide for a company level opt-out.

As a multi-stakeholder organization focused across the ecosystem, OTA recommends the following principles be considered in the formation of a multi-stakeholder process:

1. Governance Models / Steering Committee - Consider a model such as the Federal Communication Commission’s Communications Security, Reliability and Interoperability Council (CSRIC), whereas the FCC Chairman and staff appoint stakeholders to address key initiatives.<sup>8</sup> It is proposed a Steering Committee be established with key constituencies, including but not limited to, consumer and privacy advocates, technology and browser providers, trade organizations and other non-profit organizations. Participation should be limited to those stakeholders who have been involved in the privacy public policy discussion and have demonstrated a track record developing best practices as well as committed to supporting the role of self-regulation.
2. Participation & Selection of Participants – It is agreed the working group must be transparent and representative of the ecosystem. Applicants and nominees should submit a position paper outlining key roles, concerns and any appropriate disclosures including a brief bio of the designated representative.
3. Senatorial Design - It is suggested an equal number of seats or votes be allocated across the ecosystem representing key constituencies, including but not limited to consumer and privacy advocates, advertising community, web publishers, analytic and browser communities. This

---

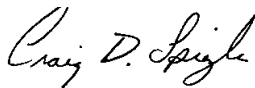
<sup>8</sup> <http://www.fcc.gov/encyclopedia/communications-security-reliability-and-interoperability-council-iii>

will help assure all voices are heard, while insuring this discussion is not dominated by one or more constituencies.

4. Leverage lessons learned from other efforts including those of the standards community and needs to balance the ability of being open to anyone versus limiting inclusion to entities who are stakeholders with subject matter expertise. Allowing anyone to participate introduces a risk of derailing efforts to drive meaningful results and having to educate non-stakeholders to the issues and complexity of the ecosystem.
5. Meetings format and venues should insure inclusiveness of vested stakeholders, alternating between the East and West Coast venues, scheduled to accommodate time zones while utilizing web and video technologies to maximize participation.
6. Metrics & Tracking – Once established it is important to support the independent adoption of any such “code or best practices”, with the goal to recognize early adopters and to provide consumers transparency of the privacy practices of the brands and sites they frequent.

The comments in this document are independent of any trade organization or special interest group and represent the rough consensus of our membership, recognizing one or more member company may not agree with every recommendation put forth. OTA looks forward to the continued dialog and participation in this effort and joining as an active participant in the multi-stakeholder process.

Sincerely,



Craig D. Spiezle  
Executive Director and President  
Online Trust Alliance