# ARTICLE 29 Data Protection Working Party

Brussels, 6 June 2014

Mr Matthias Schunter, PhD
Mr Justin Brookman, JD
Mr Carl Cargill

World Wide Web Consortium (W3C)
W3C/MIT
32 Vassar Street
Room 32-G515
Cambridge, MA 02139 USA

E-mail: public-tracking-comments@w3.org

**Re:    Article 29 Data Protection Working Party comments in response to W3C's public consultation on the W3C Last Call Working Draft, 24 April 2014, Tracking Preference Expression (DNT)**

Dear Mr Schunter, Mr Brookman and Mr Cargill,

I am writing to you on behalf of the Article 29 Data Protection Working Party.[1]

The Working Party has devoted considerable time and effort in its engagement as observer in the W3C working group on DNT.

W3C has now opened a public consultation on the W3C Last Call Working Draft of the Tracking Preference Expression (24 April 2014), referred to in this letter as 'the Draft TPE Specification'. Even though this specification only addresses the technical building blocks of DNT, it cannot be seen separately from the broader interpretation of the DNT signal by users and data controllers. The Working Party therefore assesses these specifications from the perspective of whether the Draft TPE Specification contains the building blocks needed for valid consent in the EU.[2] The necessary elements of valid consent are: freely given, specific, informed, unambiguous, and based on a user's action.[3]

---

[1] The Working Party on the protection of individuals with regard to the processing of personal data set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, having regard to Articles 29 and 30 paragraphs 1(a) and 3 of that Directive.

[2] The Working Party has provided guidance on consent in several opinions. See, e.g., the following opinions of the Working Party: 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), URL: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm.

[3] See URL: http://lists.w3.org/Archives/Public/public-tracking/2012Jan/att-0268/W3C_v2.pdf.

The Working Party believes that an effective DNT-standard will empower users, while benefitting organisations at the same time.[4] If user agent manufacturers and data controllers implement DNT well, the protocol has potential, under certain circumstances, to become a granular consent mechanism that is in line with Recital 66 of Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 (hereinafter: Recital 66). This Recital allows for users to express consent through their browser settings, but only if the consent complies with the above mentioned requirements for valid consent. The key sentence in Recital 66 is as follows.

> *Where it is technically possible and effective, in accordance with the relevant provisions of Directive 95/46/EC, the user's consent to processing may be expressed by using the appropriate settings of a browser or other application.[5]*

There are several key issues in the draft specification that risk undermining the usefulness of the standard in a European context. These issues create a real risk that Do Not Track (DNT) remains a sugar pill, from an enforcement point of view, instead of evolving into a valid and robust solution.[6]

The six key issues are: (1) terminology, (2) the fact that the specification does not ensure automatic expiration of a tracking preference, (3) doubt whether data controllers will respect user tracking preference, (4) inclusion of a definition of de-identification, as it does not match with the definition of anonymisation in European data protection law, (5) the risk of undermining valid consent by an ambiguous server response of 'potential consent' and ambiguous use of 'disregarding', and (6) the lack of special considerations for users with special needs. These issues are explained in more detail in the Annex to this letter.

The Working Party encourages all stakeholders to improve, in line with Recital 66, on the Draft TPE Specification in order to make it compliant with EU data protection law.

Yours sincerely,

On behalf of the Article 29 Data Protection Working Party,


Isabelle Falque-Pierrotin
Chair

---

[4] Cf. Resolution on Web tracking and privacy, 35th International Conference of Data Protection and Privacy Commissioners, Warsaw 23-26 September 2013. URL:
https://privacyconference2013.org/web/pageFiles/kcfinder/files/8.%20Webtracking%20Resolution%20EN%281%29.pdf.

[5] URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:en:PDF.

[6] 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

ANNEX

1. Terminology.

The terminology in the Draft Specification cannot override regulatory terminology in the EU.[7] Therefore, the Working Party suggests including the following normative language in the Draft TPE Specification, Section 2, Terminology: *This specification does not override regulatory terminology, and as such, compliance with this specification does not mean compliance with regulations.*

2. Automatic expiration of a tracking preference.

With regard to some parallel initiatives, such as notice-and-choice programs, the Working Party acknowledges that they can function as supporting measures to remind users that they can withdraw their tracking preference at any time. But the Draft TPE Specification currently lacks a building block that ensures the automatic expiration of a tracking preference. Under European data protection law, personal data must be adequate and accurate, and stored no longer than necessary. In order to comply with these requirements, the introduction of an automatic expiration feature is necessary to allow users to exercise effective control. Therefore, the Working Party recommends adding this requirement to the building blocks.

3. 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.[8] In the absence of fully informed user choice, e.g., DNT is unset,[9] 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 tool for managing consent should be implemented at the user agent level.

4. Anonymisation

The Working Party is concerned about the term *de-identify* (in section 6.2.7). The previously proposed definition of de-identification currently does not match with the definition of anonymisation in European data protection law. Merely replacing identifiers in a dataset will not lead to anonymisation. The Working Party refers to its extensive guidance on anonymisation techniques.[10]

---

[7] See section 2 of the Draft TPE Specification.
[8] See also Opinion 03/2013 on purpose limitation (WP203), URL: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.
[9] See section 5.1 of the Draft TPE Specification.
[10] Opinion 05/2014 on "Anonymisation Techniques onto the web (WP216). URL: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.

5. <u>Potential consent (P), Disregarding (D).</u>

The 'P' tracking status value indicates that the user's consent that cannot be determined in real time.[11] This building block could seriously undermine the validity of a consent mechanism in the EU because it limits the scope of the user's tracking preference. Likewise, the Working Party has serious concerns about the use of the 'Disregarding (D)' tracking status value.

The Working Party wishes to remind all stakeholders that all forms of expressing consent, need to comply with all necessary elements for valid consent.[12]

6. <u>Users with special needs.</u>

There are users for whom giving prior consent is not obvious.[13] To address users with special needs, the Working Party suggest to add the following text to section 7.7 'User interface guidelines': *Special consideration must be given to ensure that no group of web users are treated less favourably or are otherwise discriminated against, for example, as a result of a disability. This will be particularly important for those devices which have limited, or no, display and configuration capabilities.*

---

[11] Section 6.2.7 reads as follows: "*A tracking status value of* P *means that the origin server does not know, in real-time, whether it has received prior consent for tracking this user, user agent, or device, but promises not to use or share any DNT:1 data until such consent has been determined, and further promises to delete or de-identify within forty-eight hours any DNT:1 data received for which such consent has not been received.*"

[12] See also URL: http://lists.w3.org/Archives/Public/public-tracking/2012Jan/att-0268/W3C_v2.pdf.

[13] 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