Tracking Compliance and Scope

Unofficial Draft 10 June 2013

Latest editor's draft:
http://www.w3.org/2011/tracking-protection/drafts/tracking-compliance.html

Editors:
Justin Brookman, CDT
Heather West, Google
Sean Harvey, Google (until June 2012)
Erica Newland, CDT (until May 2012)

Abstract

This specification defines the meaning of a Do Not Track (DNT) preference and sets out practices for websites to comply with this preference.

Status of This Document

This document is merely a public working draft of a potential specification. It has no official standing of any kind and does not represent the support or consensus of any standards organisation.

Table of Contents

1. Scope

Do Not Track is designed to provide users with a simple preference expression mechanism to allow or limit online tracking globally or selectively.

The specification applies to compliance with requests through user agents that (1) can access the general browsable Web; (2) have a user interface that satisfies the requirements in Determining User Preference in the [TRACKING-DNT] specification; (3) and can implement all of the [TRACKING-DNT] specification, including the mechanisms for communicating a tracking status, and the user-granted exception mechanism.

2. Definitions

A ***user*** is an individual human. When user-agent software accesses online resources, whether or not the user understands or has specific knowledge of a particular request, that request is "made by the user."

The term ***user agent*** refers to any of the various client programs capable of initiating HTTP requests, including but not limited to browsers, spiders (web-based robots), command-line tools, native applications, and mobile apps [HTTP11].

A ***network interaction*** is the set of HTTP request and response, or any other sequence of logically related network traffic caused by a user visit to a single web page or similar single action. Page re-loads, navigation, and refreshing of content cause a new network interaction to commence.

A ***party*** is any commercial, nonprofit, or governmental organization, a subsidiary or unit of such an organization, or a person. For unique corporate entities to qualify as a common party with respect to this document, those entities MUST be commonly owned and commonly controlled and MUST provide easy discoverability of affiliate organizations. A list of affiliates MUST be available through a single user interaction from each page, for example, by following a single link, or through a single click.

An outsourced ***service provider*** is considered to be the same party as its client if the service provider:

1. acts only as a data processor on behalf of the client;
2. ensures that the data can only be accessed and used as directed by that client;
3. has no independent right to use or share the data except as necessary to ensure the integrity, security, and correct operation of the service being provided; and
4. has a contract in place that outlines and mandates these requirements.

In the context of a specific network interaction, the ***first party*** is the party with which the user intentionally interacts. In most cases on a traditional web browser, the first party will be the party that owns and operates the domain visible in the address bar.

The party that owns and operates or has control over a branded or labeled embedded widget, search box, or similar service with which a user intentionally interacts is also considered a first party. If a user merely mouses over, closes, or mutes such content, that is not sufficient interaction to render the party a first party.

In most network interactions, there will be only one first party with which the user intends to interact. However, in some cases, a resource on the Web will be jointly operated by two or more parties, and a user would reasonably expect to communicate with all of them by accessing that resource. User understanding that multiple parties operate a particular resource can, for example, be accomplished through inclusion of multiple parties' brands in a domain name, or prominent branding on the resource indicating that multiple parties are responsible for content or functionality on the resource with which a user reasonably would expect to interact by accessing the resource. Simple branding of a party, without more, will not be sufficient to make that party a first party in any particular network interaction.

A ***third party*** is any party other than a first party, service provider, or the user.

Whether a party is a first or third party is determined within and limited to a specific network interaction.

Data is ***deidentified*** when a party:

1. has achieved a reasonable level of justified confidence that the data cannot be used to infer information about, or otherwise be linked to, a particular consumer, computer, or other device
2. commits to try not to reidentify the data; and
3. contractually prohibits downstream recipients from trying to re-identify the data.

Tracking is the retention or use, after a network interaction is complete, of data records that are, or can be, associated with a specific user, user agent, or device.

A party ***collects*** data if it receives the data and shares the data with other parties or stores the data for more than a transient period.

A party ***retains*** data if data remains within a party's control beyond the scope of the current network interaction.

A party ***uses*** data if the party processes the data for any purpose other than storage or merely forwarding it to another party.

A party ***shares*** data if the party enables another party to receive or access that data.

3. User Agent Compliance

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).

User agents and web sites are responsible for determining the user experience by which a tracking preference is controlled. 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. User agents and web sites MUST ensure that the tracking preference choices describe the parties to whom DNT applies and MUST make available brief and neutral explanatory text to provide more detailed information about DNT functionality.

That text MUST indicate that:

1. if the tracking preference is communicated, it limits collection and use of web viewing data for certain advertising and other purposes;
2. when DNT is enabled, some data may still be collected and used for certain purposes, and a description of such purposes; and
3. if a user affirmatively allows a particular party to collect and use information about web viewing activities, enabling DNT will not limit collection and use from that party.

User agents and web sites MUST obtain an explicit choice made by a user when setting controls that affect the tracking preference expression.

A user agent MUST transmit the tracking preference according to the [TRACKING-DNT] specification.

Implementations of HTTP that are not under control of the user MUST NOT generate or modify a tracking preference.

4. First Party Compliance

If a first party receives a DNT:1 signal the first party MAY engage in its normal collection and use of information. This includes the ability to customize the content, services, and advertising in the context of the first party experience.

The first party MUST NOT pass information about this network interaction to third parties who could not collect the data themselves under this standard. Information about the transaction MAY be passed on to service providers acting on behalf of the first party

First parties MAY elect to follow third party practices.

5. Third Party Compliance

If a third party receives a DNT: 1 signal, then:

1. the third party MUST NOT collect, retain, share, or use information related to the network interaction as part of which it received the DNT: 1 signal outside of the permitted uses as defined within this standard and any explicitly-granted exceptions provided in accordance with the requirements of this standard;
2. the third party MUST NOT use information about previous network interactions in which it was a third party, outside of the permitted uses as defined within this standard and any explicitly-granted exceptions, provided in accordance with the requirements of this standard.

The third party MAY nevertheless collect, use, and retain such information for the set of permitted uses described below. Further, parties MAY collect, use, and retain such information in order to comply with applicable laws regulations, and judicial processes.

Outside the permitted uses listed below, the third party MUST NOT collect, retain, share, or associate with the network interaction identifiers that identify the specific user, user agent, or device. For example, a third party that does not require unique user identifiers for one of the permitted uses must not place a unique identifier in cookies or other browser-based local storage mechanisms.

Third parties that disregard a DNT signal MUST signal so to the user agent, using the response mechanism defined in the [TRACKING-DNT] specification.

When a third party receives a DNT:1 signal, that third party MAY nevertheless collect, retain, share or use data related to that network interaction if the data is de-identified as defined in this specification.

It is outside the scope of this specification to control short-term, transient collection and use of data, so long as the information is not transmitted to a third party and is not used to build a profile about a user or otherwise alter an individual user's user experience outside the current network interaction. For example, the contextual customization of ads shown as part of the same network interaction is not restricted by DNT:1.

It is outside the scope of this specification to control the collection and use of de-identified data.

5.1 Global Requirements for Permitted Uses

Some collection, retention and use of data is permitted, notwithstanding DNT: 1, as enumerated below. Different permitted uses may differ in their permitted items of data collection, retention times, and consequences. In all cases, collection, retention, and use of data must be reasonably necessary and proportionate to achieve the purpose for which it is specifically permitted; unreasonable or disproportionate collection, retention, or use are not "permitted uses".

5.1.1 No Secondary Uses

Third Parties MUST NOT use data retained for permitted uses for purposes other than the permitted uses for which each datum was permitted to be collected.

5.1.2 Data Minimization, Retention and Transparency

Data retained by a party for permitted uses MUST be limited to the data reasonably necessary for such permitted uses. Such data MUST NOT be retained any longer than is proporationate and reasonably necessary for such permitted uses.

Third parties MUST provide public transparency of the time periods for which data collected for permitted uses are retained. The third party MAY enumerate different retention periods for different Permitted Uses. Data MUST NOT be used for a permitted use once the data retention period for that permitted use has expired. After there are no remaining Permitted Uses for given data, the data MUST be deleted or de-identified.

Third parties MUST make reasonable data minimization efforts to ensure that only the data necessary for the permitted use is retained, and MUST NOT rely on unique identifiers for users or devices if alternative solutions are reasonably available.

5.1.3 No Personalization

Data retained for permitted uses MUST NOT be used to alter a specific user's online experience based on multi-site activity, except as specifically permitted below.

5.1.4 Reasonable Security

Third parties MUST use reasonable technical and organizational safeguards to prevent further processing of data retained for Permitted Uses. While physical separation of data maintained for permitted uses is not required, best practices SHOULD be in place to ensure technical controls ensure access limitations and information security. Third parties SHOULD ensure that the access and use of data retained for Permitted Uses is auditable.

5.2 Permitted Operational Uses for Third Parties

Regardless of DNT signal, information MAY be collected, retained and used to limit the number of times that a user sees a particular advertisement, often called ***frequency capping***, as long as the data retained do not reveal the user’s browsing history. Parties MUST NOT construct profiles of users or user behaviors based on their ad frequency history, or otherwise alter the user’s experience.

Regardless of DNT signal, information MAY be collected, retained and used for ***billing and auditing*** related to the current network interaction and concurrent transactions. This may include counting ad impressions to unique visitors, verifying positioning and quality of ad impressions and auditing compliance with this and other standards.

To the extent proportionate and reasonably necessary for ***detecting security risks and***

fraudulent or malicious activity, parties MAY collect, retain, and use data regardless of a DNT signal. This includes data reasonably necessary for enabling authentication/verification, detecting hostile and invalid transactions and attacks, providing fraud prevention, and maintaining system integrity. In the context of this specific permitted use, this information MAY be used to alter the user's experience in order to reasonably keep a service secure or prevent fraud.

Regardless of DNT signal, information MAY be collected, retained and used for ***debugging purposes*** to identify and repair errors that impair existing intended functionality.

> NOTE
>
> Expecting further text on ***audience measurement***.

5.3 Third Party Geolocation Compliance

If the operator of a third-party domain is part of a network interaction with a DNT: 1 signal, then geolocation data MUST NOT be used in that interaction at any level more granular than postal code, unless specific consent has been granted for the use of more granular location data.

6. User-Granted Exceptions

When a user sends a DNT: 0 signal, the user is expressing a preference for a personalized experience. This signal indicates explicit consent for data collection, retention, processing, disclosure, and use by the recipient of this signal to provide a personalized experience for the user. This recommendation places no restrictions on data collected from requests received with DNT: 0.

The operator of a website may engage in practices otherwise proscribed by this standard if the user has given explicit and informed consent. This consent may be obtained through the API defined in the companion [TRACKING-DNT] document, or an operator of a website may also obtain ***out of band*** consent to disregard a Do Not Track preference using a different technology. If an operator is relying on out of band consent to disregard a Do Not Track preference, the operator must indicate this consent to the user agent as described in the companion [TRACKING-DNT] document.

7. Interaction with Existing User Privacy Controls

Multiple systems may be setting, sending, and receiving DNT and/or opt-out signals at the same time. As a result, it will be important to ensure industry and web browser vendors are on the same page with respect to honoring user choices in circumstances where "mixed signals" may be received.

As a general principle, more specific settings override less specific settings.

1. No DNT Signal / No Opt-Out: Treat as DNT unset
2. DNT Signal / No Opt-Out: Treat as DNT: 1
3. Opt-Out / No DNT Signal: Treat as DNT: 1
4. Opt-Out / DNT User-Granted Exception: Treat as DNT: 0 for that site; DNT User-Granted Exception is honored

8. Unknowing Collection

If a party learns that it possesses information in violation of this standard, it MUST, where reasonably feasible, delete or de-identify that information at the earliest practical opportunity, even if it was previously unaware of such information practices despite reasonable efforts to understand its information practices.

A. Acknowledgements

This specification consists of input from many discussions within and around the W3C Tracking Protection Working Group, along with written contributions from Haakon Flage Bratsberg (Opera Software), Amy Colando (Microsoft Corporation), Roy T. Fielding (Adobe), Tom Lowenthal (Mozilla), Ted Leung (The Walt Disney Company), Jonathan Mayer (Stanford University), Ninja Marnau (Invited Expert), Matthias Schunter (IBM), John M. Simpson (Invited Expert), Kevin G. Smith (Adobe), Rob van Eijk (Invited Expert), David Wainberg (Network Advertising Initiative), Rigo Wenning (W3C), and Shane Wiley (Yahoo!).

The DNT header field is based on the original Do Not Track submission by Jonathan Mayer (Stanford), Arvind Narayanan (Stanford), and Sid Stamm (Mozilla). The DOM API for NavigatorDoNotTrack is based on the Web Tracking Protection submission by Andy Zeigler, Adrian Bateman, and Eliot Graff (Microsoft). Many thanks to Robin Berjon for ReSpec.js.

B. References

B.1 Normative references

[HTTP11]
R. Fielding et al. *Hypertext Transfer Protocol - HTTP/1.1*. June 1999. RFC 2616. URL: http://www.ietf.org/rfc/rfc2616.txt

[TRACKING-DNT]
Roy T. Fielding; David Singer. *Tracking Preference Expression (DNT)*. 02 October 2012. W3C Working Draft. URL: http://www.w3.org/TR/tracking-dnt/