Congress of the United States
Washington, DC 20515

June 19, 2012

Dear World Wide Web Consortium Tracking Protection Working Group:

In December 2010, the Federal Trade Commission (FTC) called for a browser-based "Do Not Track" mechanism that would empower consumers to "choose whether to allow the collection and use of data regarding their online . . . browsing activities."[1] The FTC identified five central features of Do Not Track: it should be universal, usable, persistent, enforceable, and cover data collection—not just data use. As co-Chairmen of the Congressional Bi-Partisan Privacy Caucus, we agree with those worldwide who have repeatedly insisted that users should have control over *both* the collection *and* the use of their personal data. We also believe that browsers that default to Do Not Track provide consumers with better control and choice with respect to their personal information.

Researchers, consumer and privacy organizations, and browser vendors have collaborated to advance a simple signal of a user's preferences about web tracking, the "DNT: 1" HTTP header. This Do Not Track technology will soon be supported by all the major web browsers, and more than ten million consumers have already expressed a preference for Do Not Track.[2] However, while there is increasing consensus among stakeholders on the Do Not Track concept, broad agreement on a specific definition and policy framework governing compliance with consumer Do Not Track preferences remains elusive. In our view, Do Not Track should encompass non-targeted advertising along with not accumulating, using, sharing, or selling the consumer's personal data.

The World Wide Web Consortium (W3C) has convened experts with many different perspectives to develop a single, global standard for the Do Not Track technology and policy. In anticipation of the next W3C Tracking Protection Working Group meeting in Bellevue, Washington from June 20-22, we urge W3C participants to commit to user control over *both* data collection and use. We understand that advocates and academics have offered substantial concessions, such as limiting first-party compliance obligations and permitting information sharing among corporate affiliates. It is time for industry participants to likewise move towards agreement by accepting a commonsense definition and governance structure for Do Not Track.

We are heartened by Twitter's recent announcement of its intention to abide by users' Do Not Track preferences as they arrive at its site. Microsoft also announced in May that the Internet Explorer 10 browser will utilize a default Do Not Track setting. We have long endorsed a

---

[1]Federal Trade Commission. (2010, December). Protecting consumer privacy in an era of rapid change: A proposed framework for business and policymakers. Retrieved June 12, 2012, from http://www.ftc.gov/os/2010/12/101201privacyreport.pdf

[2] Kaste, M. (2012, April 10). 'Do not track' web browser option gains steam. *npr.* Retrieved June 14, 2012, from http://www.npr.org/2012/04/10/150335249/do-not-track-web-browser-option-gains-steam

PRINTED ON RECYCLED PAPER

standard that allows consumers to affirmatively choose whether to permit collection of their personal information and targeting of advertisements. In this spirit, we call on W3C participants to make the protection of consumer privacy a priority and support Microsoft's announcement by endorsing a default Do Not Track setting.

Thank you for your attention to this important matter. If you have any questions, please have your staff contact Joseph Wender in Congressman Markey's office (202-225-2836) or Emmanual Guillory in Congressman Barton's office (202-225-2002).

Sincerely,

Edward J. Markey
Co-Chairman
Congressional Bi-Partisan Privacy Caucus

Joe Barton
Co-Chairman
Congressional Bi-Partisan Privacy Caucus