**Comments from American Association of Advertising Agencies (4A’s)**

The following comments are submitted by the 4A’s to the World Wide Web Consortium (W3C) Tracking Protection Working Group (TPWG) in response to the “Last Call for Comments” on the group’s Tracking Preference Expression (TPE) draft. The 4A’s participated in many of the working group discussions, meetings and other deliberations as a past W3C member. We have thus developed an understanding of the various components of the Do-Not-Track specification. This specification has raised serious concerns about what information and control Internet consumers will genuinely hold, In addition this proposed specification will have adverse implications for when and how online data can be collected. These factors will impact many 4A’s member agencies as well as the online advertising industry as a whole. Our specific concerns are itemized below.

**Inauthentic User Choice**

The specification lacks a reliable method for validating and ensuring that each DNT signal is set as the result of an actual, informed choice by the end user. This means that routers, antivirus software, browser plugins, proxies, or ISPs, can all insert a DNT signal into the browser’s HTTP request, and the recipient server has no way of knowing whether it reflects the user’s choice or that of another entity entirely. That is not an authentic expression of consumer preference. Instead, it will create confusion when users attempt to manage their privacy and exercise their privacy choices relating to data collection.

**Inability to Implement**

The specifications draft thus far neither translates nor reads in a user-friendly manner and thus will prevent (instead of ensure) consistent deployment. For example, the protocol lacks a method to identify and validate the origin of the DNT signal, which means other variables, (aforementioned routers, antivirus software, browser plugins etc.) may all randomly insert a DNT signal. No server can confidently respond with an indication of how to treat a DNT signal. Terms within the TPE specification such as "data regarding a particular user's activity," "multiple distinct contexts," "resources", and "jointly controlled by a set of parties" are ambiguous, and risk significantly broad and varied interpretations. The only companies that would have to honor DNT are those who do not currently have any information about certain end users. As such, users will have a very difficult time understanding when DNT applies.

**Market Inequality**

The draft specification is strongly prejudicial to large companies and exempts some entities from any program requirements. This places many small and mid-sized companies –who are such a vital part of the growth and vitality of the Internet –in a disenfranchised position that will have market effects that ultimately disadvantage many Internet consumers. The inevitable result will be more consolidation among dominant players, higher prices for products and services and less variety and choices for consumers.

**Inappropriate Forum**

Lastly, the Tracking Protection Working Group itself simply is not the appropriate forum for critical policy making decisions. The W3C as a technical body brings a storied history of developing technical specifications for key Internet infrastructure methods and protocols. However, identifying and addressing clearly defined privacy harms is wildly out of scope with this history and beyond the capabilities of the working group and its charter. The Tracking Protection Working Group is simply not the appropriate forum for conducting constructive conversations or developing achievable collaborative solutions to these complex issues. The working group has struggled for many years and witnessed the departure of many key stakeholders (industry members, technologists, consumers advocates and academics alike). Its failure achieve consensus on even the most basic concepts (such as definitions) bears out this unfortunate reality. The TPE document now presented for comment does not represent the consensus of a broad set of stakeholders but rather the narrow vision of a select few remaining authors.

**Conclusion**

4A’s believes strongly that managing and evolving existing self-regulatory frameworks such as the Digital Advertising Alliance (DAA) will most effectively address clearly defined privacy harms by continuing to provide effective consumer controls without inhibiting innovation and market growth. These programs have demonstrated wide deployment which the W3C is not likely to deliver with a standard that does not reflect consensus on so many key issues and approaches.