



Brussels, 01 October 2015

By e-mail:
public-tracking-comments@w3.org

Article 29 Data Protection Working Party comments in response to W3C's public consultation on the W3C Last Call Working Draft, 14 July 2015, Tracking Compliance and Scope

Dear Mr Schunter, Mr Cargill and Mr Doty,

I am writing to you on behalf of the Article 29 Data Protection Working Party.

On 6 June 2014 and 19 June 2015, the Working Party responded to the public consultation on the World Wide Web Consortium (W3C) Last Call Working Draft of the Tracking Preference Expression (24 April 2014), referred to in this letter as 'the Draft TPE Specification'. W3C has now opened a public consultation on the W3C Last Call Working Draft of the Tracking Compliance and Scope (14 July 2015), referred to in this letter as 'the Draft DNT Compliance Specification'.

The Draft DNT Compliance Specification addresses the broader interpretation of the Do Not Track (DNT) signal by users and data controllers.¹ However it cannot be considered in isolation to the technical building blocks of DNT as defined in the Draft TPE Specification. The Working Party therefore assesses these two specifications from the perspective of whether the Draft DNT Compliance Specification forms a framework that could be regarded as an adequate compliance mechanism for signifying consent to the processing of personal data in the EU.²

The Working Party recognizes the potential of the DNT standard as a mechanism to empower users to express preferences as to whether they want to be tracked or not, and to have their choices transmitted and/or relayed to all the involved parties. However, the Working Party is concerned that the proposed specification does not provide a mechanism that would be regarded adequate under the European Data Protection and Privacy legal framework, referred to in this letter as 'the EU legal framework'.

¹ The Working Party has provided guidance on the term data controller in its Opinion 1/2010 on the concepts of 'controller' and 'processor' (WP169).

² The Working Party has provided guidance on consent in several opinions. See, e.g., the following opinions of the Working Party: Opinion 05/2014 on Anonymisation Techniques (Wp216), Opinion 15/2011 Consent (WP187), Working Document 02/2013 providing guidance on obtaining consent for cookies (WP208), Opinion 04/2012 on Cookie Consent Exemption (WP194), Opinion 2/2010 on online behavioural advertising (WP71), and Opinion 03/2013 on purpose limitation (WP203).

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The secretariat is provided by Directorate C (Fundamental Rights and Union Citizenship) of the European Commission, Directorate-General for Justice and Consumers, B-1049 Brussels, Belgium, Office No MO-59 02/013.

Website: http://ec.europa.eu/justice/data-protection/index_en.htm

In the EU, consent for the processing of personal data includes the activity of collection. Therefore, the Draft DNT Compliance Specification must include instructions of ‘Do Not Collect’, ‘Do Not Use’, and ‘Do Not Share’.³

Furthermore, data controllers bound by the EU legal framework – regardless of whether they are a first party or a third party – still require unambiguous consent for the processing of personal data including for the purposes of online behavioral advertising (OBA). In this regard, the limitation of DNT to only third party tracking presents another crucial obstacle, where DNT would not suffice to achieve compliance with the EU legal framework.⁴

The Working Party has previously raised concerns on other specific aspects including the interplay of DNT with any out-of-band consent mechanisms and the transparency of such possibilities for users. The Working Party has also indicated that use of the term de-identification deserves further clarification.⁵ All such points are still open issues. Moreover, the Working Party is concerned about the application of the concept of a graduated response not being normative.⁶ Suggestions for (normative) language is provided in the Annex.

In conclusion, we feel that whilst an individual data controller could demonstrate compliance with the EU legal framework through a bespoke interpretation of a DNT signal, the aforementioned gaps between the DNT compliance level and what is required by the EU legal framework undermine the usefulness of the standard in a broad European context. The Draft DNT Compliance Specification would fall short of the expectations of EU regulators, data controllers, and users for a granular solution for expressing valid consent through browser settings that would be compliant with the EU legal framework.⁷

The Working Party encourages all stakeholders including data controllers to improve, in line with Recital 66 of the ePrivacy Directive,⁸ on the Draft DNT Compliance Specification in order to make it compliant with EU data protection and privacy law.

Yours sincerely,

On behalf of the Article 29 Working Party,

Isabelle FALQUE-PIERROTIN
Chairwoman

CC:

By e-mail: rob@blaeu.com, npdoty@w3.org

³ See the Annex ‘Respecting a user tracking preference’ and the Draft TPE Specification, Section 2.4.

⁴ The Working Party has provided guidance on consent to OBA and more generally, online tracking, where it elaborated in depth on the five necessary elements of valid consent, which are that consent should be: (1) freely given, (2) specific, (3) informed, (4) unambiguous, and (5) based on a user’s action.

⁵ The Working Party has provided guidance on the subject in its Opinion 05/2014 on Anonymisation Techniques (WP216).

⁶ See the draft DNT Compliance Specification, Subsection 3.3.2.3.

⁷ Cf. International Working Group on Data Protection in Telecommunications (IWGDPT), Working Paper on Web Tracking and Privacy: Respect for context, transparency and control remains essential. URL: http://www.datenschutz-berlin.de/attachments/979/675_46_32.pdf?1379937149.

⁸ Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009.

ANNEX

1. Compliance.

The terminology in the Draft DNT Compliance Specification cannot override regulatory terminology in the EU. Therefore, the Working Party suggests including the following language: ‘This specification does not override regulatory terminology, and as such, compliance with this specification does not mean compliance with the law and/or regulations.’

2. Respecting a user tracking preference.

It is important that it is clear for data controllers to which activities the user consents. A DNT:0 signal must not be interpreted by a data controller as consent for anything other than clearly defined tracking activities.⁹ Therefore, the Working Party suggests including the following language: ‘In the absence of fully informed user choice, e.g., DNT is unset,¹⁰ a data controller, or a data processor acting on behalf of the data controller, SHOULD assume that a user is not aware of tracking. He MUST therefore ask for consent prior to tracking.’ Moreover, the Working Party would like to note that - in order to put the user back into control - any Do Not Track implementation for managing consent in line with Recital 66 of the ePrivacy Directive should be implemented at the browser (configuration) level.

3. Anonymisation.

The Working Party remains concerned about the concept of de-identification (in section 2.9.1).¹¹ The Working Party suggests including the following language: ‘In cases where the process of de-identification of (personal) data is not properly assessed against privacy risks and the possibility of identification of users cannot be excluded, compliance with this specification does not mean compliance with other legislative law and/or regulations.’

4. Out of band consent, potential consent (P), and disregarding (D).

The Working Party suggests including the following normative language: ‘Out of band consent MUST be obtained in an unambiguous manner and specific to the intended purpose. Data collected with out of band consent MUST only be used for that specified purpose.’

5. Graduate response

The Working Party suggests changing the sentence ‘When feasible, a graduated response to a detected security incident is preferred over widespread data collection’ to a normative requirement (i.e., ‘(...) SHOULD be preferred (...).’¹²

⁹ Cf. Opinion 03/2013 on purpose limitation (WP203).

¹⁰ See the Draft TPE Specification, Section 5.1.

¹¹ See Opinion 05/2014 on Anonymisation Techniques (WP216), p. 11. The opinion addresses three key risks which are essential to anonymisation techniques: (1) singling out, (2) linkability, and (3) inference.

¹² See the draft DNT Compliance Specification, Subsection 3.3.2.3.