WILMERHALE

W3C Compliance Specification Continues Do Not Track's Forward Progress

APRIL 28, 2016

Progress continues at the World Wide Web Consortium (W3C) to establish a Do Not Track (DNT) standard to help users control or limit third-party tracking online. Launched in 2011, the DNT working group was formed to produce both technical and compliance rules, and on Tuesday, April 26, after years of passionate debate, the W3C finally issued a Candidate Recommendation to establish a compliance specification for DNT. This comes in the wake of last year's recommendations regarding the technical rules around communicating users' tracking expression preferences with servers and web applications.

The Candidate Recommendation details the limits on the collection, retention, and use of data collected by "third parties" and the sharing of data not permanently de-identified when a user broadcasts a "DNT:1" signal. "First parties," defined as "a party with which the user intends to interact, via one or more network interactions, as a result of making that action," remain free to collect and use data about users on their own websites, which generally includes customizing content, services, and advertising. Contextual advertising remains unrestricted by "DNT:1" signals, but first parties must not share data about these sorts of network interactions with third parties.

Things are more complicated for third parties (according to the document, a Third Party is "any party other than that user, a first party for that user action, or a service provider acting on behalf of either that user or that first party"). Under the Candidate Recommendation, data collection and use by third parties is generally only be permissible under a "DNT:1" signal where: (1) a user has granted explicit consent; (2) the data is permanently de-identified; or (3) the data is collected for a set of permitted uses. Permitted collection and use includes:

- Frequency capping (limiting the number of times a user sees a particular advertisement);
- Financial logging such as billing or auditing practices like counting ad impressions, verifying positioning and quality of ad impressions, and auditing compliance;
- Detecting security incidents, provided that data is not used for operational behavior beyond what is reasonably necessary to protect the service; and
- Debugging purposes to identify and repair errors that impair existing intended functionality.

Several general requirements apply to these permitted uses. For example, third parties are not

permitted to use this data for any secondary uses or to personalize a user's online experience. Reasonable security measures, as well as data minimization, retention, and transparency requirements, are also required before third parties can collect or use data from users' "DNT:1" signals.

The specification also permits sharing where data is "permanently de-identified." This is defined as "data where there exists a high level of confidence that no human subject of the data can be identified, directly or indirectly, by that data alone or in combination with other retained or available information." A non-normative section of the specification explains that de-identification could be demonstrated by ensuring it is no longer possible to:

- Isolate some or all records which correspond to a device or user;
- Link two or more records (either from the same database or different databases), concerning the same device or user; or
- Deduce, with significant probability, information about a device or user.

The W3C is accepting comments on this Candidate Recommendation at public-tracking-comments@w3.org. The W3C intends the Candidate Recommendation to become a Proposed Recommendation by June 15, 2016. This would create a formalized DNT compliance standard and potentially provide industry with clarity as to how to respond to DNT signals in the future, if companies choose to do so.