Responsibility for the compliance of add-ons

In this Call for Objections the Tracking Protection Working Group was asked, whether to include in the TPE specification an additional sentence on the responsibility for add-on compliance.

The CfO was set up to solve and close the ISSUE-153: What are the implications on software that changes requests but does not necessarily initiate them? (https://www.w3.org/2011/tracking-protection/track/issues/153).

The Co-Chairs evaluated the group's inputs to this Call for Objections and found that Option A received more substantiated objections and that Option B is determined as group consensus for ISSUE-153.

The Call for Objections was open from January 15, 2014 to January 29, 2014. In total 9 members of the Working Group participated and presented arguments against or in favor of the two options. The full results of the questionnaire are public at https://www.w3.org/2002/09/wbs/49311/tpwg-addons-153/results.

The Options

1. Option A: **editors' draft text**

   A user agent MUST have a default tracking preference of unset (not enabled) unless a specific tracking preference is implied by the decision to use that agent. For example, use of a general-purpose browser would not imply a tracking preference when invoked normally as "SuperFred", but might imply a preference if invoked as "SuperDoNotTrack" or "UltraPrivacyFred". Likewise, a user agent extension or add-on MUST NOT alter the tracking preference unless the act of installing and enabling that extension or add-on is an explicit choice by the user for that tracking preference.

   A user agent extension or add-on MUST NOT alter the user's tracking preference setting unless it complies with the requirements in this document, including but not limited to this section (Determining a User Preference). Software outside of the user agent that causes a DNT header to be sent (or causes existing headers to be modified) MUST NOT do so without ensuring that the requirements of this section are met; such software also MUST ensure the transmitted preference reflects the individual user's preference.

2. Option B: **UA that permits add-ons jointly responsible**

   Add to current language:

   A user agent that permits an extension or plug-in to configure or inject a DNT header is jointly responsible, with the plug-in or extension, for ensuring compliance to the extent possible.

Explanatory considerations on the choice of definition

The proposed options differed only in the additional sentence of Option B, stating a joint responsibility for the user agent and the add-on sending the DNT header.

The decision was based on the substance of the objections against each option. The goal was to identify the option with the least substantiated objections. After evaluating the Working Group's inputs, we determined that Option A received more substantial objections and that B is determined as group consensus for ISSUE-153.

Objections against Option A:

Option A did not receive objections against the editors' draft text itself but against keeping the text without the extension of Option B. The majority of participants voiced the concern that Option A would not adequately ensure the compliance of add-ons and weaken the confidence in the DNT signal.

Shane Wiley wrote: "I strongly oppose this option. This approach opens the door for non-compliant bad actors to inject DNT signals in an unchecked and undiscoverable manner (no way to detect who the setter was in the current architecture). If we desire industry adoption and healthy implementation rates, Servers must be provided some level of confidence that DNT signals are set by users through appropriate disclosure and meaningful control."

We consider the argument of weakened confidence in the DNT signal as a substantial one. For the server side it will not always be transparent, whether the DNT signal was sent by the user agent or a (potentially noncompliant) add-on. If the introduced joint responsibility of user agent and add-on could strengthen the recipient's confidence in the DNT signal to reflect the user preference, it would be a benefit for the future adaption of the TPE.

Several other participants raised similar objections against Option A. Chris Mejia wrote: "When it comes to user choice, I believe it would be irresponsible to hinge the decision of whether an informed choice was made explicitly by the user, on a standard that allows for the user agent to decide (for the user) that it is "implied" that using that agent indicates that DNT should equal 1 by default-- that's far too subjective. We should absolutely require that the user make this setting themselves (in ANY agent that affects the sending of DNT header signals); that they express their choice directly and explicitly via a setting mechanism that must be changed from the default state of un-set. I believe it's necessary to ensure that browser plug-ins and browser extensions are held to the same compliance standard and requirements as the browser itself. Otherwise, plug-ins or extensions could be used to manipulate a user's tracking preference signal, without the user having made an informed and educated choice, or without even notifying the user of the change."

Likewise, Berin Szoka objected to Option A: "In theory, this option seems reasonable. But in practice, it seems likely that this option will allow non-compliant user agents to game the system by having the authority to decide when a user preference to turn on DNT is 'implied by the decision to use that agent.' I do not see how that part of the standard could be given practical effect: what would stop a user agent from simply asserting that their users wanted DNT on? Is this not what Microsoft, for instance, has already done with its 'general-purpose browser?' Given this reality, this option could derail the entire consensus upon which DNT rests and thus seriously undermine industry adoption of the standard. Against that cost, the relatively minor hassle of having to check a box to turn on DNT after setting up / adding a privacy-friendly user agent seems relatively trivial and well-worthwhile. We cannot expect the DNT standard to be completely costless to users."

Jeff Wilson wrote: “We object to option A. What might ‘imply’ a preference is subjective. Experiences will be unpredictable and inconsistent, and tracking options will likely be set without informed choice.”

Other participants explicitly voiced their preference for Option B over Option A.

Jack Hobaugh wrote: “Option B is necessary to insure that to the extent possible, browser plug-ins and browser extensions are held to the same degree of compliance with the TPE as is the user agent itself. Without such language, plug-ins or extensions could be used to circumvent compliance with the TPE.”

Mike O’Neill stated to prefer Option B “because it encourages browsers and add-ons to co-operate in offering a user more control over tracking, but without trying to limit the ability of add-ons to change headers.”

Objections against Option B:

The arguments against Option B were comparatively minor. Two participants raised concerns that the additional sentence of Option B would add “unnecessary legalese” to the technical TPE specification.

Walter van Holst wrote: “This option adds unnecessary legalese to a technical specification. The editor's draft is, despite being somewhat more verbose, clear to implementers. Also, this option is ambiguous in the sense that it can be interpreted as an obligation to UAs to police their extensions, which is not conductive to an open web.”

Rob van Eijk argued that the extra sentence belonged in the TCS specification instead of the TPE. “Although the issue is opened against the TPE, I object to this draft text. Because of the purpose of this CFO, which is to get us nearer to Last Call status, the nature of 'getting to a close' is about how much the TPE document needs to stand on itself. For that reason, some of the key definitions are ported over from the compliance document.
I object, because these paragraphs belong in the compliance document, not in the TPE. Normative requirements about the default setting of a user agent and/or user agent extention are at the core of the question what tracking means in a W3C DNT standard. The answer to that question should be dealt with in the compliance document, not in the technical protocol specification i.e., TPE.
I also object because a TPE without this draft text can be used just fine for testing and implementation. The draft text does not add anything that would make testing and implementation impossible.”

While we agree that unnecessary compliance or policy requirements should not be included in the technical specification, the arguments of other participants pro Option B and in objection to Option A indicated substantial benefits by the addition of Option B to the specification. Moreover, the TPE always includes substantive requirements on user agents to ensure that a DNT request reflects the intention of the user. Several participants pointed out that Option B could reduce the risk of non-compliant behavior of add-ons and strengthen the confidence in the DNT signal.

One of the participants supporting Option B is Shane Wiley: “It's critical that appropriate technical support mechanisms, where possible, be leveraged to reduce the likelihood of bad actors falsifying user preference signals. This approach provides the most balanced and thoughtful approach to a weak technical architecture that can be easily abused by bad actors. It's for this reason that this language appropriately belongs in the TPE."

Similarly, Chris Mejia underlined the potential benefits of Option B: "I believe it's necessary to ensure that browser plug-ins and browser extensions are held to the same compliance standard and requirements as the browser itself. Otherwise, plug-ins or extensions could be used to manipulate a user's tracking preference signal, without the user having made an informed and educated choice, or without even notifying the user of the change."

Brad Kulick seconded these benefits with regard to the recipient's confidence in the DNT signal: „I strongly support reasonable efforts, such as this, that continue to support the balance in the application of this technical specification. User agents (UA) provide platforms by which extensions or plugins can be built to do a variety of tasks, including altering user DNT signals. Unfortunately, extensions' and plug-ins' alterations of DNT settings are not transparent and, therefore, open for unchecked abuse. Coupling responsibility to the parties that provide the platform for such access to DNT signal modification, and who are visible participants, fosters a more compliant ecosystem with which a greater confidence in DNT signals can be placed."

Jeff Wilson wrote, that this Option "is more likely to provide a consistent experience and ensure that the preference is explicitly set by the user. Reliable signals are more likely to be honored."

With regard to these comments supportive of Option B, the objection of unnecessary compliance text has to be deemed less substantiated. While Walter van Holst's concern that the text proposal could lead to the obligation to user agents to "police" their add-ons, we believe that this risk is reduced by the extension "to the extent possible". While the introduced joint responsibility needs to be specified by an accompanying Compliance document, the high-level requirement for user agents and add-ons to jointly safeguard that a DNT signal is sent according to the user's preferences does not exceed the scope of the technical TPE spec. We expect early implementation feedback to provide more insights on how stakeholders deal with this joint responsibility.

Result

In conclusion, the ISSUE-153: What are the implications on software that changes requests but does not necessarily initiate them? (https://www.w3.org/2011/tracking-protection/track/issues/153) is hereby closed, and the following definition represents the Working Group's consensus:

> A user agent MUST have a default tracking preference of unset (not enabled) unless a specific tracking preference is implied by the decision to use that agent. For example, use of a general-purpose browser would not imply a tracking preference when invoked normally as "SuperFred", but might imply a preference if invoked as "SuperDoNotTrack" or "UltraPrivacyFred". Likewise, a user agent extension or add-on MUST NOT alter the tracking preference unless the act of installing and enabling that extension or add-on is an explicit choice by the user for that tracking preference.
>
> A user agent extension or add-on MUST NOT alter the user's tracking preference setting unless it complies with the requirements in this document, including but not limited to this section (Determining a User Preference). Software outside of the user agent that causes a DNT header to be sent (or causes existing headers to be modified) MUST NOT do so without ensuring that the requirements of this section are met; such software also MUST ensure the transmitted preference reflects the individual user's preference.

A user agent that permits an extension or plug-in to configure or inject a DNT header is jointly responsible, with the plug-in or extension, for ensuring compliance to the extent possible.