TILT (TILBURG INSTITUTE FOR
LAW, TECHNOLOGY, AND SOCIETY)
LAW & TECHNOLOGY
WORKING PAPER SERIES

Do Not Track initiatives: regaining the lost user control

Irene Kamara
TILT, Tilburg University, The Netherlands
i.kamara@uvt.nl

&

Eleni Kosta

TILT, Tilburg University, The Netherlands
e.kosta@uvt.nl

TILT Law & Technology Working Paper No. 007/2019
23 October 2019, Version: 1.0

This paper can be downloaded without charge from the
Social Science Research Network Electronic Paper Collection
http://ssrn.com/abstract=3466822

An overview of the TILT Law & Technology Working Paper Series can be found at:
http://www.tilburguniversity.nl/faculties/law/research/tilt/publications/workingpapers/

Please refer to the published version:

Irene Kamara and Eleni Kosta, Do Not Track initiatives: regaining the lost user control, *International Data Privacy Law*, Volume 6, Issue 4, November 2016, Pages 276–290, **https://doi-org.tilburguniversity.idm.oclc.org/10.1093/idpl/ipw019**

1. Introduction

Recently, in a case characterized as the 'European privacy judicial decision of a decade',[1] the England and Wales Court of Appeal was called to decide on whether Google will have to pay damages to Apple Safari users, who were being tracked by the Google advertising platform, without their knowledge and consent.[2] The Court of Appeal ruled in favour of the claimants, a decision which is expected to open the gates for individual users requesting damages for illegal tracking.[3] The marketing industry has invested significantly in online advertising and such investments are expected to increase: revenues from digital advertising in the US are expected to grow and overtake other platforms, and indeed digital advertising is projected to overtake TV as the biggest advertising category by the end of 2017.[4] This means that the advertisers are in urgent need of finding efficient ways to gain the highest possible return for every advertisement they place on the Internet. Surveys show that consumers are more likely to click on an advertisement relevant to their preferences, previous online purchase history or location, rather than on an irrelevant one.[5] Marketers talk about a personalised experience for users, a digital one-to-one marketing, helpful to the consumer, who is being 'served' with information based on their own habits. However, targeted advertisement is only the end result of a process, which involves users being tracked across the Internet and various entities gathering, storing, processing data and developing consumer profiles. What appears as a change in marketing methods of approaching prospective consumers—personalised over mass marketing—involves a new industry behind this 'web personalisation', consisting of various stakeholders, such as web providers, ad delivery

1 O.Tene, 'The European Privacy Judicial Decision Of A Decade: Google V. Vidal-Hall' (Privacyassociation.org, 2015) <https://privacyas sociation.org/news/a/the-european-privacy-judicial-decision-of-a-de cade-google-v-vidal-hall/> accessed 28 March 2016

2 Google Inc v Vidal-Hall & Ors [2015] EWCA Civ 311 (27 March 2015).

3 The case is pending before the UK Supreme Court, which on 28th July 2015 has granted permission to Google to appeal in part the Court of Appeal of England and Wales' decision. <https://www.supremecourt.uk/news/permission-to-appeal-decisions-28-july-2015.html> accessed 25 September 2016.

4 K Matsa and others, 'Digital Advertising and News' (Pew Research Center's Journalism Project, 2012) <http://www.journalism.org/2012/02/ 13/digital-advertising-and-news/> accessed 28 March 2016; Sydney Ember, 'Digital Ad Spending Expected to Soon Surpass TV' The New York Times (7 December 2015) <https://www.nytimes.com/2015/12/07/business/media/digital-ad-spending-expected-to-soon-surpass-tv.html?_r=0> accessed 25 September 2016.

5 L Perscetto, 'Online Advertising and Privacy Survey Shows Consumers Hold Strong Preference For Targeted Advertising – Audiencescience' (AudienceScience, 2004) <http://www.audiencescience.com/online-advertising-and-privacy-survey-shows-consumers-hold-strong-preference-fortargeted-advertising/> accessed 15th October 2015.

companies, web developers, and others. Behavioural tracking and online behavioural advertising support a new section of the Internet economy, in which the major currency is users' data.

But how did we go from 'On the Internet nobody knows you are a dog'[6] to 'I know what you will do next summer'? The technologies used to track consumers' browsing behaviour are advanced and constantly improving. Tracking cookies, but also other technologies serving tracking purposes, such as Web-bugs, HTML 5, evercookies, etc., gather the ID trails of users, while they browse the Internet, and compile personal profiles. A wide range of data is used for this profiling, varying from IP addresses, gender, nationality, zip codes, age, marital status and other demographic data, to consumer preferences as to types of products, services, etc. As EPIC states: '*In the offline world this would be comparable to having someone follow you through a shopping mall, scanning each page of every magazine you browse, every menu entry you read at the restaurant*'.[7] Behavioural tracking is often organized and persistent to such an extent that it is compared to monitoring and surveillance, especially when it is possible for the consumers' profiles to be linked to personal data, which render the data subject identifiable, such as names, ID numbers, credit card numbers, and social service numbers.

The European Commission, along with the US Federal Trade Commission, are promoting the so-called Do Not Track (DNT) initiative, which is based on the idea of giving users the opportunity to opt out from tracking for purposes including behavioural advertising. To this end, Mozilla has introduced the DNT header to Firefox, while Microsoft has deployed Tracking Protection Lists in Internet Explorer 9 (IE9). Reactions from the industry supportive of web personalization were intense, especially from the advertising providers, who claimed for example with regard to DNT headers, that the 'implementations from Microsoft and Mozilla undermine the balance in today's ad-supported Internet ecosystem'.[8]

Negotiations on the standardization of the DNT header started in 2011 at the World Wide Web Consortium (W3C) in order to provide a uniform technological solution on how to express user preferences. Currently, there are two documents under development by the

[6] P Steiner, The New Yorker, vol 69 (LXIX, 1993) no 20 p 61.
[7] Electronic Privacy Information Center EPIC (Washington), Privacy International London, Privacy and Human Rights, An International Survey of Privacy Laws and development, Washington, 2005 p112.
[8] S Taplinger, 'DAA To Senate: For Consumer Choice, Build On What Already Works j Thedma.Org' (thedma.org, 2013) <http://thedma.org/news/daa-to-senate-for-consumer-choice-build-on-what-already-works/> accessed 28 March 2016.

W3C Tracking Protection Working Group; the Tracking Preference Expression (DNT) and the Tracking Compliance and Scope. Both documents have received the status of W3C Candidate Recommendation.[9] The Tracking Preference Expression defines the DNT request header for expressing the user's preference in relation to tracking, while the Tracking Compliance and Scope document presents practices which allow the receiver of the request to comply with the user's preference. From a European perspective, the alignment of several DNT practices with the European Data Protection legislation is questionable, as it will be discussed below.

This article wishes to examine the added value of the DNT initiative with the EU data protection legislation. In order to answer this research question, the article aims to achieve three goals: first, to examine DNT as a solution addressing tracking and profiling issues at (Internet) user level, empowering the user with choice on tracking. Secondly, it aims to study DNT as an initiative implemented in different ways by diverse stakeholders: regulators, industry, privacy advocates. The stated intentions of the stakeholders are in favour of DNT and thus mostly not mutually exclusive. In reality however, the different approaches are neither coordinated, nor aligned in order to achieve a strong widely accepted DNT mechanism, especially on issues relating to the regulation of data protection and privacy.[10] Thirdly, the contribution seeks to identify the potential added value of DNT initiatives and in particular the W3C DNT standard(s) and their relationship and compatibility with the EU data protection legislation.

This article first briefly examines why and when users need to be protected against behavioural tracking and profiling, what the EU legislative instruments are and what are their shortcomings and gaps with regard to sufficient protection to the individual from tracking practices. It then analyses the background of the DNT initiatives; its roots and development in the US, the acceptance and implementation by industry and

[9] According to the World Wide Web Consortium Process Document, the stages for W3C Technical Reports are: Working Drafts, Candidate Recommendations, Proposed Recommendations and W3C Recommendations. In relation to Working Drafts: 'A Working Draft is a document that W3C has published for review by the community, including W3C Members, the public, and other technical organizations. Some, but not all, Working Drafts are meant to advance to Recommendation'. Further, 'a Candidate Recommendation is a document that satisfies the Working Group's technical requirements, and has already received wide review'. See World Wide Web Consortium Process Document of 1st September 2015, <http://www.w3.org/2015/Process-20150901/>.

[10] For instance 'big data', the 'right to be forgotten' and 'privacy by design' are a few examples of new attractive data protection terms that are widely used, discussed or endorsed by diverse parties without concrete agreed meaning.

endorsement by the US legislature. Finally, the article examines and critically analyses the relevance of the proposed international W3C DNT standards and the DNT initiatives in general to the EU legislation on personal data protection. The last section summarises the conclusions of the article.

2. Behavioural tracking: when and why do we need protection?

2.1. Behavioural tracking and profiling

The International Working Group on Data Protection in Telecommunications, commonly known as the 'Berlin Group', provides a definition of web tracking:

"*The collection, analysis and application of data on user activity from a computer or device while using various services of the Information Society (the Web).*"[11]

Similarly, online behavioural tracking has been defined as the act or process of following Internet users' online actions and/or habits and retaining of information, when they are using the World Wide Web.[12] Most often, behavioural tracking is part of a profiling procedure. Profiling is the process of inferring a profile ('profile generation') and the process of treating persons in light of this profile ('profile application').[13] Hildebrandt defines profiling as:

[11] International Working Group on Data Protection in Telecommunications, 'Working Paper on Web Tracking and Privacy: Respect for context, transparency and control remains essential', 53rd meeting, 15–16 April 2013, Prague, available online at<http://www.datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-intelecommunications-iwgdpt/working-papers-and-common-positionsadopted-by-the-working-group> accessed 25 September 2016. As there is no commonly accepted definition of web tracking, the Berlin Group relies on the work of Rob van Eijk on Online Behavioural Advertising.

[12] P Eckersley, 'What Does The "Track" In "Do Not Track" Mean?' (Electronic Frontier Foundation, 2011) <https://www.eff.org/deeplinks/2011/02/what-does-track-do-not-track-mean> accessed 28 March 2016.

[13] L Bygrave, 'Minding The Machine: Art. 15 Of The EC Data Protection Directive And Automated Profiling' (2001) 17 Computer Law & Security Review <http://www.sciencedirect.com/science/article/pii/S0267364901001042> accessed 25 September 2016. Bert-Jaap Koops, 'Some Reflections On Profiling, Power Shifts, And Protection Paradigms' Mireille

> "*the process of discovering correlations between data in databases that can be used to identify and represent a human or a nonhuman subject (individual or a group) and/or the application of profiles (sets of correlated data) to individuate and represent a subject or to identify a subject as a member of a group or a category*."[14]

Online Behavioural Advertising uses profiling broadly. It enables the personalisation of the advertisement to the user's interests and preferences. The detailed profile is the result of a procedure of collecting and correlating data so that the user receives advertisements relevant to products and services they would like to see or purchase.

The first stage of profile generation is the gathering of data. The collection of data of Internet users about their online behaviour or demographic data for the purpose of profiling is realized through the use of several tracking technologies.[15] A common and broadly used technology for performing behavioural tracking is cookies.[16] Cookies may

Hildebrandt and Serge Gutwirth (eds), Profiling the European Citizen (1st edn, Springer 2008) 326, makes a different distinction, identifying three stages of profiling: (i) the pre-profiling stage, which involves the collection and storage of data, (ii) the profile making, which involve the analysis of data collections in order to make profiles, and (iii) the profile use, which involves the application of a profile in a concrete case.

[14] M Hildebrandt and S Gurtwith (eds), Profiling the European Citizen (Springer 2008) 19.

[15] Search engine queries are not included in this definition, due to the different way of function. They are related to contextual advertising, which is different from Online Behavioural Advertising. On analytics: Steve Rosenbush, 'Facebook Exec Says Data Analysis Had 'Huge Impact' On Mobile Revenue' (WSJ, 2013) <http://blogs.wsj.com/cio/2013/10/30/facebook-exec-says-data-analysis-had-huge-impact-on-mobile-revenue/> accessed 28 March 2016.

[16] Apart from traditional HTTP cookies, flash cookies are also widely used for tracking purposes. See A M McDonald, 'Footprints Near The Surf: Individual Privacy Decisions In Online Contexts' (Doctor of Philosophy (PhD), Canergie Mellon University 2010). Flash cookies can also be used to recreate cookies, which the Internet user has previously deleted. See J Chester, 'Cookie Wars: How New Data Profiling And Targeting Techniques Threaten Citizens And Consumers In The "Big Data" Era' Gutwirth and others (eds), European Data Protection: In Good Health? (1st edn, Springer 2012) 24. Researchers from Carnegie Mellon University found that thousands of web sites use flash cookies with codes, which result in unblocking cookies Internet Explorer blocked by default. P G Leon and others, Token Attempt: The Misrepresentation of Website Privacy Policies through the Misuse of P3P Compact Policy Tokens (2010) <http://cylab.cmu.edu/research/techreports/2010/tr_cylab10014.html> accessed 25 September 2016. Another example of a technology used for tracking is web beacons (otherwise called 'web bugs', 'clear GIFs', '1 by 1 GIFs', 'pixel tags'), which are graphics or small images set on a web page. They are invisible to the Internet user and their purpose is to monitor who is reading the web page and provide data to the server. When combined with a cookie, the web bug can identify information such as the web page visited, the time of visit, and other details. Read on
web beacons, J C Sipior, Burke T Ward and Ruben A Mendoza, 'Online Privacy Concerns Associated With Cookies, Flash Cookies, And Web Beacons' (2011) 10 Journal of Internet Commerce. W T Harding, AJ Reed and R L Gray, 'Cookies And Web Bugs: What They Are And How They Work Together' (2001) 18 Information Systems Management 23. The art 29 Data Protection Working Party

be first party cookies (set by entities that operate the website visited by the user) or third party cookies (set by entities that do not operate the website visited by the user).[17] Any type of data may be used for the creation of a profile for Online Behavioural Advertising purposes: demographic, media, survey, purchasing and psychographic data are used to determine the exact profiles that are most likely to buy specific products and services.[18] The gathering of the data is followed by the creation of the user profile(s). Profiling techniques evoke aggregation of data and combination of seemingly irrelevant information. Hildebrandt notes that without these techniques, tracking technologies merely generate data.[19] The data that are collected are 'processed by calculation, comparison and statistical correlation software',[20] which create profiles with the combination of the collected data through analysis of particular patterns.[21] Profiles can be individual profiles of users, but most commonly they are group profiles of users sharing a common preference, location, or something else. Website visits, purchases, hobbies, movies watched, age or age range, location(s), and other pieces of information may be the common denominator of a group profile. The profiles are grouped with labels that facilitate the work of advertisers, such as 'football lovers' or 'current affairs

(hereafter WP29), in its Opinion 9/2014, notes that also device fingerprinting can be an alternative to HTTP cookies for tracking or analytics. The WP29 highlighted the risks that device fingerprinting entails for users, as it facilitates tracking by third parties, drawing particular attention to the fact that device fingerprinting is a covert operation that eliminates any chance for reaction from the users. Read art 29 Working Party, Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting, WP 224, November 2014, p 4. In the context of the Internet Engineering Task Force device fingerprinting has been defined as 'the process of an observer or attacker uniquely identifying (with successfully high probability) a device or application instance based on multiple information elements communicated to the observer or attacker'. A Cooper and others, 'RFC 6973: Privacy Considerations for Internet Protocols' (Hjp.at, 2013) <http://www.hjp.at/doc/rfc/rfc6973.html> accessed 28 March 2016.

[17] Art 29 Data Protection Working Party, Opinion 4/2012, p 5. Read also, B Krishnamurthy and Craig E Wills, 'On The Leakage Of Personally Identifiable Information Via Online Social Networks' (2010) 40 ACM SIGCOMM Computer Communication Review. C E Wills and M Zeljkovic, 'A Personalized Approach To Web Privacy: Awareness, Attitudes And Actions' (2011) 19 Info Mngmnt & Comp Security 53.

[18] Federal Trade Commission, 'Online Profiling A Report To The Congress' (2000), ft 18.

[19] M Hildebrandt, 'The Future Of Identity In The Information Society, Challenges And Opportunities' K Rannenberg and others (eds), The Future of Identity in the Information Society: Challenges and Opportunities (1st edn, Springer Science & Business Media 2009) 284.

[20] Recommendation CM/Rec (2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling, Adopted by the Committee of Ministers on 23 November 2010 at the 1099th meeting of the Ministers' Deputies.

[21] Solove argues that Data mining is also used for surveillance purposes by public authorities (governments, etc) in order to prevent threats to public security, such as terrorist attacks, Daniel Solove, 'Data Mining And The Security-Liberty Debate' (2008) 75 The University of Chicago Law Review 343–62.

enthusiasts'.[22] Such group profiles may not include names or addresses. However, behavioural targeting data can be used to 'single out' individuals, by tying a name to behavioural targeting data[23] and thus render them identifiable.[24]

2.2. When and why do we need protection

A main issue of tracking and profiling for targeted advertising is the fact that Internet users are in most cases unaware of the tracking activity.[25] Tracking is usually 'invisible', performed in such a way that would require knowledge beyond that of an average Internet user to notice the tracking activity, often it would require the knowledge of an expert to prevent it. Unlike HTTP functional cookies, tracking cookies often have a distant expiration date.[26] If the user is not aware of their existence, in order to delete them, then tracking cookies will track him or her for long periods of time. Questions are therefore raised on whether the tracking activity as part of profiling threatens the right to respect for private life and data protection of users.

[22] England and Wales Court of Appeal, Google Inc v Vidal-Hall, ibid. Read also R E Leenes, 'Reply by Ronald Leenes (TILT): Addressing the Obscurity of Data Clouds' (17 April 17 2009). TILT Law & Technology Working Paper No 012/2009, http://ssrn.com/abstract.1393193 accessed 25 September 2016, p 2.

[23] F J Zuiderveen Borgesius, 'Singling Out People Without Knowing Their Names – Behavioural Targeting, Pseudonymous Data, And The New Data Protection Regulation' (2016) 32 Computer Law & Security Review.

[24] See also art 29 Working Party 2007, WP 136. Another categorization of the profiles, inferred by the WP29, is between predictive and explicit profiles, where explicit profiles are based on the information provided by the users of an online service themselves, and predictive 'established by inference from observing individual and collective user behaviour over time' Art 29 Working Party 2010, WP 171, p 7.

[25] Read on attitudes and knowledge of consumer participants in a survey conducted by the Institute for Information Law of the University of Amsterdam and overview of other surveys in the EU and US in R van Eijk and others, 'Online Tracking: Questioning The Power Of Informed Consent' (2012) 14 info, Emerald Group Publishing Limited. S Taplinger, 'DAA To Senate: For Consumer Choice, Build On What Already Works j Thedma.Org' (thedma.org, 2013) <http://thedma.org/news/daa-to-senate-for-consumer-choice-build-on-what-already-works/> accessed 28 March 2016.

[26] A session cookie is valid only for one session and is deleted after the user exits the browser. On the other hand, 'persistence is a technique implemented by Application Delivery Controllers that ensures requests from a single user are always distributed to the server on which they started. . .Without this capability, applications requiring load balancing would need to find another way to share session information or resort to increasing session and connection time outs to the point that the number of servers needed to support its user base would quickly grow unmanageable'. L. MacVittie, Cookies, Sessions, and Persistence, White paper, FP5 Networks, July 2008, <https://f5.com/resources/white-papers/cookies-sessions-and-persistence> accessed 25 September 2016.

A recent Eurobarometer survey conducted in March 2015 showed that two-thirds of respondents (67 per cent) are concerned about not having complete control over the information they provide online.[27]Moreover, a majority of respondents (53 per cent) say they are uncomfortable about online digital advertising and profiling, of whom 17 per cent say they are very uncomfortable and 36 per cent fairly uncomfortable. The report shows that the 'targets' of the targeted advertising lack substantial knowledge about Online Behavioural Advertising, its function and purposes. This lack of awareness is a decisive factor for the users, as it makes it impossible for them to protect themselves from unwanted tracking and Online Behavioural Advertising. After all, 'it is difficult to opt-out from something you do not know'.[28]

Other potential risks relate to surveillance, service discrimination, and the so-called 'filter bubble'.[29] In relation to surveillance, even though the primary purpose of online behavioural tracking as examined in this article is targeted advertising, one should not disregard the possibility of the information collected and collated about individuals being requested for law enforcement or other purposes. This would pose a threat to the presumption of innocence and the right against self-incrimination, but it could also limit freedom of expression, as the person— if aware of the potential for access by law enforcement entities—could limit opinions and ideas he or she receives and shares, due to fear of interference by public authorities. The risk of further use of the profiles is also a real one. Website operators usually include clauses limiting their liability for further disclosure of the collected data in their Privacy and Cookie Policies. Hoofnagle recommends handling online advertising and third-party tracking as a security threat,[30] arguing that online advertising and security interests are conflicting. According to a study conducted on behalf of the European Union Agency for Network and Information Security (ENISA), service and price discrimination can be customized to the users with the aid of tracking and profiling.[31] Previous purchases or repeated interest in a service

[27] European Commission, 'Data Protection Eurobarometer. Report', Special Eurobarometer 431, June 2015.
[28] W G, 'Internet Tracking: Stalking or a Necessary Tool for Keeping the Internet Free?' (2011) 20 CommLaw Conspectus 223, 2011–012.
[29] E Pariser, The Filter Bubble (Penguin Press 2011).
[30] C J Hoofnagle, Federal Trade Commission Privacy Law And Policy (CUP 2016).
[31] Claude Castelluccia and Arvind Narayanan, 'Privacy Considerations Of Online Behavioural Tracking' (European Network and Information Security Agency 2012) <https://www.enisa.europa.eu/activities/identityand-trust/library/deliverables/privacy-considerations-of-online-behavioural-tracking> accessed 28 March 2016.

may influence the prices the user is offered for products or services, even though they might be of the same quantity and quality.

Last but not least is the 'filter bubble', a term first coined by Eli Pariser,[32] who compared information that various individuals receive from the web. Such information is tailored to one's own beliefs and preferences, creating a virtual 'filter bubble'. Past interests, searches, and browsing history determine the future information each user receives, leaving a broad range of different perspectives, opinions, and news out of this user's reach. Gutwirth and De Hert also draw attention to profiling activity that leads to the accumulation of power by entities that produce it and to the loss of control by individuals.[33]

3. The DNT initiative: an attempt to deal with user tracking and profiling

3.1. Tracing the roots of DNT

The DNT initiative was launched in the USA. The absence of legislation on data protection at the federal level created a need for the industry itself (advertising networks, website providers, etc.) to respect the privacy of the consumers and allow them to decide whether they wished to be tracked (or not). DNT started as an initiative similar to the National Do Not Call Registry in the USA, which is a self-registration list of consumers that do not want to receive telemarketing calls.[34] The Do Not Call Registry was established due to consumer complaints about advertisers calling them to promote products or services. The Federal Trade Commission (FTC) started the initiative in order to facilitate a distinction between the consumers who wanted to receive commercial calls and those who did not. The second category of consumers can register their wish not to be called for advertising purposes on the FTC website. The advertisers can access the list

[32] Pariser (n 30).
[33] S Gutwirth and P de Hert, 'Regulating Profiling In A Democratic Constitutional State', in H Mireille, G Serge (eds), Profiling the European Citizen: Cross-Disciplinary Perspectives (1st edn, Springer Science . Business Media BV 2008).
[34] The US National Do Not Call registry, managed by the Federal Trade Commission, <https://www.donotcall.gov/> accessed 20 September 2016.

and verify whether the persons they intend to call are listed. In order to avoid potential misuse of the list, the FTC took measures for limiting the access to the Do Not Call Registry.[35] This initiative is a means to offer choice to consumers, and allow them to express their preference on a marketing call from advertisers.

The DNT is based on a similar logic of empowering the data subject, but for online advertising. The proposal for the DNT was submitted in 2007 to the Federal Trade Commission by consumer protection associations and privacy advocates.[36] The original idea of DNT was to create a national list similar to the Do Not Call Registry, as a first step to offer transparency to consumers in relation to tracking and targeting activities. According to the proposal, 'any advertising entity setting a persistent identifier on a user device should be required to provide to the FTC the domain names of the servers or other devices used to place the identifier'.[37] Furthermore, the group of privacy advocates proposed that companies providing browser applications should provide a functionality (i.e. a browser feature, plug-in, or extension) that allows users 'to import or otherwise use the DNT List of domain names, keep the list up-to-date, and block domains on the list from tracking their Internet activity'.[38]

3.2. Implementation by industry: the example of Microsoft and Mozilla

The security and privacy researcher Christopher Soghoian and the Mozilla privacy engineer, Sid Stamm claim to have developed a prototype add-on for Firefox in July 2009.[39] The idea was inspired by the initial proposal of consumer organizations and privacy advocates, but was actually changed quite significantly, as DNT was suggested as a browser header.[40] The rationale was that the header employed a decentralized design and avoided in this way 'the substantial technical and privacy challenges inherent to compiling, updating, and sharing a comprehensive registry of tracking services or web

[35] Sellers About DNC Provisions In TSR Federal Trade Commission' (Ftc.gov) <https://www.ftc.gov/tips-advice/business-center/guidance/qatelemarketers-sellers-about-dnc-provisions-tsr#accessingtheregistry> accessed 28 March 2016.
[36] See document: <https://www.cdt.org/files/privacy/20071031consumer protectionsbehavioral.pdf> accessed 20 September 2016.
[37] See document: ibid.
[38] ibid.
[39] <http://paranoia.dubfire.net/2011/01/history-of-do-not-track-header.html> accessed 20 September 2016.
[40] Centre for Democracy and Technology, The History of the Do Not Track Header, 31October 2007.

users'.[41] As Mayer and Narayanan, explain, the DNT signals a user's opt-out preference with an HTTP header.[42]

The DNT mechanism is a browser setting that offers users the choice to allow (or not) the tracking of their online activities. The main idea is that the browser enables 'privacy', thus offering the capability to the user to choose protection against any tracking technology, tracking entity without territorial limitations. The mechanism sends a signal ('header') to the tracking entity that the user wants or does not want to be tracked. The header (DNT) recognizes three signals ('values'): (1) signifies the wish of the user not to be tracked, (0) means that the user wishes to be tracked and (null) means that the user has not set his or her preference.[43]

In July 2010, the Wall Street Journal published an article based on an experiment about tracking technologies (cookies, beacons, etc.) that the 50 most popular websites in the US place on user's computer.[44] The 50 websites had stored 3180 tracking files on one computer alone.[45] A few months later, in December 2010, the FTC published a report introducing the 'Do Not Track' mechanism as a suggestion for the businesses and policymakers. In its preliminary staff report, the FTC urged the industry to provide consumers with a 'simple "Do Not Track" mechanism' that would allow them to choose whether they want to allow websites to collect information about their Internet activity and use it to deliver targeted advertisements and for other purposes.[46] The FTC envisaged DNT as a universal browser-based mechanism that could be accomplished by legislation or through 'robust, enforceable self-regulation'.[47] The report emphasizes that a DNT mechanism should ensure that the consumer choice would not have to be asked on an industry-by-industry or company-by-company basis and that the choices would be persistent. It is also acknowledged however that the consumers may wish for a more

[41] Jonathan Mayer and Arvind Narayanan, 'Do Not Track - Universal Web Tracking Opt Out' (Donottrack.us) <http://donottrack.us/> accessed 28 March 2016.
[42] Ibid. Read also: Arvind Narayanan, '"Do Not Track" Explained' (33 Bits of Entropy, 2010) <http://33bits.org/2010/09/20/do-not-track-explained/> accessed 28 March 2016.
[43] Mozilla Firefox version 25.0.1.
[44] 'Tracking The Trackers: Our Method' (WSJ, 2010) <http://online.wsj.com/news/articles/SB10001424052748703977004575393121635952084>accessed 28 March 2016.
[45] The Wall Street Journal, 'What They Know' (WSJ) <http://blogs.wsj.com/wtk/> accessed 28 March 2016.
[46] 'Do Not Track j Federal Trade Commission' (Ftc.gov) <https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/do-nottrack>accessed 28 March 2016.
[47] Federal Trade Commission, 'Protecting Consumer Privacy In An Era Of Rapid Change: A Proposed Framework For Businesses And Policymakers' (Federal Trade Commission 2010) 66.

granular mechanism offering them the possibility to choose the types of advertisements. Two years later, in its recommendations report, the FTC announced Bills which addressed the creation of DNT mechanisms as pending in the White House and the Senate.[48]

One of the first debates about DNT was about the default setting (value) of DNT; whether the default would be the tracking or not tracking preference.[49] The discussion started when Microsoft set the value (1) (do not allow tracking), as the default setting in Internet Explorer 10.[50] This setting practically entails that unless the user actively changes the setting to value (0), the tracking entity should not track the user. This setting is obviously the most-privacy-friendly, as it protects even users that are not aware of the tracking activity. Privacy by default advocates, who support the enforcement of privacy settings by default, argue that the preference DNT (1) should be the default setting. On the other hand, against privacy by default are many advertising networks and advertisers, who see this setting as a major loss of profit. They claim that users tend to be reluctant to change the default settings of their equipment[51] for reasons of security or due to lack of knowledge. As a result, advertising networks would not have the opportunity to reach out prospective consumers, who might be interested in tailored advertising. Although both sides may have reasonable arguments, it seems that protection by default is gaining ground, at least in the European Union, as protection by 'default' is included as an obligation in the General Data Protection Regulation.[52]

The implementation of DNT as a form of self-regulation by the industry, has the significant shortcoming, that compliance of the tracking entity with the DNT preference of the user is not enforceable. The compliance depends on the companies themselves.[53]

[48] Ibid.
[49] J Fairfield, 'Do Not Track as Default', (2013) 11(7) Northwestern Journal of Technology and Intellectual Property.
[50] C Albanesius, 'Internet Explorer 10 Released For Windows 7' (PCMAG, 2012) <http://www.pcmag.com/article2/0,2817,2412077,00.asp> accessed 28 March 2016.
[51] J Spool, 'Do Users Change Their Settings?' UIE Brain Sparks (Uie.com, 2011) <http://www.uie.com/brainsparks/2011/09/14/do-users-changetheir-settings/> accessed 28 March 2016.
[52] See Recital (78) and art 25 (2) of the General Data Protection Regulation. However, the actual meaning of privacy by design and privacy by default in the context of the General Data Protection draft is not clear. Read further: B-J Koops and R Leenes, 'Privacy Regulation Cannot Be Hardcoded. A Critical Comment On The "Privacy By Design" Provision In Data-Protection Law' (2013) 28 International Review of Law, Computers & Technology.
[53] Several companies have declared they will honour Do Not Track signal. See Do Not Track Implementations <http://donottrack.us/implementations> accessed 20 September 2016.

The voluntary self-commitment of the companies is jeopardised by the diversity of the implementation of DNT in each browser. The most illustrative example is the abovementioned Microsoft Internet Explorer 10 and the reaction of companies to its settings by not respecting the preference of the user not to be tracked.[54] After two years of implementation of the DNT as default state in the Internet Explorer browser, Microsoft announced that the upcoming versions of the browser would no longer implement the DNT as default. The company based this policy change on the argument expressed by W3C, the standardization consortium, that a default DNT setting does not reflect the user's deliberate choice and preference. For reasons of alignment with the DNT standard which is currently under development by W3C but also in order to deprive the signal receivers from any excuses not to honour the Not tracking signal, the company committed to continue supporting the DNT initiative by keeping the feature on the IE browser and providing clear information to the customers on how to turn on the feature, according to their wishes.[55]

3.3. The W3C Do Not Track standard

The W3C, the international standardization community for the development of standards for the World Wide Web, undertook to host the discussions for the development of a technical standard in order to respond to the problem of diverse implementation of the DNT. The initiative from the W3C responds to the need for a universal common approach to the DNT header guaranteed by an international organization. The W3C is an organization with significant work in the field of the Internet and the World Wide Web. In September 2011, the Tracking Protection Working Group was formed, with wide participation from stakeholders representing several groups with contrasting views and interests, such as experts from advertising networks including the Interactive Advertising Bureau, the Digital Advertising Alliance, eBay, Apple, Facebook, Yahoo,

[54] Stephen Shankland, 'Apache Web Software Overrides IE10 Do-Not-Track Setting' (CNET, 2012) <http://news.cnet.com/8301-1023_3-57508351-93/apache-web-software-overrides-ie10-do-not-track-setting/> accessed 28 March 2016.

[55] Microsoft, An update on Microsoft's approach to Do Not Track, Microsoft Corporate Blogs, 3 April 2015.

Google, Mozilla Foundation, Opera, Microsoft, Electronic Frontier Foundation, Future of Privacy Forum, and Stanford University.[56]

The progress of the Working group has been particularly slow, raising questions about the achievement of a high-quality outcome widely accepted by the participants.[57] The delays were due to the disagreement of the participants on crucial matters. The Working Group could not reach an agreement—after over two years since the launch of the discussion—for a definition of 'tracking' and the scope of DNT. Moreover, open issues concerning the exemptions, the distinction between first parties and outsourcing service providers acting as first party were substantial obstacles to the progress of the standard.[58]

The Working Group has decided to produce two documents instead of one: the 'Tracking Preference Expression' and the 'Tracking Compliance and Scope'.[59] The TPE defines the DNT request header field as an HTTP mechanism for expressing the user's preference regarding tracking, while the Tracking Compliance and Scope defines 'a set of practices for compliance with a user's Do Not Track (DNT) tracking preference to which a server may claim adherence'.[60] The choice of division of the DNT standard into two different documents regulating two stages of the same process (the indication of user preference and the compliance of the receiver with this preference) raises questions as to the completeness and comprehensiveness of the standard. A stand-alone Compliance and Scope standard could lead to inconsistent implementation of the standard, which weakens rather than strengthens the DNT initiative. In other words, the Tracking Preference standard has limited value in protecting the users if companies do not follow the Compliance and Scope standard.[61]

[56] See the full list of participants on the website of W3C: http://www.w3.org/2000/09/dbwg/details?group.49311&public.1

[57] See for example: K Kaye, 'Do-Not-Track On The Ropes As Ad Industry Ditches W3C' (Adage.com, 2013) <http://adage.com/article/privacyand-regulation/ad-industry-ditches-track-group/244200/> accessed 28 March 2016, J Aquino, J Mayer To "Do Not Track" Working Group: I Quit j Adexchanger' (AdExchanger, 2013) <http://www.adexchanger.com/online-advertising/jonathan-mayer-to-do-nottrack-working-group-i-quit/> accessed 28 March 2016; D Auerbach, 'Ad Industry's Assault On "Do Not Track" Continues At The W3C Amsterdam Meeting' (Electronic Frontier Foundation, 2012) <https://www.eff.org/deeplinks/2012/10/ad-industrys-assault-do-not-track-continues-w3c-amsterdam-meeting> accessed 28 March 2016.

[58] Tracking Preference Expression (DNT)W3C , W3C Candidate Recommendation 20 August 2015, <http://www.w3.org/TR/trackingdnt/>accessed 15 June 2016.

[59] Tracking Compliance and Scope W3C Candidate Recommendation 26 April 2016, <http://www.w3.org/TR/tracking-compliance/> accessed 15 June 2016.

[60] Tracking Preference Expression (DNT)W3C, Abstract.

[61] See p. 3 of the article on the status of the two W3C documents.

Independent of the evolution of the specific W3C DNT standards, the idea of a standardized mechanism to set the preference of the user has many positive aspects. Firstly, standards are technical specifications which provide best practices: efficient solutions in a given situation for an intended goal. In that respect, a standardized DNT mechanism would be an easy, efficient tool for both the user expressing his or her preference on tracking, and the entity receiving the signal. In addition, a standardized mechanism guarantees consistent application and interpretation of what DNT means. Secondly, standards-development in organizations such as W3C is transparent and open, thus providing guarantees for a legitimate outcome, which does not favour the interests of one party or the other. Thirdly, a standardized DNT mechanism would score high in usability for the data subject, as issues of usability of the standard are usually taken into account in the development process. Fourthly, the element of participation in such standardization processes as in W3C is crucial for a positive outcome. Privacy advocates and representatives of civil rights groups would ensure that data subjects' interests are properly considered and promoted. At the same time, the active participation of trackers, browser companies and others, is a significant preliminary guarantee for further commitment to respect the preference of the user. Since a standard is voluntary, the broader the participation in the standard development process, the higher the acceptance of the outcome.

3.4. Implementation by the legislature: the example of the DNT transparency law in California

Besides the implementation by the industry and the standardization efforts in W3C, the first law to support DNT was put in force in 2013 in California. The California Online Privacy Protection Act (CalOPPA) requires the operators of websites or online services to display a privacy policy which, among other things, discloses the categories of Personally Identifiable Information (PII) that are gathered via the website and others.[62] The law was amended in 2013 in order to require additional information disclosures from the website operators to the consumers of the website. In particular, in line with the discussion on the

[62] B Hengesbaugh and Amy de La Lama, 'How Should I Respond To California's Do-Not-Track Requirements?' (Privacyassociation.org, 2013) <https://privacyassociation.org/news/a/how-should-i-respond-to-californias-do-not-track-requirements> accessed 28 March 2016.

DNT initiative, the law requires information to be disclosed on how the operators respond to the DNT signals.

The amended section 22575(b)(5) requires that the

Privacy Policy shall:[63]

> "(5) *Disclose how the operator responds to Web browser "do not track" signals or other mechanisms that provide consumers the ability to exercise choice regarding the collection of personally identifiable information about an individual consumer's online activities over time and across third-party Web sites or online services, if the operator engages in that collection*".

The CalOPPA is a disclosure law, requiring transparency in the behaviour of the operators regarding DNT, instead of enforcing the DNT itself. The Attorney General of the California Department of Justice explains that the law does not prohibit online tracking, nor it depends on 'a standard for how an operator should respond to a DNT browser signal or to any mechanism that automatically communicates a consumer's choice not to be tracked'.[64]The aim of the provisions is to allow consumers to make an informed choice. The guidance provided for the implementation of the new obligation, instructs the operators to place a notice that relates to online tracking on an easily accessible place on the website and disclose among other things any third parties that collect PII.[65]

Taking into account the pending standardization of the DNT browser mechanism[66] and the hesitant acceptance of part of the industry towards DNT, this amendment is one positive step towards adding legal substance to the initiative. Such a legal obligation to disclose how the operator responds to DNT signals has legal effects and is enforceable; an operator who says it that does comply with the DNT signal but in reality does not, or has changed its approach without updating the notice and being transparent about this change to website users, violates the above law. Apart from any public mistrust this behaviour might generate, the operator is also liable for this violation and would probably be subject to sanctions. According to CalOPPA, users may claim exceeding

[63] Source: <http://www.leginfo.ca.gov/cgi-bin/displaycode?section.bpc&group.22001-23000&file.22575-22579> accessed 20 September 2016.
[64] H Kamala, 'Making Your Privacy Practices Public. Recommendations On Developing A Meaningful Privacy Policy' (California Department of Justice 2014).
[65] Ibid.
[66] See section on the W3C DNT standard.

authorized access to computers, trespass, and other things, while the California Attorney General may impose pecuniary fines for each violation.[67] In general, transparent policies about the response to DNT are a necessary preliminary ingredient for a future strong DNT regulatory enforcement mechanism.[68] For the moment, the mere obligation for transparency on DNT response offers an important instrument both to the users and the supervisory authority in case of violation, and in that respect CalOPPA marks progress in the debate, as it shows a potential uptake from the regulator. A transparency law could also be one way forward for the EU legislation and DNT, following the example of CalOPPA.

4. Regulatory approaches to tracking and profiling in the EU

4.1. General Data Protection Regulation and profiling

Following the 'constitutionalisation' of the right to data protection,[69] the European Commission proposed a General Data Protection Regulation (GDPR) in order to reform the European Data Protection Directive.[70] After four years of intense political negotiations, the GDPR was published in the Official Journal in May 2016.[71] The GDPR contains specific provisions that relate to tracking technologies and profiling that can be

[67] CalOPPA art A.B. 370.
[68] The concern is that this stronger regulatory enforcement mechanism might not be established in terms of legislation. Enforceability is a one of the major challenges of the DNT initiative.
[69] On the constitutional recognition of personal data protection in the (non-binding at the time) EU 2001 Charter of Fundamental Rights as a separate fundamental right read among others: P de Hert and S Gutwirth, 'Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation In Action' S Gutwirth and others (eds), Reinventing Data Protection? (1st edn, Springer 2009); also G Gonzalez Fuster, The Emergence of Personal Data Protection as a Fundamental Right of the EU (Springer International Publishing 2014).
[70] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM (2012) 11 final, <http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf> accessed 20 September 2016.
[71] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, L 119/1, 4.5.2016.

applicable besides the Article 5(3) of the ePrivacy Directive that will be analysed below.[72] Recital 72 provides that profiling as such is subject to the rules of the Regulation. The Regulation reflects the intent of the European legislature to address the issue with detailed provisions for both tracking and profiling.[73] According to Recital 30 individuals are often associated with online identifiers. The devices the individuals use, applications, tools, and protocols facilitate such association. In the category of 'online identifiers', the Regulation explicitly includes Internet Protocol (IP) addresses thereby, ending the debate on whether the IP addresses may be used to identify the data subject. This is in line with the Opinion of the WP29.[74] Moreover, cookies and Radio Frequency Identification (RFID) tags are also included in the category of online identifiers. Recital 30 describes tracking and profiling as the association of the individuals through the identifiers 'may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them'.[75] The phrase 'in particular', which was not included in the initial EC proposal or the Parliament First reading, leaves open the possibility that the 'traces' left by the association of individuals with online identifiers are used to identify those individuals, even without the use of unique identifiers. Recital 24 sets the criteria to differentiate mere processing from monitoring behaviour (profiling), which are: (i) tracking of individuals on the Internet, (ii) use of personal data processing techniques, and (iii) application of a 'profile' to an individual with the use of these techniques. Additionally, the application of the profile for the purpose of taking decisions concerning the user, or for analysing or

[72] See Recital 173 of the General Data Protection Regulation: 'This Regulation should apply to all matters concerning the protection of fundamental rights and freedom vis-a-vis the processing of personal data, which are not subject to specific obligations with the same objective set out in Directive 2002/58/EC, including the obligations on the controller
and the rights of individuals. In order to clarify the relationship between this Regulation and Directive 2002/58/EC, the latter Directive should be amended accordingly. Once this Regulation is adopted, Directive 2002/ 58/EC should be reviewed in particular in order to ensure consistency with this Regulation.'

[73] Read further: Ir Kamara, 'Behavioural Profiling in the Postconstitutionalisation Data Protection Regime' in A Hoc, S Wattier and G Willems (eds), Human Rights as a Basis for reevaluating and reconstructing the law: Acts of the 4th ACCA Conference held in Louvain-la-Neuve on May 29th, 2015 (1st edn, Bruylant 2016) 385–400.

[74] Art 29 Working Party, Opinion 4/2007 on the concept of personal data,<http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf> accessed 20 September 2016.

[75] Recital 30 GDPR.

predicting his or her personal preferences, behaviours and attitudes, confirms the nature of the processing as 'monitoring'.[76]

Article 21 of the GDPR establishes the general right of the data subject to object to processing of personal data, when this processing is based on the grounds of (e) or (f) of Article 6(1), namely processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority, and processing is necessary for the purposes of the legitimate interests pursued by the controller or a third party. The data subject is in particular granted the right to object to profiling when it is based on any of the above two provisions of Article 6(1). The limitation only to the grounds of (e) or (f) of Article 6(1), leaves out the possibility to object to profiling when this is based on the performance of a contract (Article 6(1)(b)) or the consent of the data subject (Article 6(1)(a)) and on other grounds, thus a considerable amount of profiling cases. The GDPR offers data subjects the right to object to the processing of their personal data for direct marketing purposes, which includes profiling, and the data shall no longer be processed for such purposes.[77]

In the context of the use of information society services, the data subject may exercise his or her right to object by automated means using technical specifications.[78] A technical specification is a document that 'prescribes technical requirements to be fulfilled by a product, process or service'.[79] This provision inserts in the EU legislation a legal basis for a DNT mechanism, expressing the objection of the data subject to profiling for the performance of a task carried out in the public interest and the legitimate interests of the controller of any other party.[80] In practical terms, since the right to object to profiling can be exercised only in specific cases (art. 6(1)(e),(f)), the grounds of processing of art. 6 should be 'translated' in the technical specification in a way that there is a differentiation between the allowed and not allowed grounds for objection. In addition, the specification would need to distinguish between 'direct' and other marketing in order to facilitate such

[76] The Recital (21) reads: '. . . In order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether individuals are tracked on the Internet including potential subsequent use of data processing techniques which consist of profiling an individual, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes'.

[77] Art 21 (3) GDPR.

[78] Art 21 (5) GDPR.

[79] European Parliament and the Council, Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93, OJ L 218/30, 13.8.2008, art 2(8).

[80] See s 3 p.18.

objection of the data subject. In general, even though the final text of Article 21 did not follow the Parliament's proposal for establishing a new separate right to object to profiling and empower significantly the data subject, Article 21 as adopted does provide safeguards and rights that the previous regime lacked. The provision of Article 21(5), which allows the right to object to processing for the grounds of Article 21(1), including profiling, to be exercised using technical specifications. This provision is quite important for the standardization of DNT, as it creates a legal basis for the expression of data subject's wish using a technical standard (specification).

Apart from the right to object to profiling for the above grounds, Article 22 of the GDPR introduces another right, a right not to be subject to a decision based solely on automated processing, which is similar—but not identical—to Article 15 of the Data Protection Directive.[81] Article 22(1) provides:

> "*The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her*."

The substantial elements of the right of the individual not to be subject to a decision based on automated processing of data are that the decision needs to: (i) produce legal effects or significantly affect the individual, and (ii) be based solely on automated processing. Recital 71 provides information on the first condition with the examples of refusal of an online credit application and recruiting practices without human intervention.[82] The new Article 22 does not condition the granting of the right to the intention of the processing; this is rather the evaluation of personal aspects such as creditworthiness, reliability etc. Article 22(2) provides the exceptions to the above right. When the decision based on automated processing is necessary for entering or the performance of a contract between the controller and the data subject, is authorized by law or based on the data subject's explicit consent, the right not to be subject to decisions based on automated profiling shall not be invoked by the data subjects.[83]

[81] Art 15(1) of Data Protection Directive 95/46/EC provides: 'Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.'
[82] Rec (71) GDPR.
[83] Art 22(2) (a), (b), (c) GDPR.

4.2. Article 5(3) of the ePrivacy Directive and its relation to tracking

As cookies facilitate the tracking of individuals, the European regulator has chosen to regulate their installation on the terminal equipment of users and their subsequent uses which facilitate the access to the stored information. The regulation of the installation and use of cookies was incorporated in Article 5(3) of the ePrivacy Directive and has raised heated debates among citizens, policymakers and the industry. The ePrivacy Directive requires that the installation or use of cookies is only allowed when the user or the subscriber has been provided with clear and comprehensive information and has provided his or her consent.[84] The requirement for consent was introduced in 2009 via the Citizens Rights Directive[85] replacing the previous regime that required the provision of clear and comprehensive information and offered the users or subscribers the right to refuse the installation or use of cookies.[86] This transition from a right to refuse to the provision of consent has completely changed the way that cookies should be installed on the terminal equipment of users. The established practices of internet browsers, who were storing cookies on the computers and mobile devices of users by default, allowing them to override this choice in the browser settings, were rendered incompatible with the new requirements. Recital 66 of the Citizen's Rights Directive gives substantial grounds to the application of the TPE standard in the EU. The Recital highlights the importance of clear and comprehensive information provided to the user with user-friendly methods.

The Recital states:

> "*the user's consent to processing may be expressed by using the appropriate settings of a browser or other application*".[87]

The discussion on the applicability of the DNT preference to the EU jurisdiction therefore, is mainly concentrated on the question of whether the TPE fulfils the conditions for valid

[84] Art 5(3) ePrivacy Directive.
[85] European Parliament and the Council of the European Union, Directive 2009/136/EC amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws ('Citizens' Rights Directive') [2009] OJ L337/11 (18.12.2009).
[86] For an analysis of the legislative developments in relation to cookies, see E Kosta, 'Peeking into the Cookie Jar: The European Approach Towards the Regulation of Cookies' (2013) 21 International Journal of Law and Information Technology 380–406.
[87] Rec (66) Citizen's Rights Directive.

consent to the storing or access to information already stored on the user's equipment. As a starting point, in the EU the focus is relocated from the tracking activity as a whole to the subactivities of 'storing' and 'accessing information'[88] and the conditions for their legitimacy.

The provision of consent through the configuration of the browser settings would need to fulfil the requirements of valid consent of the Article 5(3) of the ePrivacy Directive.[89] The choice of the European regulator to require informed consent in relation to cookies has a direct impact on the default settings that should be put in place for the installation of cookies. The Article 29 Working Party argued that the current practices of providing user consent for the installation of cookies do not meet the new requirements of Article 5(3) of the ePrivacy Directive and, even if modified, it would still be very difficult for them to meet the requirements of the Directive.[90]The Working Party expressed the concern that recognizing the accepting consent of users as a default in browser settings could lead to 'erosion of the definition of consent and … subsequent lack of transparency'.[91] The European Commission recognized that the provisions of the ePrivacy Directive relating to tracking "may need to be evaluated in light of the constant evolution of technology."[92] Such a need is even more pressing after the recent adoption of the European GDPR.[93]

[88] It should be noted that in terms of protection of the right to respect for private life, the behavioural tracking activity has different and very significant implications, such as the risk of surveillance by private companies or the public sector. This discussion is not under the scope of this article.
[89] Kosta (n 87).
[90] Art 29 Data Protection Working Party, 'Opinion 2/2010 on online behavioural advertising, WP171' (2010), p 13.
[91] Art 29 Data Protection Working Party, 'Opinion 1/2009 on the proposals amending Directive 2002/58 on privacy and electronic communications (e-Privacy Directive), WP159' (2009), p 10.
[92] Commission Staff Working Document, A Digital Single Market Strategy for Europe - Analysis and Evidence Accompanying the document: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions A Digital Single Market Strategy for Europe, COM(2015) 192 final, Brussels, 6.5.2015, SWD(2015) 100 final, p 47.
[93] 'If the ePrivacy Directive is not transformed into a regulation and remains a directive, it would be necessary to transform it into a selfstanding instrument, after the adoption of the General Data Protection Directive, following the example of the proposed Law Enforcement Directive. As a result there would be two instruments containing provisions on personal data protection with mirroring provisions but on different levels. Moreover, if the scope of application of the ePrivacy Directive will be widened and include services which do not belong to the electronic communications sector in the strict sense, the ePrivacy Directive will no longer address a separate sector but the entire online environment, which is also one of the main targets of the proposed Data Protection Regulation. This overlap will inevitably create a very complex situation': J Dumortier and

4.3. Challenges for implementation of DNT in the EU jurisdiction

The Article 29 Working Party has officially addressed comments to the W3C with regard to the TPE (version of 24 April 2014—Last Call Working Draft).[94] The WP29 stressed the potential of the specification becoming a granular consent mechanism, in line with Recital 66 of the Citizen's Right Directive, but identified the following six important issues that risk undermining the use of the standard from an EU perspective:

- Different terminology from the EU data protection legislation. The WP29 suggested including the following phrase: "This specification does not override regulatory terminology, and as such, compliance with this specification does not mean compliance with regulations".[95]
- The absence of an automatic expiration of a tracking preference.
- The doubt that controllers will honour the tracking preference of the user.
- The lack of a definition of "de-identification".
- The risk of 'undermining valid consent by an ambiguous server response of "potential consent" and ambiguous use of "disregarding".
- The lack of provision for users with special needs.

The Tracking Protection Working Group (WG) received the comments of the WP29 and discussed the issues raised by the WP29. On the issue of definitions, the WG registered the issue as concerning priority of local legislation,[96] and adopted with consensus the

E Kosta, 'Study for the European Commission DG Communications Networks, Content & Technology on the ePrivacy Directive: Assessment of Transposition, Effectiveness and Compatibility with the Proposed Data Protections Regulation, June 2015' https://ec.europa.eu/digital-agenda/en/news/eprivacy-directive-assessment-transposition-effectiveness-and-compatibility-proposed-data accessed 20 September 2016.

[94] Art 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), 6 June 2014, <http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140606_wp29_ts_standardisation_letter_to_w3c.pdf> accessed 20 September 2016.

[95] Art 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), 6 June 2014, Annex.

[96] Issue -244 priority of local legislation, <https://www.w3.org/2011/tracking-protection/track/issues/244> accessed 20 September 2016.

decision not to follow the suggestion of the WP29 to include the relevant phrase.[97] The issue of automatic expiration of preferences seriously concerned the WG,[98] which considered introducing the relevant feature. In relation to the last point raised by WP29, the WG took no action as the experts decided that the issue of user accessibility interface was out of the scope of the specification.[99]

In October 2015, the WP29 responded to W3C's public consultation on the W3C Last Call Working Draft of Tracking Compliance and Scope.[100] The WP29 repeated what had been said in the previous letter of 2014, that the draft specification should be seen as containing building blocks needed for obtaining valid consent. The main issues the WP29 communicated to W3C were related to terminology used in the draft specification, but also the actual content.

- First challenge: terminology

With regard to the terminology, the WP29 observed the differences between the terminology of the draft specification and the regulatory terminology of the EU. Quite importantly, it suggests the addition of the same clarification proposed for the TPE, that compliance with the specification does not mean compliance with regulations, implying in this way that additional steps need to be taken in every individual case to ensure compliance. The respect of the user tracking preference is fundamental, as the mechanism should not be used for blank consent; the user should know in advance to which tracking activities he or she consents. Control of consent to user can be facilitated by the implementation of tools for managing consent at the user agent level. The WP29 also

[97] The response from the Tracking Protection Working Group was to take no action, as this was considered to be an 'obvious' statement that does not need to be included in a technical specification. <https://lists.w3.org/Archives/Public/public-tracking/2014Jul/0055.html> accessed 20 September 2016

[98] Issue-258: automatic expiration of a tracking preference automatic expiration of a tracking preference <https://www.w3.org/2011/tracking-protection/track/issues/258> accessed 20 September 2016, and Issue-266: automatic expiration of a tracking preference exception via API parameter,https://www.w3.org/2011/tracking-protection/track/issues/266 accessed 20 September 2016.

[99] Issue 245: highlighting accessibility in user interface guidelines, <https://www.w3.org/2011/tracking-protection/track/issues/245> accessed 20 September 2016.

[100] Art 29 Data Protection Working Party, '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' 1 October 2015, <https://lists.w3.org/Archives/Public/publictracking-comments/2015Oct/att-0003/20151001_Ares_2015_4048580_W3C_compliance.pdf> accessed 20 September 2016.

raises the issue of two tracking status values: the 'Potential consent' and the 'Disregarding', which could undermine the validity of a consent mechanism in Europe by limiting the scope of the user's tracking preference.[101]

Indeed, the issue of differentiation in terminology is a potential source of confusion and thus could undermine the effectiveness of the W3C standard in the EU jurisdiction. The 95/46/EC Data Protection Directive, as well as the General Data Protection Regulation, include definitions of 'processing', 'consent' etc. It is true that the DNT standard does not address only the collection and processing in general of personal data, but also of other types of information, for instance related to traffic and analytics, which might not in all cases qualify for 'personal data'. However, the fact that some of the tracking data might be personal, and thus should be protected under the specific legislation on personal data protection, demands for a uniform terminology in the standard. Common terminology would ease the work of an entity operating in the EU, having to comply with both the legislation and opting to respect the DNT standard.

- Second challenge: collection, use or both as 'tracking'?

A critical challenge is also the definition of 'tracking' in DNT. A DNT header that only forbids the use of data to track the Internet user does not protect the user from a substantial part of the activity: the collection of the data. The DNT should prevent both collection and use of the data. The EU legislation considers collection as processing operation (Article 2 Data Protection Directive, Article 4(3) GDPR) and thus offers the same level of protection as when there is use of personal data. This is justified by the increased endangerment to fair processing from the collection of data. Also, another argument for protecting against collection of data is that in practice it may be difficult, if not impossible, to follow what happens to the data once collected by the third party trackers, due to the number of entities that track a user, access and share his or her data. As a result, having strict requirements for collection is one way to guarantee that the data will not be misused once collected.

In the opposite case of restricting only the use of data, the data controller would have to keep the data in a format that indicates the wish of the data subject not to use them. And

[101] The reply and resolutions of the WG regarding the issues raised in letter of WP29 are accessible here: <https://lists.w3.org/Archives/Public/public-tracking-comments/2015Dec/0007.html> accessed 20 September 2016.

this would further entail that the indication would follow the data when they are processed by sub-contractors or other entities on behalf of the controller. The question that then arises is why collect such data for advertising purposes, if their use for targeted advertising is not allowed by the user. In relation to the scope of tracking, an important issue is whether DNT covers both first party and third party tracking.[102]

Currently, the Compliance and Scope specification (W3C Candidate Recommendation 26 April 2016) allows the first party entities that receive a Not tracking signal (DNT:1) to collect, retain, and use data, including customising content, services and advertising for the actions of the user. For the first party entity, compliance with the signal means not sharing the data with third parties, as further elaborated upon in section 3.2 of the specification. The current draft provides the flexibility to first party entities to follow the stricter requirements established for the third-party entities, but given that compliance with the specification is achieved in both cases, it is rather unlikely that an entity would self-commit to the stricter regime.

- Third challenge: purpose of 'tracking'

Another challenge is to define whether the purpose of tracking should be an element of the scope of DNT. The FTC report of 2010 refers to DNT as a 'consumer choice mechanism for online behavioural advertising'.[103] Entities that track for any other purpose are therefore out of the scope of the tracking protection according to the FTC approach. This approach raises more issues such as the clarity and transparency of a generic 'Do Not Track' term that would reasonably create an expectation to the user/data subject that the choice refers to tracking in general, not for a very specific case, the one of behavioural advertising. Furthermore, if this approach is followed, a very detailed definition of 'online behavioural advertising' is needed to ensure the uniform application of the standard. Also, this limitation of the scope should be reflected in the title of the header, thus enabling the user to understand the choice he or she makes.

- Fourth challenge: consent overriding DNT preference

In relation to 'consent'—apart from the differentiation in terminology—the WP29 highlighted another important issue related to the DNT standard (the document on

[102] See discussion earlier in this contribution.
[103] Federal Trade Commission, 2010, p.66.

Compliance and Scope in particular). The Compliance and Scope document provides that a party may track a user, when the user has given "explicit and informed consent". Once a party relies on this type of consent to override a Do Not Track preference, it is obliged to indicate it, in the way described in the Tracking Preference Expression (DNT) standard. When it cannot be proven by the data controller that such consent has been unambiguously given for the purposes of tracking, then the WP29 suggested that there should be no assumption that consent has been provided or that the user is aware of the tracking, but rather the data controller has to ask for specific consent for the intended purpose.[104]

- Fifth challenge: default browser settings allowing tracking

Looking at the DNT mechanism beyond the W3C specification, there has been criticism of the browsers that by default allow the storing of information: it is ambiguous to what extent the user knows how to configure the settings on the browser in order to opt-out from tracking. The former European Data Protection Supervisor (EDPS) also commented on the issue of default preference: the EDPS stressed the importance of the default setting being the privacy-friendly option, as many users lack the skills to change the browser settings.[105] The WP29 has strongly objected to the default browser settings as a means to provide prior consent of the user. More specifically, in its Opinion on the amendments to the ePrivacy Directive it stated:

> "*Most browsers use default settings that do not allow the users to be informed about any tentative storage or access to their terminal equipment. Therefore, default browser settings*

[104] Art 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), 6 June 2014, http://ec.europa.eu/justice/data-protection/article-29/documentation/otherdocument/files/2014/20140606_wp29_ts_standardisation_letter_to_w3c.pdf accessed 25 September 2016.

[105] Hustinx Peter, 'Do not Track or Right on Track? – The Privacy Implications of Online Behavioural Advertising' Public Lecture, University of Edinburgh, School of Law Edinburgh, (7 July 2011) <https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Speeches/2011/11-07-07_Speech_Edinburgh_EN.pdf> accessed 20 September 2016. At the same speech, the former EDPS criticised the expressed support by the Commission 'for a US driven 'do-not-track' initiative' seemed at the time 'to fall short of the e-Privacy Directive requirements' (mostly referring to opt-in/ opt-out compatibility with the article 5(3) of the ePrivacy Directive).

> *should be "privacy friendly" but cannot be a means to collect free, specific and informed consent of the users, as required in Article 2 (h) of the Data Protection Directive."*[106]

One of the arguments relates to the time of provision of a valid consent. Prior consent of the tracking activity would mean that the user is provided with the necessary information, before the processing of the data. Nevertheless, often in reality such an intermediary stage of no activity until the user indicates his or her wish is not possible. As soon as the user's device interacts with a website there is transmission of information.

- Sixth challenge: enforceability of DNT

A general concern relating to the DNT initiative, but also to every self-regulatory attempt, is the lack of regulatory oversight and the lack of enforceability, a concern also expressed by the WP29 in its letter on the TPE. Even if a tracking entity claims to respect the DNT signal of the user, the reliability of the statement and its actual implementation should be verified by data protection authorities. Such an inspection would probably fall out of the competence of the EU supervisory authorities, unless the DNT mechanism would be handled as a means to comply with the legislation. In any case, the risk for the user of illusion of privacy may be as dangerous for the individual as the actual violation of privacy. Transparency and reliability are crucial for the DNT mechanism.

5. Conclusions – DNT as a tool to empower the Internet user?

Tracking for online behavioural advertising purposes is widely employed, persistent and most often covert. The online and offline lives of users as shared on the Internet is recorded, compiled in profiles and used for profit. The result, as experienced by the user, is seemingly harmless: an interesting ad or a tempting commercial offer. The real impact however to the privacy and protection of persona data of the individual is fundamentally more severe: price and service discrimination, information filter bubble, surveillance and

[106] Art 29 Data Protection Working Party, Opinion 1/2009 on the proposals amending Directive 2002/58/EC on privacy and electronic communications (e-Privacy Directive), WP159, 10 February 2009, para 7.

misuse of personal data. At judicial level, judges are confronted with the question of the legitimacy of tracking and profiling and their impact on the protection of the rights of the individuals. As stated in landmark decision of the UK Court of Appeal, tracking may cause anxiety and distress to the individuals. While some Internet users might not be concerned with the issue, others will be— once informed about tracking activity—or already are concerned. Tracking technologies are constantly evolving; the same goes for data mining techniques and other methods to identify correlations of the collected data.

In Europe, the ePrivacy Directive regulates the storing and access to information already stored in the terminal equipment of the user that is relevant for profiling, while the GDPR includes specific provisions on profiling. The explicit right to object to profiling when it is based on the legitimate interests pursued by the controller or is necessary for the performance of a task carried out in the public interest, is a limited, but still positive change. In addition, the GDPR includes provisions on direct marketing and the right not to be subject to decisions based on profiling. Both legal instruments include provisions allowing the user preference to be expressed with technical means, that is browser settings and technical specifications (Recital 66 of Citizens Rights Directive and Article 21(5) of GDPR).

The DNT initiative was launched in response to persistent tracking. The aim was to empower the user with an informed choice. The diversity of implementation of DNT harmed rather than upheld the initiative. As a result, companies started publicly declaring they are not honouring the DNT signal, thus the user preference. The W3C standardization activity started as a promising solution, but temporarily seemed to lose its momentum. Substantial disagreements held back the progress of the work. However, in 2014 and 2015 interest in the W3C standard was revived, when two draft standards were published for public consultation. Implementing the DNT initiative in Europe would require adaptation of the initiative to the legislation of the Union. Despite being laconic in its letters to W3C, the WP29 touched upon crucial issues for the compatibility of the DNT standards with the EU legal framework. Adaptations in the W3C standards are substantial to that end and certainly not a path without obstacles; terminology, scope, default settings, consent, first/third party tracking are but a few.

Notwithstanding the implementation issues and the challenges, one should acknowledge the potential contribution of a DNT mechanism in empowering the user to gain control over tracking. DNT offers users two important elements: information and a choice to allow or not tracking activity. Along with legislation, which is and should be the main instrument to protect user rights, DNT, if properly supported by laws demanding

transparency and punishing fraudulent statements, may have an additional value towards achieving that goal.

Funding

Part of the research for this article was made possible by a VENI personal research grant from NWO, the Netherlands Organisation for Scientific Research.