PubMatic
305 Main Street, 1st floor
Redwood City, CA 94063

June 17, 2014

Via Email to public-tracking-comments@w3.org
Tracking Protection Working Group
W3C

Re: Comments on Tracking Preference Expression (DNT) W3C Last Call Working Draft 24 April 2014

To Whom It May Concern,

PubMatic submits these comments in connection with the Last Call Working Draft entitled "Tracking Preference Expression" (DNT), which was published on April 24, 2014.

PubMatic's mission is to enable publishers to realize the full potential of their digital assets. Since its founding in 2006, the company has offered publishers innovative, industry-changing products, services and systems to help optimize the potential of their digital assets. PubMatic is consistently one of the first to market new products and services, including yield optimization for publishers across ad networks, real-time bidding (RTB), audience data analytics, and unified revenue optimization packages.

The W3C, and in particular, the Tracking Protection Working Group ("TPWG"), has invited broad community review of their Working Draft, especially of "technical requirements and dependencies." The Group encourages reviewers to identify technical problems with the draft, and to point out where it fails to further goals of user privacy and user control. As an industry leader in programmatic digital advertising, PubMatic is uniquely qualified to represent the views of many in the digital advertising industry on these topics.

PubMatic applauds the work done by the TPWG in moving toward a workable technical specification for a DNT expression. This has proven to be a difficult process, and we commend the members of the Working Group for their efforts. Ultimately, however, we believe that the Draft reveals, once again, the difficulty with applying the TPWG's technical expertise to public policy issues. The important issues surrounding consumer privacy, and in

this case, DNT, are good candidates for productive dialog among policymakers. Such policy debates should not be the undertone for, or carry over into, the TPWG's technical specification.

Ultimately, we believe that the technical specification inappropriately exhibits the TPWG's bias for having users enable the DNT preference by including slanted and improper definitions of key terms, a notice-and-choice mechanism that leans towards DNT:1, and undue limitations on DNT:0 expression. These policy preferences have no place in the technical specification, which should be limited to accurately defining the boundaries of DNT preference expression, and no more.

A. Definition of Tracking is Overbroad and Unnecessary

First, the definition of "tracking" as used by the TPWG is too broad, suggesting that the TPWG's standard for Do Not Track means more than simply "Do Not Target," and leans towards "Do Not Collect." *This is a policy decision that should be reserved for a later date*, and that is not necessary to define how DNT choices should be expressed. However, from a technical standpoint as well, equating "tracking" with "collecting" is erroneous and overbroad. For example, collection of data about users may be necessary for website functionality or user experience. Alternatively, collection of data may be required for fraud prevention or compliance with law, or for network security.

The Center for Democracy and Technology (CDT) offers the following definition of tracking, which we offer for the sole purpose of illustrating that "tacking" is broader than "collecting" (PubMatic does not otherwise endorse the CDT proposal): "tracking is the collection and correlation of data about the Internet activities of a particular user, computer, or device, over time and across non-commonly branded websites, for any purpose other than fraud prevention or compliance with law enforcement requests."[1] *The CDT's proposal underlines how critical it is to the definition of "tracking" that the term involves more than simply collecting data*. Rather, tracking must involve some affirmative step taken with the data to reveal some further information about the user, or to target that user for future advertisements or personalization.

Even still, *no* definition of tracking is appropriate in this technical specification. Defining "tracking" is necessarily a policy issue, and should be undertaken in the later policy documents, following full and vigorous discussion. In fact, the W3C acknowledges in its explanatory memorandum accompanying its policy document entitled "What Base Text to

[1] Justin Brookman, *What Does "Do Not Track" Mean?, A Scoping Proposal by the Center for Democracy and Technology*, January 31, 2011. http://www.cdt.org/files/pdfs/CDT-DNT-Report.pdf.

Use for the Do Not Track Compliance Specification" that "many public discussions about the Do Not Track standard have stated the main disagreement as 'Do Not Target vs. Do Not Collect.'" In the same document, the W3C rejects the DAA's proposed definition of tracking because it is too narrow, and does not include collection.

Moreover, defining "tracking" is simply unnecessary for the technical specification. A server does not need to know whether the party is a first or third party in order to respond, because "first party" and "third party" are compliance definitions, not technical definitions. In sum, the TPWG's definition of "tracking" should be removed from the technical specification to better reflect the scope of a technical specification.

B. Definition of Third Parties

The TPWG's definition of "third parties" is similarly skewed and technically improper. The definition reads: "For any data collected as a result of one or more network interactions resulting from a user's action, a third party is any party other than that user, a first party for that user action, or a service provider acting on behalf of either that user or that first party." Notably, the definition specifically *excludes* service providers, a group that fits squarely within the parameters of "third party." All third parties necessarily act as service providers when they provide services to ad publishers. For example, a site may pay for PubMatic to offer up the site's collected user data segments for sale to other digital advertising players. Is PubMatic a "third party" or a "service provider"? We think that we're operating in the capacity of a service provider, but that term is undefined, so it's hard to tell.

Such a flawed definition creates difficulty for service providers like PubMatic. We cannot perform the service we are hired for if a user has DNT:1 enabled, even when that user has consented to the site's terms of use, if we are considered a "third party." Thus, the TPWG's definition of "third party" exhibits a preference for leaving service providers out of the definition, a preference that yields no value other than to complicate the technical specification. As noted above, because a server does not need to know whether a party is a "first" or "third" party in order to respond, this definition need not be included at all. If it is included, it must be amended so that service providers such as PubMatic are better represented and informed as to their DNT obligations.

C. Notice-and-Choice Mechanism is Not Value Neutral

While PubMatic commends the TPWG's requirement that users make an affirmative choice to not be tracked, it believes the specification inappropriately weakens that requirement in a variety of circumstances. It is crucial that any interpretation of user preference expression maintain as much of a value-neutral quality as possible. Such a quality would be best

reflected by a notice-and-choice mechanism that gives the user no "push" in either direction, whether towards DNT:1 (a preference against tracking) or DNT:0 (a preference for tracking). The TPWG recommends a mechanism that does just the opposite, giving the user a "push" towards the choice of DNT:1, meaning the user prefers not to be tracked, even in the absence of an expressed preference. The Group wrote that their goal was "to be able to explain what it means to *turn on DNT* to users with widely varying levels or [sic] technical sophistication" (emphasis added). The TPWG openly admits that it is seeks to achieve a broad standard by which consumers can easily, and consistently, choose not to be tracked. A group with such a clear agenda cannot be best suited to issue a value-neutral technical recommendation.

Indeed, it is clear that this agenda permeates the spirit of the technical specification. For example, in Section 4, the TPWG writes that "a user agent MUST offer users a minimum of two alternative choices for a "Do Not Track" preference: *unset* or *DNT:1*. A user agent MAY offer a third alternative choice: *DNT:0*." Such a requirement makes it *mandatory* for user agents to offer users the preference to not be tracked (DNT:1) but *does not make it mandatory* to offer the choice to be tracked (DNT:0). Such an unbalanced rule indicates that the TPWG believes that it is more important for users to have the option to enable DNT than to disable it. Similarly, in Section 5.1, the specification reads, "servers may interpret the lack of an expressed tracking preference as they find most appropriate for the given user, particularly when considered in light of the user's privacy expectations and cultural circumstances." It is well outside the realm of technical specifications to engage in speculation as to what a user's personal expectations and cultural circumstances are. Further, it is an immense and irrational burden to place on servers that has no purpose other than to place a thumb on the DNT:1 scale.

Another concern is that, although the TPWG prohibits any intermediary or agent other than the user from setting a DNT preference expression, a party receiving a DNT signal is not able to discern who set the signal. Therefore, a DNT:1 signal set by an intermediary such as a router, proxy, or anti-virus software, may be honored when the user's true preference is DNT:0. Thus, though the TPWG wishes that the signal reflect solely the user's informed choice, the technical spec does not require that. PubMatic is concerned about the very real possibility that these intermediate services might see it as an advantage to advertise that they insert a DNT:1 signal on behalf of their users, as a type of privacy protection. In reality, this would be a disservice to users who have consciously chosen a preference expression, and would impede the ability of servers to accurately read users' preferences.

Similar concerns arise in Section 6 of the specification. Section 6.2.7 instructs that a tracking status of *p* (potential consent) "means that the origin server does not know, in real-time, whether it has received prior consent for tracking this user, user agent, or device, but promises not to use or share any DNT:1 data until such consent has been determined." An

origin server that sends a *p* tracking status value must provide a link to a resource for obtaining consent status. Again, the fact that the TPWG requires an additional link for obtaining consent status indicates that the Group believes that if the user simply knew he had a choice, he would choose not to be tracked. This is a policy preference and has no place in a technical specification. The same can be said for the language in Section 6.5.9: "If the tracking status value indicates prior consent (*c*), the origin server must send a *config* property referencing a resource that describes how such consent is established and how to revoke that consent." Again, the requirement that an origin server must give the user an option to revoke consent, when there is no similar requirement for revoking a preference for not tracking, indicates a policy choice in favor of not tracking. PubMatic believes that a tracking status of *r* ("refer to our privacy policy or our compliance specification") should be an available option as well. Since the compliance regime states exactly what the site does with regards to user data, the *r* value would increase transparency and provide more complete information than other tracking value options.

Last, in Section 6.5.3, the TPWG requires that origin servers identify the compliance regimes they adhere to. While increasing communication in this way is commendable, the TPWG's policy recommendation follows: "Communicating such a claim of compliance is presumed to increase transparency, which might influence a user's decisions or configurations regarding allowed tracking, but does not have any direct impact on this protocol." This type of language belongs in the policy-oriented compliance document. It is beyond the scope of the technical specification to presume that this practice will influence users' decisions or configurations. The specification is meant only to shed light on the best way to interpret a user's already-indicated decision or configuration, if one should exist.[2]

The most important property of a notice-and-choice mechanism is its value-neutrality, so that users can exercise a meaningful choice. It is all too clear in the text of the technical specification that the TPWG has an interest in influencing users to choose DNT:1, which undermines the integrity of the mechanism as a whole.

D. Undue Limitations on DNT:0 Preference Expression

The TPWG continues its push to persuade users to choose DNT:1 by making it difficult for a user to express a preference for DNT:0 after choosing DNT:1, and by creating limitations on

[2] The technical specification also yields confusion over what to do with conflicting DNT preference expressions. For example, a site may obtain consent from a user to track that user and provide the user's information to a third party, based on the user's agreement to the site's terms and conditions. If the third party then receives a DNT:1 signal from the user, it is faced with a decision as to which tracking expression preference it should honor. The technical specification does not provide guidance as to which preference trumps: the DNT:1 signal, or the user-provided consent.

how exceptions to the choice to enable DNT may be used, imposing undue burdens on service providers. Again, this underlines the TPWG's policy stance that "if users only knew – they would choose properly," with the "proper" choice being to choose DNT:1. This viewpoint prevents the technical specification from presenting the responses to user preferences in a balanced, value-neutral way.

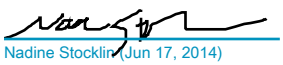
For example, Section 7.6 specifies that if a user sends a tracking exception to an origin server and a third party, the third party will receive the DNT:0 signal, and may track the user and collect or process the data. However, the third party may only transmit the collected data for uses related to that specific interaction to its own sub-services. There is no means to express a preference to the contrary. The specification reads, "the sub-services to the named third party do not acquire an independent right to process the data for independent secondary uses unless they, themselves, receive a DNT:0 header from the user agent." Further, the exception only extends to one level of third parties, creating an issue for third parties, like PubMatic, who service relies on working with demand partners and technology partners, which involves little, if any, privacy implications for consumers, but which handicaps an entire portion of the as serving industry. If the exception is not extended to each partner, it cannot be meaningfully employed by PubMatic. Thus, PubMatic and other third party service providers are forced to check if each demand partner and technology partner is included in the exception, or to forego use of that exception. These limitations on how a tracking exception can be used and what parties can honor it impose heavy burdens on third parties and sub-services even when the origin server has received a clear DNT:0 signal.

Similarly, Section 7.7 states "it is the responsibility solely of the site making the call to determine that an exception grant reflects the user's informed consent at the time of the call. It is expected that the site will explain, in its online content, the need for an exception, and the consequences of granting or denying an exception, to the user." For example, the TPWG suggests inserting an "infobar stating 'Example News (news.example.com) has indicated to Browser that you have consented to granting it exceptions to your general Do Not Track preference. If you believe this is incorrect, click Revoke." Again, placing additional warnings and notices about a potential or granted exception indicates that the TPWG sees tracking as a danger and exceptions to DNT as something to watch carefully. This policy slant has no place in a technical specification.

As a whole, the TPWG's Working Draft indicates a clear preference for, and enables user agents to, influence consumers' Do Not Track decisions. That is not a technical specification, but rather an embedded authorization for user agents to manipulate consumers on a public policy issue. Where this enablement exists (as we have noted above), it should be excised from the technical specification. The TPWG should also reexamine and amend its definitions of "tracking," "first party," and "third party." From a technical standpoint, the

definitions are flawed and misleading, and creates impediments for service providers like PubMatic to comply with the proposed specification. From a policy standpoint, the commentary and preferential lean embedded in the definitions have no place in the technical specification and should be excised. PubMatic respectfully submits these comments and urges the W3C, and the TPWG, to reevaluate their Working Draft in light of these considerations.

Sincerely,



Nadine Stocklin, Esq.
General Counsel, PubMatic, Inc.

PubMatic

305 Main Street, 1st floor
Redwood City, CA 94063

June 17, 2014

Via Email to public-tracking-comments@w3.org
Tracking Protection Working Group
W3C

Re: Comments on Tracking Preference Expression (DNT) W3C Last Call Working Draft 24 April 2014

To Whom It May Concern,

PubMatic submits these comments in connection with the Last Call Working Draft entitled "Tracking Preference Expression" (DNT), which was published on April 24, 2014.

PubMatic's mission is to enable publishers to realize the full potential of their digital assets. Since its founding in 2006, the company has offered publishers innovative, industry-changing products, services and systems to help optimize the potential of their digital assets. PubMatic is consistently one of the first to market new products and services, including yield optimization for publishers across ad networks, real-time bidding (RTB), audience data analytics, and unified revenue optimization packages.

The W3C, and in particular, the Tracking Protection Working Group ("TPWG"), has invited broad community review of their Working Draft, especially of "technical requirements and dependencies." The Group encourages reviewers to identify technical problems with the draft, and to point out where it fails to further goals of user privacy and user control. As an industry leader in programmatic digital advertising, PubMatic is uniquely qualified to represent the views of many in the digital advertising industry on these topics.

PubMatic applauds the work done by the TPWG in moving toward a workable technical specification for a DNT expression. This has proven to be a difficult process, and we commend the members of the Working Group for their efforts. Ultimately, however, we believe that the Draft reveals, once again, the difficulty with applying the TPWG's technical expertise to public policy issues. The important issues surrounding consumer privacy, and in

PM comments to W3C Tech Specs FINAL

EchoSign Document History June 17, 2014

Created:	June 17, 2014
By:	Nadine Stocklin (nadine.stocklin@pubmatic.com)
Status:	SIGNED
Transaction ID:	XAKGAUC7X4IX644

“PM comments to W3C Tech Specs FINAL” History

Document created by Nadine Stocklin (nadine.stocklin@pubmatic.com)
June 17, 2014 - 2:17 PM PDT - IP address: 173.228.51.146

Document e-signed by Nadine Stocklin (nadine.stocklin@pubmatic.com)
Signature Date: June 17, 2014 - 2:20 PM PDT - Time Source: server - IP address: 173.228.51.146

Signed document emailed to Brynn Ursa (brynn.ursa@pubmatic.com) and Nadine Stocklin (nadine.stocklin@pubmatic.com)
June 17, 2014 - 2:20 PM PDT