Scope

Do Not Track is designed to provide users with a simple mechanism to express their preference on whether to allow or stop online tracking, introduces machine-readable elements that allow web-sites to explain their tracking behaviour, and an API to monitor the current DNT status and let users give or revoke their consent for tracking by servers across the web or when embedded on specific sites. Complying with the user's preference as described in this document includes limits on the collection, retention, use, and sharing of personal data, and the use of browser or device resident storage.

REQUIREMENTS

When an origin server receives Web requests with DNT set, and the user has not given their specific consent for tracking or non-essential storage use using a mechanism that complies with the “out-of-band consent” mechanism described in the TPE, it will take the following measures with respect to those users' data, subject to the Exceptions, also listed below:

1. STORAGE AND TRACKING:

No data will be stored, used or derived from other data on the user’s device, other than the limited use of short duration HTTP cookies to hold data pertaining to a user “session”, or the use of storage which is strictly necessary to fulfil a service specifically requested by the user or is solely required to enable the underlying communications channel. Such cookies must expire, i.e. automatically deleted by the user agent, after no more than 12 hours, and must never be regenerated. This means that no action will be taken to identify the user or their user agent outside the above 12 hour window.

No “browser fingerprinting”, or the use of ambient or data already stored to derive a unique or nearly unique user identifier, will occur.

As far as possible any data previously caused to be stored by the origin server, other than the short duration “session” cookies described above, will be immediately deleted.

2. LOG RETENTION:

Logs of HTTP requests may be retained, as long as any user identifying information such as the source IP address has been removed. The short term retention of log information containing user identifying information such as IP addresses is allowed for a period of up to 10 days, solely for the purpose of detecting and counteracting any Denial of Service or other attack such as a spam submission, or fraudulent transaction.

3. OTHER DOMAINS:

If an origin server transfers identifiable or identifying user data about DNT Users to contractors, affiliates or other parties, or embeds from or posts data to other domains, the controller will either:

1. Ensure that the operators of those domains abide by this policy overall and declare a Tracking Status Resource “compliance” property that contains a URI reference to this document.

OR

1. Obtain a contractual commitment from the recipient to respect this policy for the DNT Users' data.

4. CONSENT

If data needs to be stored in or linked to the user agent, other than for the short term retention of session state, for example to “log in” to a website, then the origin server must

1. Inform the user in a clear and unambiguous way the purpose for any use of user agent storage or the otherwise processing of personal data.

AND

1. Indicate clearly how long the storage will be used or any personal data retained.

AND

1. Ask the user for an affirmative indication of their consent for this.

If the user gives their consent then this MAY be registered in the user agent using the JavaScript Do Not Track Consent API described in the TPE. The “maxAge” or “expires” properties must be set so the consent will be revoked before or immediately upon the expiry of the retention period given in the associated user information. If the user agent implementation does not support the consent expiry capability the origin server must arrange for the removal of the consent registration, and any associated storage or retained personal data, itself.

If a user agent does not support the Consent API then consent can be registered by some “out-of-band” mechanism such as a persistent HTTP cookie containing authentication information. In this case the origin server must return a Tk header with a Tracking Status Value of “C” as described in the TPE. The data used by the “out-of-band” mechanism, and any storage or retained personal data collected, must be deleted at or before the first opportunity to do so following the expiry of the retention period given in the associated user information.

5. EXCEPTIONS

Data from DNT Users collected by this domain may be logged or retained only in the following specific situations:

1. We may retain and share anonymized datasets, such as aggregate records of readership patterns; statistical models of user behaviour; graphs of system variables; data structures to count active users; or logs with truncated and/or encrypted IP addresses and simplified User Agent strings. "Anonymized" means we have conducted risk mitigation to ensure that the dataset, plus any additional information that is in our possession or likely to be available to us, does not allow the reconstruction of reading habits, online or offline activity of groups of fewer than 5000 individuals or devices. If we retain or share anonymized datasets under this exception we will publicly document our anonymization methods in sufficient detail to allow outside experts to evaluate the effectiveness of those methods.
2. From time to time, there may be errors by which user data is temporarily logged or retained in violation of this policy. If such errors are inadvertent, rare, and made in good faith, they do not constitute a breach of this policy. We will delete such data as soon as practicable after we become aware of any error and take steps to ensure that it is deleted by any third-party who may have had access to the data.