Comparison of Tracking Compliance and Scope April 29, 2013 Editors' Draft to June Draft

Editors' Draft: http://www.w3.org/2011/tracking-protection/drafts/tracking-compliance.html

June Draft: http://www.w3.org/2011/tracking-protection/drafts/tracking-compliance-june.html

ISSUE-5 What is the definition of tracking?

- June Draft: *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.
    - Located in the Definition section
- Editors' Draft: "Tracking" is understood by this standard as the collection and retention of data across multiple parties' domains or services in a form such that it can be attributed to a specific user, user agent, or device.
    - Located in the Scope section

ISSUE-10 What is a first party?

- June Draft adds: Whether a party is a first or third party is determined within and limited to a specific network interaction.

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

- Similar to Editors' Draft, grammatical changes

ISSUE-24 Possible exemption for fraud detection and defense

- June Draft: Removes "graduated response" adds "to the extent proportionate".

ISSUE-25: How is audience measurement addressed under DNT? (permitted use or otherwise)

- Same

ISSUE-31: Minimization -- to what extent will minimization be required for use of a particular exemption? (conditional exemptions)

- June Draft: 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.

- Editors' Draft: Data retained by a party for permitted uses *MUST* be limited to the data reasonably necessary for such permitted uses, and *MUST* be retained no longer than is reasonably necessary for such permitted uses. A third party *MUST* make reasonable data minimization efforts to ensure that only data necessary for each permitted use is retained. A third party *MUST* provide public transparency of their data retention period for each permitted use. Once a retention period for a given use has expired, the data *MUST NOT* be used for that permitted use; when there are no remaining permitted uses for some data, that data *MUST* either be deleted or rendered unlinkable.

ISSUE-134 Would we additionally permit logs that are retained for a short enough period?

- June Draft: 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.
- Editors' Draft: Option (1) Information may be collected, retained, and used any purpose, so long as the information is retained for no longer than N weeks and the information is not transmitted to a third party and the information is not used to build a profile about a user or otherwise alter any individual's user experience (apart from changes that are made based on aggregate data or security concerns).
    - Option (2) Operators *MAY* collect and retain data related to a communication in a third-party context for up to N weeks. During this time, operators may render data *deidentified* or perform processing of the data for any of the other permitted uses.

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

- June Draft: Retains same first party compliance restrictions of editors' draft, drops the "Additional/Alternative First Party Compliance Requirements".
- Editors' Draft: Contains an option box for those additional requirements with the normative text:
  When DNT:1 is received,
    1. A first party *MUST NOT* combine or otherwise use identifiable data received from another party with data it collected while a first party;
    2. A first party *MUST NOT* share identifiable data with another party unless the data was provided voluntarily by the user and is necessary to complete a business transaction with the user; and
    3. A party *MUST NOT* use data gathered while a first party when operating as a third party.

User Agent Issues[1]

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

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?

- June Draft: 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.

- Editors' Draft: Option (1) A user agent MUST offer a control to express a tracking preference to third parties. The control MUST communicate the user's preference in

[1] The User Agent section tries to merge the draft framework, Sunnyvale conversations, and the Tracking Preference Expression's "determining user preference" text, and may end up in the Tracking Preference Expression specification.

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 a user;

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.

- Option (2) 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.

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

- June Draft: 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.

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

- June Draft: 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.

- Editors' Draft: Option (1) Data is *deidentified* when a party:

  (1) has taken measures to ensure with 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) does not to try to reidentify the data; and
  (3) contractually prohibits downstream recipients from trying to re-identify the data.

  - Option (2) Data can be considered sufficiently *deidentified* to the extent that it has been deleted, modified, aggregated, anonymized or otherwise manipulated in order to achieve a reasonable level of justified confidence that the data cannot reasonably be used to infer information about, or otherwise be linked to, a particular user, user agent, or device.

Third Party Compliance

- June Draft additions:

  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.

Service Provider Definition

- June Draft: 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.
- Editors' Draft alternative: Outsourced ***service providers*** are considered to be the same party as their clients if the outsourced service providers only act as data processors on behalf of that party in relation to that party, silo the data so that it cannot be accessed by other parties, and have no control over the use or sharing of that data except as directed by that party.

Other Changes

- June Draft:
    - drops "Disregarding Non-Compliant User Agents", but includes language in the Third Party Compliance section above,
    - drops "Public Commitment" sections,
    - separates out "Unknowing Collection" section,
    - moves contextual, first party, short term collection out of third party permitted uses into general requirements,
    - uses fewer subsections,
    - and drops separate Introduction section