Tracking Compliance and Scope

W3C Editor's Draft 22 June 2013

This version:
http://www.w3.org/2011/tracking-protection/drafts/tracking-compliance.html
Latest published version:
http://www.w3.org/TR/tracking-compliance/
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)

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 section describes the status of this document at the time of its publication. Other documents may supersede this document. A list of current W3C publications and the latest revision of this technical report can be found in the W3C technical reports index at http://www.w3.org/TR/.

This draft works off of the unofficial June Draft, a substantial change from the previous Editors' Draft. The April 30 Working Draft captures that text (including multiple options in several sections) if you wish to refer to it.

This document was published by the Tracking Protection Working Group as an Editor's Draft. If you wish to make comments regarding this document, please send them to public-tracking@w3.org (subscribe, archives). All comments are welcome.

Publication as an Editor's Draft does not imply endorsement by the W3C Membership. This is a draft document and may be updated, replaced or obsoleted by other documents at any time. It is inappropriate to cite this document as other than work in progress.

This document was produced by a group operating under the 5 February 2004 W3C Patent Policy. W3C

maintains a public list of any patent disclosures made in connection with the deliverables of the group; that page also includes instructions for disclosing a patent. An individual who has actual knowledge of a patent which the individual believes contains Essential Claim(s) must disclose the information in accordance with section 6 of the W3C Patent Policy.

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]. This standard applies to 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.

A ***network interaction*** is the set of HTTP requests and responses, 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 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 their clients' data outside of Permitted Uses; 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.

ISSUE 10: What is a first party?

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 taken reasonable steps to ensure that the data cannot reasonably be re-associated or connected to a specific user, computer, or device;
2. has taken reasonable steps to protect the non-identifiable nature of data if it is distributed to non-affiliates and obtain satisfactory written assurance that such entities will not attempt to reconstruct the data in a way such that an individual may be re-identified and will use or disclose the de-identified data only for uses as specified by the entity.
3. has taken reasonable steps to ensure that any non-affiliate that receives de-identified data will itself ensure that any further non-affiliate entities to which such data is disclosed agree to the same restrictions and conditions.
4. will commit to not purposely sharing this data publicly.

Data is ***delinked*** when a party:

1. has achieved a reasonable level of justified confidence that data has been de-identified and cannot be internally linked to a specific user, computer, or other device within a reasonable timeframe;

2. has taken reasonable steps to ensure that data cannot be reverse engineered back to identifiable data without the need for operational or administrative controls.

Non-Normative: Delinked data could still have some level of internal linkage within a discrete dataset if the process to delink data occurs on a set time interval, for example, hourly or daily. Implementers should consider only exercising the market research and product development permitted uses in the de-identified but still internally linkable state.

Issue 188: Definition of de-identified (or previously, unlinkable) data

Tracking is the collection and retention, or use of activity across non-affiliated websites linked to a specific user, computer, or device.

Issue 5: What is the definition of tracking?

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 (and not retaining) it to another party.

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

Issue 16: What does it mean to collect data? (caching, logging, storage, retention, accumulation, profile etc.)

3. User Agent Compliance

Issue 132: Should the spec speak to intermediaries or hosting providers to modify any responses/statements about DNT compliance?

Issue 151: User Agent Requirement: Be able to handle an exception request

Issue 172: How should user agents be required to provide information about DNT?

Issue 194: How should we ensure consent of users for DNT inputs?

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 are responsible for determining the user experience by which a tracking preference is controlled. User agents 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 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 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.

Parties attempting to receive user granted exceptions through the API defined in the companion [tpe] document must also comply with these principles.

4. First Party Compliance

If a first party receives a DNT:1 signal the first party MAY engage in its collection and use of information within the first party context. 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 without consent about this network interaction to third parties who could not collect the data themselves when DNT:1 is received. 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.

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

Issue 170: Definition of and what/whether limitations around data append and first parties

5. Third Party Compliance

In a particular network interaction, if a third party receives a DNT: 1 signal, then that third party MUST NOT track outside of the Permitted Uses and any explicitly-granted exceptions

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

Outside the permitted uses or de-identification, the third party MUST NOT collect, retain, or share network interaction identifiers that identify the specific user, computer, or device.

Parties that disregard a DNT signal MUST respond 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. For example, the contextual customization of ads shown as part of the same network interaction is not restricted by DNT: 1.

Issue 134: Would we additionally permit logs that are retained for a short enough period?

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

5.1 General Principles for Permitted Uses

Some collection, retention and use of data is permitted, notwithstanding DNT:1 for specific uses. 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. Data retained for Permitted Uses may only be used for those purposes.

5.1.2 Data Minimization, Retention and Transparency

Data retained by a party for permitted uses must be minimized to the data reasonably necessary for such permitted uses. Such data must not be retained any longer than is proportionate and reasonably necessary for such permitted uses.

Parties must provide public transparency of the time periods for which data collected for permitted uses are retained. The 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 and delinked.

Issue 31: Minimization -- to what extent will minimization be required for use of a particular exemption?

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.

5.2 Permitted Uses

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. -

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.

Issue 24: Possible exemption for fraud detection and defense

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***.

Issue 25: How is audience measurement adressed under DNT? (permitted use or otherwise)

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.

A party 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 through ***out of band*** consent to disregard a Do Not Track preference using a different technology. If party is relying on out of band consent to disregard a Do Not Track preference, the party must indicate this consent to the user agent as described in the companion [TRACKING-DNT] document.

7. Interaction with Existing User Privacy Controls

An opt-out choice made by a user may exist concurrently with a DNT signal.

As a general principle, more specific settings made by an informed user are recognized over less specific settings.

DNT	Opt-Out	Outcome
No Signal	Off	No DNT compliance obligations
DNT:1	Off	Process the DNT signal in compliance with DNT obligations
No Signal	On	Honor compliance obligations made through the party's opt-out mechanism or the applicable self-regulation opt-out mechanism
DNT UGE	On	Processing may occur as allowed by the UGE to the extent that such processing is not violative of obligations made through the opt-out mechanism

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), Nick Doty (W3C), Roy T. Fielding (Adobe), Yianni Lagos (Future of Privacy Forum), Tom Lowenthal (Mozilla), Ted Leung (The Walt Disney Company), Jonathan Mayer (Stanford University), Ninja Marnau (Invited Expert), Thomas Roessler (W3C), Matthias Schunter (IBM), Wendy Seltzer (W3C), John M. Simpson (Invited Expert), Kevin G. Smith (Adobe), Peter Swire (Invited Expert), 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. 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/