User Interface / Default Issues

Alan Chapell Proposed Text April 3, 2013

5. User Agent Compliance

A user agent *MUST* offer a control to express a tracking preference to third parties. The control *MUST* communicate the user's preference in accordance with the [*TRACKING-DNT*] recommendation and otherwise comply with that recommendation. A user agent *MUST NOT* express a tracking preference for a user unless the user has given express and informed consent to indicate a tracking preference.

While we do not specify how tracking preference choices are offered to the user or how the preference is enabled, each implementation MUST follow the following user interface guidelines:

1.   The User Agent is responsible for determining the user experience by which a tracking preference is enabled. For example, a user might select a check-box in their user agent's configuration, or install an extension or add-on that is specifically designed to add a tracking preference expression so long as the checkbox, extension or add-on otherwise follows these user interface guidelines;

2.   The User Agent MUST ensure that the tracking preference choices are communicated to users clearly and conspicuously, and shown at the time and place the tracking preference choice is made available to auser;

3.   The User Agent MUST ensure that the tracking preference choices accurately describe DNT, including the parties to whom DNT applies, and MUST make available via a link in explanatory text where DNT is enabled to provide more detailed information about DNT functionality.

Non-Normative:

The User Agent plays a key role in enacting the DNT functionality. As a result, it is appropriate for the User Agent to play an equally key role in describing DNT functionality and educating users about DNT in order for this standard to be meaningful.

While the user interface guidelines do not specify the exact presentation to the user, they are intended to help ensure that users understand their choices with respect to DNT. For example, outlining the parties (e.g., First Parties, Service Providers, Third Parties) to whom DNTapplies and using language that a reasonable user is likely to understand is critical for ensuring that users are in position to provide their informed consent to a tracking preference.

Moreover, as DNT functionality is complex, it is important that User Agents educate users about DNT, including but not limited to offering a clearly described link that takes the user to additional information about DNT functionality. For example, given that some parties may chose not to comply with DNT, it would be helpful for browsers to educate users about how to check the response header and/or tokens to see if a server is responding with a "public commitment" of compliance.

Finally, recognizing that DNT settings may be set by non-browser User Agents acting in violation of the user interface guidelines, the browsers should take reasonable steps to ensure that DNT settings are valid.

Shane's proposal has suggested the additional compliance requirements of user agents:
1. The User Agent must also make available via a link in explanatory text where DNT is enabled to provide more detailed information about DNT functionality
2. Any User Agent claiming compliance must have a functional implementation of the browser exceptions in this specification

Adrian Bateman Proposed Text April 10, 2013

I want to emphasise that we still support Option 2 (http://www.w3.org/2011/tracking-protection/drafts/tracking-compliance.html#def-consent-silence) leaving the definition of consent to local laws.

I offer the following text for consideration as an alternative to Alan's proposal:

5. User Preferences

User agents and web sites MUST obtain express and informed consent when setting controls that affect the tracking preference expression. The controls *MUST* communicate the user's preference in accordance with the [*TRACKING-DNT*] recommendation.

User agents and web sites offering tracking preference choices to users MUST follow the following user interface guidelines:

1.   User agents and web sites are responsible for determining the user experience by which a tracking preference is controlled;

2.   User agents and web sites MUST ensure that tracking preference choices are communicated to users clearly and accurately and shown at the time and place the tracking preference choice is made available to a user;

3.   User agents and web sites SHOULD ensure that the tracking preference choices describe the parties to whom DNT applies and SHOULD make available explanatory text to provide more detailed information about DNT functionality.

Tracking Preference Expression April 30, 2013

- **Language has not changed since Oct. 2, 2012**

http://www.w3.org/2011/tracking-protection/drafts/tracking-dnt.html#determining

3. Determining User Preference

The goal of this protocol is to allow a user to express their personal preference regarding tracking to each server and web application that they communicate with via HTTP, thereby allowing each service to either adjust their behavior to meet the user's expectations or reach a separate agreement with the user to satisfy all parties.

Key to that notion of expression is that the signal sent *MUST* reflect the user's preference, not the choice of some vendor, institution, site, or any network-imposed mechanism outside the user's control; this applies equally to both the general preference and exceptions. The basic principle is that a tracking preference expression is only transmitted when it reflects a deliberate choice by the user. In the absence of user choice, there is no tracking preference expressed.

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.

If the user's choice is DNT:1 or DNT:0, the tracking preference is *enabled*; otherwise, the tracking preference is *not enabled*.

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.

We do not specify how tracking preference choices are offered to the user or how the preference is enabled: each implementation is responsible for determining the user experience by which a tracking preference is enabled. For example, a user might select a check-box in their user agent's configuration, install an extension or add-on that is specifically designed to add a tracking preference expression, or make a choice for privacy that then implicitly includes a tracking preference (e.g., Privacy settings: high). The user-agent might ask the user for their preference during startup, perhaps on first use or after an update adds the tracking protection feature. Likewise, a user might install or configure a proxy to add the expression to their own outgoing requests.

Although some controlled network environments, such as public access terminals or managed corporate intranets, might impose restrictions on the use or configuration of installed user agents, such that a user might only have access to user agents with a predetermined preference enabled, the user is at least able to choose whether to make use of those user agents. In contrast, if a user brings their own Web-enabled device to a library or cafe with wireless Internet access, the expectation will be that their chosen user agent and personal preferences regarding Web site behavior will not be altered by the network environment, aside from blanket limitations on what resources can or cannot be accessed through that network. Implementations of HTTP that are not under control of the user *MUST NOT* generate or modify a tracking preference.

4. Expressing a Tracking Preference

4.1 Expression Format

. . . A user agent *MUST NOT* send a tracking preference expression if a tracking preference is not enabled. This means that no expression is sent for each of the following cases:

- the user agent does not implement this protocol;
- the user has not yet made a choice for a specific preference; or,
- the user has chosen not to transmit a preference.

In the absence of regulatory, legal, or other requirements, 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. Likewise, servers might make use of other preference information outside the scope of this protocol, such as site-specific user preferences or third-party registration services, to inform or adjust their behavior when no explicit preference is expressed via this protocol.

4.2 DNT Header Field for HTTP Requests

. . . A user agent *MUST* send the *DNT* header field on all HTTP requests if (and only if) a tracking preference is enabled. A user agent *MUST NOT* send the DNT header field if a tracking preference is not enabled.

. . . An HTTP intermediary *MUST NOT* add, delete, or modify the DNT header field in requests forwarded through that intermediary unless that intermediary has been specifically installed or configured to do so by the user making the requests. For example, an Internet Service Provider *MUST NOT* inject DNT: 1 on behalf of all of their users who have not expressed a preference.

ISSUE-4: What is the default for DNT in client configuration (opt-in or opt-out)? (Closed)

http://www.w3.org/2011/tracking-protection/track/issues/4

Thomas Lowenthal, 26 Oct 2011, 16:39:25 Resolved by consensus on Oct 26 call. Out of scope: user presentation issue.

December 21, 2011:

http://www.w3.org/2011/12/21-dnt-minutes

PROPOSED LANGUAGE in FPWD:

<aleecia> The goal of this protocol is to allow a user to express their personal preference regarding cross-site tracking to each server and web application that they communicate with via HTTP, thereby allowing each server to either adjust their behavior to meet the user's expectations or reach a separate agreement with the user to satisfy both parties. Key to that notion of expression is that it must reflect the user's preference, not the preference of some institutional or network-imposed mechanism outside the user's control.

The remainder of this specification defines the protocol in terms of whether DNT is enabled or not enabled. We do not specify how that preference is configured: the user agent is responsible for determining the user experience by which this preference is set.

For example, a user might configure their own user agent to tell servers "do not track me cross-site", install a plug-in or extension that is specifically designed to add that expression, or make a choice for privacy that then implicitly includes a tracking preference (e.g., "Privacy settings: high"). For each of these cases, we say that DNT is enabled.

- *jmayer:* language should be one on user agents, and one on institution or proxy. Renaming these issues to be clearer. ... Want to make clear, for what it's worth, don't have my support on issue-4. Don't see it as necessarily about user expression... without getting into that debate now, let's make that an explicit issue.
- *schunter:* closing issue-4
- *roy:* If DNT: 1 isn't a user preference, I'm going to ignore it.
- *schunter1:* If a company puts on DNT for employees, servers should honor that.
- *roy:* Might allow from small companies, not large companies.
- *schunter1:* Closed Issue 4, moved to Issue 13.

Clarifying Issues

May 30, 2012:

http://www.w3.org/2012/05/30-dnt-minutes#item09

- *aleecia:* What motivates this is we talked about intermediaries. The user agent should convey the user's voice... is it okay to have a default of DNT:1 or DNT:0. Example of AVG

- *<WileyS>* I've submitted an issue for User Agents to record that they were the party to set the DNT:1 signal and this be conveyed in the header. This provides transparency for the sender.
- *aleecia:* another issue, unsure to take this up: What about the browser DNT setting contradicting the setting of addons?
- *<jmayer>* Another issue we have to decide: can a server ignore "DNT: 1" if it has reason to believe it wasn't explicitly set? I think the answer there should be plainly no.
- *aleecia:* We have DNT 1, 0 or unset. Do we want to take on how UA should present this choice to the user?

June 6, 2012: Default Issue:

http://www.w3.org/2012/06/06-dnt-minutes#item03

- *<aleecia>* PROPOSED: there must be user choice, which can include choosing a privacy-protecting setting (e.g. slider) or the UA itself (e.g privateBrowser)
- *<dsinger>* can we check whether Roy's text reflects the consensus?
- *Aleecia:* I am not hearing any dissent on this point
- *<jmayer>* I strongly disagree that this was a consensus view.
    o *<jmayer>* But I'm willing to compromise.
- *suegl:* We do think that DNT is something you could have a default setting on
- *BerinSzoka:* It seems like, from this conversation, that resolving this issue requires bringing some of the UI design into scope
- *Aleecia:* No, that's out of scope by charter
- *rvaneijk:* I also would like to [..] possibility of a user interacting with a startup flow, if so, then I would be happy
- *<rigo>* roy, would your mind change if there is an interaction as Rob suggested?
- *<fielding>* Rigo, not if it was asked when installing the operating system. If it was asked on first use by a real user, yes
- *jchester2:* Want to say that I support the compromise saying that the default is not in fact setting DNT, but with the hope of resolving this with a package that protects privacy. ... in the absence of adopting a final package, giving up a consumer right ot have DNT1 as a default should be there. I support this in the context of the compromise.
- *Aleecia:* As chair, I am calling this a consensus. Roy did a good job of starting the text, I will take an action to flesh that text out. It will belong in the compliance doc, we will post it to the mailing list to discuss.
- *Aleecia:* is being an AVG user sufficient to be consent? What general guidance can we give here?
- Aleecia: What happens when a UA does not comply with what we have for a specification?

Issue-2: What is the meaning of DNT (Do Not Track) header? (Closed)

http://www.w3.org/2011/tracking-protection/track/issues/2

ISSUE-78: What is the difference between absence of DNT request header and DNT = 0? (Closed)

http://www.w3.org/2011/tracking-protection/track/issues/78

JC Cannon:

http://lists.w3.org/Archives/Public/public-tracking/2011Dec/0170.html

I like Sid's approach now that the use of "no header" has been explained. It certainly seems like no header should be the proper default.
Here's the way I think about the difference between DNT:0 and no header:

Sid Stamm:

http://lists.w3.org/Archives/Public/public-tracking/2011Dec/0169.html

DNT:0 means "you can track me", regardless of the society or jurisdiction, it is explicit consent. In places where the social norms accept tracking for people who haven't been asked (USA), DNT:0 is equal to no header. In places where social norms reject tracking for people who haven't explicitly provided informed consent (UK), DNT:1 is equal to no header.

Because header seems to be socially-centered or perhaps based on jurisdiction, I'm advocating that lack of header means "whatever society accepts because the individual hasn't weighed in" and the presence of the header is an explicit request one way or the other.

If it clears things up, perhaps we could add a third value that means the same thing as no header. Then we would have:

0: User accepts tracking
1: User rejects tracking
2: User's preference undefined

But if that's the case, it seems to me that implementing the third option (2 here) should be optional for user agents -- to save bytes we could just not send the header if the user's preference hasn't been established or discovered.

ISSUE-81: Do we need a response at all from server? (Closed)

http://www.w3.org/2011/tracking-protection/track/actions/13

Matthias Schunter:

http://lists.w3.org/Archives/Public/public-tracking/2012Jan/0198.html

A site that receives DNT;1 MUST follow the corresponding practices as defined in the [standards compliance] document and SHOULD send a corresponding DNT response header.

Note: If a site chooses not to send a response header, then the user agent does not obtain information whether the preference has been accepted or not. This may have negative consequences for the site such as:
 - Preventive measures by user agents
 - Being flagged as non-compliant by scanning tools that look for response headers

Vincent Toubiana:
http://lists.w3.org/Archives/Public/public-tracking/2012Jan/0202.html

I still think that the site "MUST send a corresponding DNT response header" otherwise website could stop respecting DNT without users being aware of it.

ISSUE-95: May an institution or network provider set a tracking preference for a user? (Closed)

http://www.w3.org/2011/tracking-protection/track/issues/95

TPE (20 Jan 2012) says

Key to that notion of expression is that it must reflect the user's preference, not the preference of some institutional or network-imposed mechanism outside the user's control. Although some controlled network environments, such as public access terminals or managed corporate intranets, might impose restrictions on the use or configuration of installed user agents, such that a user might only have access to user agents with a predetermined preference enabled, the user is at least able to choose whether to make use of those user agents. In contrast, if a user brings their own Web-enabled device to a library or cafe with wireless Internet access, the expectation will be that their chosen user agent and personal preferences regarding Web site behavior will not be altered by the network environment, aside from blanket limitations on what sites can or cannot be accessed through that network.

Roy Fielding, 20 Jan 2012, 21:36:22

Tom Lowenthal

http://lists.w3.org/Archives/Public/public-tracking/2011Nov/0305.html

Alternative text suggestion:

A decision to send a Do Not Track signal SHOULD be based on the affirmatively expressed preference of the user. In general the signal SHOULD only be sent by a user's agent, and SHOULD NOT be modified by any intermediary.

There are some situations where an entity other than the user wishes to express a Do Not Track preference on the user's behalf. Such situations may include those where the user has designated another person as their system's administrator, such as in a shared computing environment like an employer's network, or a public-use computer system like a library. If a non-user wishes to express a Do Not Track preference on a user's behalf, this SHOULD be done by configuring the user's agent to send the desired signal.

Intermediaries to an HTTP(s) connection SHOULD NOT modify, add, or remove a DNT signal sent by a user's agent. There may be limited situations where an intermediary reasonably acts on a user's behalf. If an intermediary modifies or sends a Do Not Track signal on the user's behalf, and that modification or sending does not occur within the user-agent, the scope of such modification should be as limited as possible. Extreme care should be taken to ensure that any modification accurately and completely expresses the user's preference. In particular, the intermediary should take care to avoid disrupting user's site-specific preferences and exceptions, and not to cause undue impact to the user's browsing experience.

NOTE: it is understood that it is very difficult to technically verify or enforce these provisions regarding intermediaries. They are included to express what is and is not appropriate behavior for all participants in the web ecosystem.

Shane Wiley Proposal:

http://lists.w3.org/Archives/Public/public-tracking/2011Nov/0304.html

"Generally, the setting and/or unsetting of a Do Not Track signal SHOULD only be established by a user proactively. Intermediaries to an HTTP/S request SHOULD NOT attempt to modify the DNT signal in any way. There are limited situations where it MAY be appropriate for an intermediary to modify a user's DNT settings on their behalf such as through employer networks

or public networks (libraries, for example). But, care should be taken even in these cases to limit the scope of modification as much as possible to decrease the possible impact to a user's web surfing experience as overriding DNT signals could disrupt content consumption through user granted site-specific exceptions. NOTE - it is understood this particular compliance standard cannot be technically enforced but it should be clear to all web ecosystem participants what the standard baseline is in this matter."
Roy Fielding, 20 Jan 2012, 21:36:22

ISSUE-143: Activating a Tracking Preference must require explicit, informed consent from a user (Raised)

http://www.w3.org/2011/tracking-protection/track/issues/143

Description:

As we've developed draft text for obtaining explicit, informed consent from a user for out-of-bound user granted exceptions, it's equally important that activation of a tracking preference be coupled with the same explicit, informed consent.

For example, activating a tracking preference should require explicit language identifying this as an option and informing the user of the scope of the option's application.

For example, an security software package should NOT activate DNT by default (with an explanation buried deeply in their TOS or help center) and the user must explicitly select this option upon install/use of the product.

Using this same test, I don't believe there is "explicit, informed" consent from users activating DNT within IE9's Traffic Protection Lists and this should be called out when a TPL is activated.

To further support this view, much like response headers allow a party to respond to articulate when they've received out-of-band consent, I request that a similar element be added to request headers. In this model, a new data element would need to be added (perhaps in the extension) for a party to articulate that they have captured a user's consent to activate DNT and identify themselves in this manner as the "capturee" of the consent. It'll be vital that web browser vendors lock down the ability for a 3rd party tool or extension to mimic their signature in this process and only allow 3rd party tools to activate DNT on a user's behalf by articulating who they are.

This way, if industry feels a party is inappropriately setting a tracking preference, we can take steps to discover which headers are coming from this party and take steps to request the party move to an "explicit, informed" consent model prior to honoring the DNT headers coming from the implementation of their tool.

ISSUE-149: Compliance section for user agents (Raised)
http://www.w3.org/2011/tracking-protection/track/issues/149

Description:

> We have some related sub-issues we may need to break out, or perhaps we can do this as one. We will talk as a group to see which of the itemized points below are things we wish to take on. I expect we will need to create a new section in the Compliance document specifically about user agents.

> First, and a motivating factor underlying other issues, we have the example of the AVG anti-spyware package enabling DNT:1 for new users who purchase their product. As a group, we have discussed the idea that users must be making some choice for privacy -- perhaps via slider, or by downloading MyPrivateWebBrowser, or something -- in order for them to send DNT:1. Reasonable people who were part of those discussions are disagreeing as to whether installing AVG counts as a decision for privacy, or not. This is problematic. Whatever decision we make as a group, we need to (a) be clear about it ourselves so we can (b) write it down clearly for others.

> Second, due to multiple addons that support Do Not Track, there could be conflicts. For example, a user could turn off DNT (not unset, actually off, sending DNT:0) in Firefox, yet install Abine's "Do Not Track Plus" addon (which sends DNT:1). More fun, users could have three different addons, each with a different value. Do we have either best practices or requirements for user agents here?

> Third, while we have documented DNT as being on / off / unset, do we want to write that as a requirement for user agents? User interface is out of scope by charter, but we could require user agents to offer all three options. Currently we only state all three are possible values (which we do document well.)

> Finally, we have issue-143 against the TPE document that is at least somewhat a compliance issue as well, around informed consent and browser choices. This is tied into many of the issues above. We may wish to add a new issue, or move issue-143 to a compliance issue for the time being, or neither.

August 2012 Call for Objections: (Issue 149)

https://www.w3.org/2002/09/wbs/49311/tripart/

1. Tri-part choice requirement for user agents

Should we add a requirement that compliant user agents must provide functionality for sending DNT:0 as well as DNT:1 and unset, and require that all options be equally easy to exercise in the interface?

Option A: Silence

(Keep just the existing text that MUST reflect the user's preference etc. User agents -- general purpose browsers or extensions -- do not have to provide a DNT:0 option that is equally easy to turn on as DNT:1.)

3. Objections to Option B: Three choices with equal effort

Option B: A user agent MUST require equal effort to configure their agent to each of a minimum of three choices for a Do Not Track preference: 1, 0 or unset.

Results:

https://www.w3.org/2002/09/wbs/49311/tripart/results

Decision:
http://lists.w3.org/Archives/Public/public-tracking/2012Sep/0197.html

Based on the inputs at hand and our analysis in this document, we conclude that silence, i.e., not mandating a 3-state user interface, drew the least strong substantive objections from the Working Group. This decision is based on the following arguments that are derived from the submitted data.

      • Biased User Agents: We understand the substantial concern that user agents may be biased and we believe that mitigating this concern is very important. However, we believe that mandating a 3-state user interface does not address the concerns unless a full UI is specified, which we cannot do by charter. Even with 3 options, these options may still be misrepresented and may lead to a biased UI.

      • UA Differentiation and Innovation: The ability for user agents to innovate and differentiate is a major component in identifying the least strong objection for several reasons:
            Privacy advocates as well as advertisers will benefit from UI innovations and from differentiations. As a consequence, we expect manufacturers of user agents to build the best possible and unbiased tools for collecting user preferences.
            Minimizing the restrictions on implementers will enable more and simpler user agent implementations.
            We aim for segmentation of the market and targeting of user agents. I.e., depending on the preferences of a particular user, the user may choose the right user agent.
            User agents are in the best position to understand how best to gather a user's preference.

      • Ability to Express Preferences: Our standard aims at expressing user preferences, which makes this a high concern. While this was used as an argument for 3-state agents, the evidence did not establish that a single approach to user agents (as compared to an ecosystem of targeted user agents for different segments) is the right and only way forward. As a consequence, we believe that it is likely that users will partially express their preference by selecting the "right" user agent for their needs.

• Testability against spec: We should aim for a testable recommendation as much as possible, and consider this of medium importance. While the existence (or lack there of) of a 3-state user interface is easily testable, participants stated that statements such as an unbiased presentation or "similar effort" are difficult to test.

October 4, 2012
Formal Objection to the TPWG Chairs' Decision Regarding A "Tri-part choice requirement for users agents."

http://lists.w3.org/Archives/Public/public-tracking/2012Oct/0104.html

ISSUE-150: DNT conflicts from multiple user agents (Raised)
Jonathan Mayer
http://lists.w3.org/Archives/Public/public-tracking/2012Oct/0187.html

Proposed text on duplicate headers:

If a server receives duplicate DNT headers, it MUST act as if it had received a single DNT header.

Proposed text on conflicting headers:

If a server receives conflicting DNT headers, it MUST act as if it had received a single DNT: 1 header. It is a best practice for the server to alert the user about possible user agent misconfiguration.

June 20, 2012 Meeting:
http://www.w3.org/2012/06/20-dnt-minutes#item06

Issue 150:

- *<aleecia>* A given device may have multiple sources of user preferences, for example a browser could have a DNT user setting, plus an add-on or plug-in could have a DNT user setting. One DNT choice must be sent. We do not specify how conflicts are resolved.
- *<trackbot>* ISSUE-150 -- DNT conflicts from multiple user agents – raised
- Amsterdamn: http://www.w3.org/2012/10/03-dnt-minutes
- going to close 150 with: up to the browsers to resolve DNT conflicts beween multiple plugins

Issue 143:

- *ifette:* what about identifying who set the preferences?

Issue 149:

- *tl:* we should not increase complexity of simple tools
  ... browser add on will just turn on DNT:1
- *aleecia:* 1/ user agent must be able to do one choice; 2/ three choices on, off, unset; 3/ 3 choices with equal effort of setting of all
  - o *<justin>* ifette, So on the symmetry point, you think we should prescribe that upon install (or in settings), everyone would need to offer equally weighted options for "do you want to tell websites not to track me" and "alternatively, do you want to tell websites they can track you all the time"? We want to put that in the spec?
  - o *tl:* we should not increase complexity of simple tools
    ... browser add on will just turn on DNT:1
    - ▪ Poll: silence 14, three choices: 23, one choice: 14.

ISSUE-153: What are the implications on software that changes requests but does not necessarily initiate them? (Pending Review)

http://www.w3.org/2011/tracking-protection/track/issues/153

http://lists.w3.org/Archives/Public/public-tracking/2012Oct/0634.html

Proposed text:

If user-controlled software modifies a DNT header sent by a user agent, it is a best practice for the software to clearly explain its modifications to the user.

Nick Doty

http://lists.w3.org/Archives/Public/public-tracking/2012Aug/0001.html

Proposal:

After this existing sentence in the TPE spec:
> 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.

Add:
> Software outside of the user agent that causes a DNT header to be sent (or modifies existing headers) MUST NOT do so without following the requirements of this section; such software is responsible for assuring the expressed preference reflects the user's intent.

ISSUE-163: How in the spec should we ensure user agents don't twist a user preference one way or another? (Raised)

http://www.w3.org/2011/tracking-protection/track/issues/163

ISSUE-172: How should user agents be required to provide information about DNT? (Raised)

Shane Wiley
http://lists.w3.org/Archives/Public/public-tracking/2012Oct/0637.html

[Proposed, New Text in Quotes " "]

Section 5. User Agent Compliance

A user agent must offer a control to express a tracking preference to third parties. The control must communicate the user's preference in accordance with the [TRACKING-DNT] recommendation and otherwise comply with that recommendation. A user agent must not express a tracking preference for a user unless the user has given express and informed consent to indicate a tracking preference.

"The User Agent MUST make available explanatory text to provide more detailed information about DNT functionality within easy and direct access for the particular environment prior to DNT being enabled."

Jonathan Mayer
http://lists.w3.org/Archives/Public/public-tracking/2012Oct/0186.html

Proposed text:

It is a best practice for the user agent to refer the user to an accessible explanation of the Tracking Preference Expression and Tracking Compliance and Scope recommendations. For example, in the interface for enabling Do Not Track, a browser might include a "Learn More" link to an informative webpage.

Discussion in Amsterdam:
http://www.w3.org/2012/10/03-dnt-minutes
- browser folks object to link to explanatory text when DNT is enabled
- *<jmayer>* Proposal: SHOULD provide users with information about Do Not Track. Don't specify the form of that information.
- WileyS the goal here is to have pre-selection means of informing the user, not a post-selection means
- no one in the room in favor of link, so moving on
- *aleecia:* if we change the MUST to SHOULD, and then give examples of best practices, give an example with no UI, and give info about DNT at the point of download, could people live with that
- *mikez:* DAA will supply alternative text
- *mikez:* can't live with suggested proposal to change MUST to SHOULD

AVG DNT setting:

http://www.avg.com/us-en/faq.tpl-stdfull.num-4902

AVG describes its use of the W3C DNT protocol, noting that it's on by default, but user-configurable.