Vivek Narayanadas
Director, Legal & Privacy Affairs
The Rubicon Project, Inc.
12181 Bluff Creek Drive, 4th Fl.
Los Angeles, CA 90094

June 18, 2014

World Wide Web Consortium
Tracking Protection Working Group
W3C/MIT
32 Vassar Street
Room 32-G515
Cambridge, MA 02319

To Whom It May Concern,

The Rubicon Project, Inc. ("Rubicon Project") submits the following public comments in response to the Tracking Protection Working Group's (the "Working Group") last call draft of the Tracking Preference Expression ("TPE") specification defining the "Do Not Track" request header field. These comments are intended to clarify certain language in the TPE, and to identify for the Working Group technical problems with the specification, all of which may end up *preventing* the intended goal of the specification: to improve the user experience by technically defining a uniform mechanism through which users can announce their preference not to be tracked.

*First*, Rubicon Project is concerned that the TPE unnecessarily purports to define "tracking" and respectfully requests that this definition be removed prior to its final publication. The TPE, by its own terms, is *not* intended to "define site behavior for complying with a user's expressed tracking preference, but [rather to] provide sites with a ***mechanism*** for indicating compliance." In other words, the TPE does *not* need to define the type of activity (*i.e.*, "tracking") that should cease upon the receipt of a DNT request; it is only meant to technically define how such a request should be communicated. By including such a definition in this technical document, Rubicon Project is concerned that the Working Group is exceeding the scope of its charter, which provides that the TPE should only "define[] the ***technical mechanisms*** for expressing a Do Not Track preference" and leaves the task of "defin[ing] the ***meaning*** of a Do Not Track preference" for a subsequent document that is still being debated.

While Rubicon Project understands the desire to offer such a definition at this stage, particularly given that the definition is the same as in the current draft of the Tracking Compliance and Scope ("TCS") specification, defining such a key term in two separate documents raises the serious risk of inconsistencies. If the industry as a whole, or

influential regulatory or self-regulatory bodies, reach a consensus adopting a *different* definition of "tracking" before the TCS is issued, the Working Group will find itself with the prospect of either: (1) having to change the definition in the TCS (and having inconsistent definitions); (2) having to revisit the by-then-finalized TPE; or (3) having its specifications become obsolete even before the TCS is finalized. There is no need to take on such risks, particularly when the TPE—a purely technical document—need not include such a definition. As such, Rubicon Project requests that the Working Group remove this unnecessary definition from the TPE.

*Second*, as others have observed, the TPE provides no way for responding servers to confirm that a received DNT signal was actually set by the user agent. The lack of any available authenticating mechanism means that a responding server must respond to a DNT signal blind, simply assuming such a signal was intentionally sent by the end user. Such a result is at odds with the stated intent of the TPE, which is to empower *end users* (and not other third parties) to informedly state a preference as to tracking.

Without any authentication mechanism, intermediaries in the data stream between the user agent and the responding server have the ability and incentive to insert themselves into the data stream and state a preference purportedly *on behalf of* a user agent. ISPs, routers, add-ons, etc. have incentive to change *all* DNT signals to "1" in order to position themselves in their respective marketplaces as more "privacy-friendly" regardless of whether the user is even aware of the third party's practice, and regardless of the user's actual tracking preferences. Rubicon Project requests that the Working Group add some authentication mechanism to the TPE—for example, by requiring the use certificates to confirm the user agent's DNT selection, or a central repository storing user agent preferences—to ensure that responding servers honor the *end user*'s actual preferences, rather than the skewed preferences of third parties trying to game the system to their benefit. Such an authenticating mechanism will also allow third parties receiving a DNT signal to ensure that the actual signal-setting agent is properly presenting the end user his or her choices, in accordance with the TPE, rather than making the decision unilaterally for the end user.

*Third*, the TPE does not provide any guidance as to *when* a server must respond to a valid GET request for tracking status. Timing may not matter for many parties in the ecosystem, but it is particularly important for third parties like Rubicon Project that operate or use automated exchanges that allow real-time bidding. Because only a bid *winner* can adequately respond to the GET request, the specific tracking status resource ("TSR") response will change depending on whether the GET request is sent immediately upon loading a page (*i.e.*, before bidding on an impression is complete), or instead is sent *after* bidding is complete and the winner is determined. Rubicon Project is concerned that such a system could actually *increase* end user confusion and uncertainty, by providing different responses at different times. To the extent that user agents, plug-ins, or add-ons rely on the TSR to inform the an end user of a responding server's tracking practices, the fact that the content of the notice to the end user would

change depending on the timing of the request could undermine consumer confidence in the DNT mechanism and actually *cause* consumer confusion. Accordingly, Rubicon Project requests that the Working Group include some guidance as to how responding servers should deal with such timing issues.

Please do not hesitate to contact us if you have any questions about these comments. We look forward to receiving your response.

Sincerely,

Vivek Narayanadas
Director, Legal & Privacy Affairs