Do Not Track for Europe

Zuiderveen Borgesius, F.J.; McDonald, A.M.

Publication date
2015
Document Version
Submitted manuscript
Published in
TPRC43: The 43rd Research Conference on Communications, Information and Internet Policy paper

Do Not Track for Europe

Drs. Frederik J. Zuiderveen Borgesius† & Aleecia M. McDonald†

Table of Contents

† Frederik J. Zuiderveen Borgesius, researcher, IViR Institute for Information Law, University of Amsterdam.

‡ Aleecia M. McDonald, non-resident Fellow, Stanford University's Center for Internet and Society. Aleecia is a former co-chair of the W3C standards process for Do Not Track, volunteers for the Electronic Frontier Foundation, and consults for Disconnect.

1 Introduction

The regulation of online tracking through cookies or other means is the subject of heated debates. In European legal circles, the debate often focuses on the e-Privacy Directive, which requires companies to obtain the user's consent for the use of tracking cookies and similar tracking technologies. A common complaint about the e-Privacy Directive's rule in practice is that clicking "I agree" to hundreds of separate cookie consent requests is not user-friendly. Meanwhile, there has been discussion about a Do Not Track (DNT) standard, which should enable people to express their wishes regarding tracking with a simple button in the browser.

This paper outlines the requirements that are needed for a Do Not Track system, or a similar system, to be able to help website publishers and other companies to comply universally with European privacy law. The main points of this paper are as follows. First, a Do Not Track system for Europe is possible, and the work of the World Wide Web Consortium (W3C) on the Do Not Track standard was originally designed to support European compliance. Second, a European Do Not Track standard could emerge from W3C, or from elsewhere. Third, implementers do not need to wait for a standard, and indeed, there are current DNT implementations that are almost compliant with European law.

We welcome readers' feedback on the content of this paper, particularly thoughts about the requirements for a European Do Not Track standard which could become the basis for a common standard approach.

The paper is structured as follows. Section 2 introduces the practice of online tracking. Section 3 turns to privacy and data protection rules in Europe, starting with the fundamental right to privacy and data protection. This section also discusses the EU consent requirement for tracking cookies, and for the processing of personal data in the context of behavioural targeting. Section 4 discusses the W3C Do Not Track standard efforts, focusing on default settings, global considerations, and on the territorial scope of

various data privacy laws. Section 5 gives examples of some current implementations of Do Not Track, and shows that some implementations could almost be used to comply with EU law today. We also contrast multiple approaches including the Electronic Frontier Foundation's version of Do Not Track, and the industry self-regulation approach from the Digital Advertising Alliance and Interactive Advertising Bureau. Section 6 summarises the main requirements for a Do Not Track standard that could help companies comply with European law. Section 7 concludes.

2 Online Tracking

Much of the tracking on the Internet is driven by behavioural targeting for advertising. While users imagine visiting a website, singular, in practice most web pages are comprised of multiple pieces that come from a variety of companies. In a simplified example, behavioural targeting involves three parties: an Internet user visiting a website, a website publisher hosting the website the user visits, and an advertising network embedded as part of that website. Advertising networks are companies that serve ads on thousands of websites, and can recognise people when they browse the web on any site where they serve an ad. This gives advertising networks a breadth and depth of information about millions of people. An ad network might infer that somebody who often visits websites about off terrain vehicles is in the market for buying such a car. If that person visits a news website, the ad network might display advertising for off terrain vehicles. When simultaneously visiting that same website, somebody else who visits many websites about gardening might see ads for gardening tools. The specific ads shown on a website are tailored to the people seeing them, which occurs as the result of ad auctions that take place in fractions of a second, with the highest bidder showing their ad to their targeted user.[1]

A commonly used technology for behavioural targeting involves cookies. A cookie is a small text file that a website publisher stores on a user's computer to recognise that

[1] See on real time bidding and auctions: Castelluccia C, Olejnik L and Minh-Dung T, 'Selling Off Privacy at Auction' (2013) Inria.

device during subsequent visits. Many websites use cookies, for example to remember the contents of a virtual shopping cart (first party cookies). Ad networks can place and read cookies as well (third party cookies). Third party tracking cookies are placed through nearly every popular website. As a result, an ad network can follow an Internet user across all websites on which it serves ads. Ad networks enter into partnerships to place and read cookies on sites even when they did not win the ad auction, further extending their visibility. A visit to one website often leads to a user receiving third party cookies from dozens of ad networks.[2] In addition to cookies, companies use other tracking technologies for behavioural targeting, such as various kinds of super cookies, device fingerprinting and deep packet inspection. Therefore, deleting or blocking cookies is not always enough to prevent being tracked.[3]

Advertising funds an astonishing amount of Internet services. Without paying with money, people enjoy access to online translation tools, online newspapers, and email accounts, and can watch videos and listen to music. Internet users are comfortable with the idea of an ad-supported Internet, in part because it mirrors offline business models like ads in newspapers. However, they are often unaware of and uncomfortable with the idea of invisible tracking to support online ads. Instead, they expect ads that do not track them, like billboards.[4]

Surveys show that most people do not want behaviourally targeted advertising, because they find it creepy or privacy-invasive. A small minority indicates it does not mind the data collection and prefers behaviourally targeted advertising because it can lead to more relevant ads.[5] Because some users value behaviourally targeted advertising while others

---

[2] Hoofnagle, CJ and Good N. 'The web privacy census' (October 2012) <http://law.berkeley.edu/privacycensus.htm> accessed 30 June 2015.
[3] See generally on various tracking technologies: Hoofnagle CJ et al, 'Behavioral Advertising: The Offer You Cannot Refuse' (2012) 6(2) Harvard Law & Policy Review 273, 291; Kuehn A and Mueller M. 'Profiling the profilers: deep packet inspection and behavioral advertising in Europe and the United States' (1 September 2012) <http://ssrn.com/abstract=2014181> accessed on 1 August 2015.
[4] McDonald, A. M., and Cranor, L. F. Americans' Attitudes About Internet Behavioral Advertising Practices. Proceedings of the 9th Workshop on Privacy in the Electronic Society (WPES) October 4, 2010.
[5] See: Turow J et al, 'Americans Reject Tailored Advertising and Three Activities that Enable it' (29 September 2009) <http://ssrn.com/abstract=1478214> accessed 30 June 2015. In Europe, seven out of ten people are concerned that companies might use data for new purposes such as targeted advertising without

find it invasive, most policy approaches favour finding ways to let users choose their own level of tracking and personalization.

In both the European Union and the United States, policy approaches hinge on the idea of user consent or choice. The status quo today involves a breath-taking degree of surveillance by for-profit companies without most users' knowledge. Clearly users do not consent or choose these outcomes since they are unaware of them. Moreover, when users have taken self-help measures like deleting HTTP cookies to protect their privacy, ad companies responded by subverting user choice by using new tracking technologies, in what has been termed an arms race of measures and countermeasures.[6] Some companies are frustrated by users blocking their tracking technologies and "stealing" content by viewing it without "paying" in data.[7] Some users are frustrated that even with extraordinary attention to privacy technologies, they still have data collected without their consent.

3 European Privacy Rules

This section acts as a primer for readers who are unfamiliar with European privacy rights and laws.[8] Our goal for this paper is to examine how one might design a Do Not Track standard that applies across all European nations, reducing the cost of compliance for companies. As a result, we focus on the most privacy-protective decisions. For example, while the United Kingdom might argue for implicit consent, Netherlands laws are based on explicit consent. We do not explore these differences in depth.

---

informing them (European Commission, 'Special Eurobarometer 359: Attitudes on data protection and electronic identity in the European Union' (2011) <http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf> accessed 18 November 2012, p 146.

[6] See Hoofnagle CJ et al, 'Behavioral Advertising: The Offer You Cannot Refuse' (2012) 6(2) Harvard Law & Policy Review 273

[7] Rob Rasko. 'Ad Blocking: A Binary Solution To A Complex Problem.' (29 July 2015) <http://marketingland.com/ad-blocking-binary-solution-complex-problem-136424> accessed on 3 August 2015: "Blocking ads is akin to stealing music or movies, argues columnist Rob Rasko."

[8] The section builds on, and includes parts of, earlier work of one of the authors (See F.J. Zuiderveen Borgesius, Improving Privacy Protection in the Area of Behavioural Targeting, in particular chapter 4, 6 and 10).

3.1 Privacy as a Human Right

The right to respect for private life, or the right to privacy for short, is a fundamental right in the European legal system and is included in the European Convention on Human Rights (1950). The European Court of Human Rights interprets the Convention's privacy right generously, and refuses to pin itself down on one privacy definition. This way, the Court can apply the right to privacy in unforeseen situations and to new developments. For instance, the Court says information derived from monitoring somebody's Internet usage is protected under the right to privacy.[9]

To protect privacy in the context of online tracking and behavioural targeting, the main legal instrument in Europe is the Data Protection Directive,[10] coupled with the e-Privacy Directive's consent requirement for tracking technologies.[11] Data protection law is a legal tool that aims to ensure that the processing of personal data happens fairly and transparently. Data protection law grants rights to people whose data are being processed (data subjects), and imposes obligations on parties that process personal data (data controllers, limited to and referred to as companies in this paper).[12] Since its inception in the early 1970s, data protection law has evolved into a complicated field of law.

The Charter of Fundamental Rights of the European Union lists the fundamental rights and freedoms recognised by the European Union. The Charter copies the right to private life almost verbatim from the European Convention on Human Rights.[13]

The Charter contains a separate right to the protection of personal data. "Such data must be processed fairly for specified purposes and on the basis of the consent of the person

---

[9] ECtHR, Copland v. United Kingdom, No. 62617/00, 3 April 2007, par. 41-42.
[10] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31.
[11] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L 201/37, as amended by Directive 2006/24/EC [the Data Retention Directive], and Directive 2009/136/EC [the Citizen's Rights Directive].
[12] See: Art 2(a) and 2(d) of the Data Protection Directive.
[13] The Court of Justice of the European Union says the right to privacy in the Charter and the Convention must be interpreted identically (CJEU, C-400/10, J. McB. v L. E., 5 October 2010, par. 53).

concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified."[14]

The Charter adds that these rules must be subject to control by independent Data Protection Authorities. Data Protection Authorities interpret national privacy laws and serve a similar enforcement function as the United States Federal Trade Commission (FTC). In addition to each national Data Protection Authority, the Article 29 Working Party is an international group primarily comprised of one Data Protection Authority from each of 28 nations. Although not legally binding, the Working Party's opinions are influential. Article 29 Working Party opinions reflect a strong consensus across European privacy regulators. National Data Protection Authorities often follow the Working Party's interpretation.[15]

3.2 Informed Consent for Cookies and Similar Tracking Technologies

Since 2009, article 5(3) of the e-Privacy Directive requires any party that stores or accesses information on a user's device to obtain the user's informed consent. Article 5(3) applies to many tracking technologies, such as tracking cookies. There are exceptions to the consent requirement, for example for cookies that are necessary for transmitting communication or a service requested by the user. Hence, no prior consent is needed for cookies that are used for log-in procedures or a digital shopping cart. Article 5(3) applies regardless of whether personal data are processed. Article 5(3) applies to storing or accessing any information on people's devices. The provision is technology

[14] Article 8(2) of the Charter of Fundamental Rights of the European Union.
[15] See S Gutwirth and Y Poullet, 'The contribution of the Article 29 Working Party to the construction of a harmonised European data protection system: an illustration of "reflexive governance"?' in VP Asinari and P Palazzi (eds), *Défis du Droit à la Protection de la Vie Privée. Challenges of Privacy and Data Protection Law* (Bruxelles, Bruylant, 2008).

neutral, and also applies, for instance, if an app provider reads the address book from somebody's phone.[16] For ease of reading this paper also speaks of consent for cookies.

Many marketers suggest that people who do not affirmatively block tracking cookies in their browser give implied consent to behavioural targeting. For instance, the Interactive Advertising Bureau U.K., a trade organisation, says "default web browser settings can amount to 'consent'."[17] But this does not seem plausible. As the Article 29 Working Party notes, the mere fact that somebody leaves her browser's default settings untouched does not mean she expresses her consent to be tracked.[18]

Article 5(3) is not widely enforced yet, among other reasons because the national implementation laws are rather new. Many member states missed the 2011 implementation deadline. The approaches in the member states vary. For example, the Netherlands requires, in short, opt-in consent for tracking cookies.[19] In contrast, the United Kingdom appears to allow companies to use opt-out systems to obtain "implied" consent.[20] However, the Working Party insists that the data subject's inactivity does not signify consent.[21]

3.3 Legal Basis for Personal Data Processing

Since 2009, article 5(3) of the e-Privacy Directive requires any party that stores or accesses information on a user's device to obtain the user's informed consent. Article

---

[16] The Working Party confirms that the provision applies, for instance, to apps that access information on a user's smartphone, such as location data or a user's contact list (Article 29 Working Party 2013, WP 202 – 'Opinion 02/2013 on apps on smart devices' (WP 202) 27 February 2013, p. 10).
[17] Interactive Advertising Bureau United Kingdom 2012, p. 2. The confusion is about consent and browser settings is partly caused by recital 66 of the 2009 directive that amended the e-Privacy Directive: "in accordance with the relevant provisions of [the Data Protection Directive], the user's consent to processing may be expressed by using the appropriate settings of a browser or other application."
[18] See e.g. Article 29 Working Party, 'Opinion 15/2011 on the definition of consent' (WP 187) 13 July 2011, p. 32; p. 35.
[19] See Zuiderveen Borgesius F.J., "Behavioral Targeting. Legal Developments in Europe and the Netherlands" (position paper for W3C Workshop: Do Not Track and Beyond), 2012, www.w3.org/2012/dnt-ws/position-papers/24.pdf
[20] See Information Commissioner's Office, "Changes to cookies on our website", 31 January 2013, available at: www.ico.org.uk/news/current_topics/changes-to-cookies-on-our-website.
[21] See Article 29 Working Party, "Working Document 02/2013 providing guidance on obtaining consent for cookies" (WP 208) 2 October 2013.

5(3) applies to many tracking technologies, such as tracking cookies. There are exceptions to the consent requirement, for example for cookies that are necessary for transmitting communication or a service requested by the user. Hence, no prior consent is needed for cookies that are used for log-in procedures or a digital shopping cart. Article 5(3) applies regardless of whether personal data are processed. Article 5(3) applies to storing or accessing any information on people's devices. The provision is technology neutral, and also applies, for instance, if an app provider reads the address book from somebody's phone.[22] For ease of reading this paper also speaks of consent for cookies.

Many marketers suggest that people who do not affirmatively block tracking cookies in their browser give implied consent to behavioural targeting. For instance, the Interactive Advertising Bureau U.K., a trade organisation, says "default web browser settings can amount to 'consent'."[23] But this does not seem plausible. As the Article 29 Working Party notes, the mere fact that somebody leaves her browser's default settings untouched does not mean she expresses her consent to be tracked.[24]

Article 5(3) is not widely enforced yet, among other reasons because the national implementation laws are rather new. Many member states missed the 2011 implementation deadline. The approaches in the member states vary. For example, the Netherlands requires, in short, opt-in consent for tracking cookies.[25] In contrast, the United Kingdom appears to allow companies to use opt-out systems to obtain "implied"

---

[22] The Working Party confirms that the provision applies, for instance, to apps that access information on a user's smartphone, such as location data or a user's contact list (Article 29 Working Party 2013, WP 202 – 'Opinion 02/2013 on apps on smart devices' (WP 202) 27 February 2013, p. 10).
[23] Interactive Advertising Bureau United Kingdom 2012, p. 2. The confusion is about consent and browser settings is partly caused by recital 66 of the 2009 directive that amended the e-Privacy Directive: "in accordance with the relevant provisions of [the Data Protection Directive], the user's consent to processing may be expressed by using the appropriate settings of a browser or other application."
[24] See e.g. Article 29 Working Party, 'Opinion 15/2011 on the definition of consent' (WP 187) 13 July 2011, p. 32; p. 35.
[25] See Zuiderveen Borgesius F.J., "Behavioral Targeting. Legal Developments in Europe and the Netherlands" (position paper for W3C Workshop: Do Not Track and Beyond), 2012, www.w3.org/2012/dnt-ws/position-papers/24.pdf

consent.[26] However, the Working Party insists that the data subject's inactivity does not signify consent.[27]

3.3.1 Contract Provision as a Legal Basis

A company can process personal data if the processing is necessary for the performance of a contract with the data subject.[28] For instance, certain data must be processed for a newspaper subscription. The "necessary" requirement sets a higher threshold than useful or profitable. According to the Article 29 Working Party, a company can only rely on the legal basis necessity for contract performance if the processing is genuinely necessary for providing the service.[29] Advertising is not, in and of itself, considered necessary to perform a contract with the data subject. The Working Party's view implies that, in general, companies cannot rely on this legal basis for behavioural targeting.

3.3.2 Balancing Provision as a Legal Basis

The balancing provision allows data processing when it is necessary for the company's legitimate interests, except where such interests are overridden by the data subject's interests or fundamental rights.[30] When weighing the interests of the company and the data subject, all circumstances have to be taken into account, such as the sensitivity of the data and the data subject's reasonable expectations. For example, data processing to prevent fraud might be considered acceptable under the balancing provision, depending on the specific details. If a company relies on the balancing provision for data processing for direct marketing, data protection law grants the data subject the right to stop the

---

[26] See Information Commissioner's Office, "Changes to cookies on our website", 31 January 2013, available at: www.ico.org.uk/news/current_topics/changes-to-cookies-on-our-website.
[27] See Article 29 Working Party, "Working Document 02/2013 providing guidance on obtaining consent for cookies" (WP 208) 2 October 2013.
[28] Article 7(b) of the Data Protection Directive.
[29] Article 29 Working Party, 'Opinion 06/2014 on the notion of legitimate interests of the data controller under article 7 of Directive 95/46/EC'(WP 217) 9 April 2014, p. 17. See also Article 29 Working Party, 'Opinion 03/2013 on purpose limitation' (WP 203), 2 April 2013, p. 46.
[30] Article 7(f) of the Data Protection Directive.

processing: to opt out.[31] The Data Protection Directive does not say explicitly whether behavioural targeting can be based on the balancing provision. But the most convincing view is that behavioural targeting cannot be based on this provision, in particular when it involves tracking somebody over multiple websites. In most cases the data subject's interests must prevail over the company's interests, as behavioural targeting involves collecting and processing information about personal matters such as people's browsing behaviour. Indeed, the Working Party says companies can almost never rely on the balancing provision to process personal data for behavioural targeting.[32]

3.3.3 Unambiguous Consent as a Legal Basis

If a company cannot base personal data processing on the balancing provision or another legal basis, only the data subject's consent can provide a legal basis for processing.[33] The Working Party says consent is generally the required legal basis for personal data processing for behavioural targeting. It follows from the Data Protection Directive's consent definition that consent requires a free, specific, informed indication of wishes.[34] People can express their will in any form, but mere silence or inactivity is not an expression of will.[35]

In sum, companies are required to obtain consent in advance for most tracking technologies that are used for the data collection, and for personal data processing that powers behavioural targeting. In virtually all circumstances, EU law only allows tracking after the individual's prior consent.

---

[31] Article 14 of the Data Protection Directive.
[32] In 2013 the Working Party said that the data subject's unambiguous consent is the only appropriate legal basis for behavioural targeting (Article 29 Working Party, 'Opinion 03/2013 on purpose limitation' (WP 203), 2 April 2013, p. 46).
[33] Article 7(a) of the Data Protection Directive: the data subject's unambiguous consent can provide a legal basis for personal data processing.
[34] Article 2(h) of the Data Protection Directive.
[35] C Kuner, *European Data Protection Law: Corporate Regulation and Compliance* (Oxford University Press 2007), p. 68; Article 29 Working Party, 'Opinion 15/2011 on the definition of consent' (WP 187) 13 July 2011, p. 11.

In practice, however, consent for data processing has been cumbersome to obtain. In particular, HTTP cookies automatically save to a user's device as soon as she visits the website, yet consent is needed *before* storing information (such as a cookie) on a user's device. The Article 29 Working Party notes this problem as one of the reasons they find industry programs to set opt-out cookies insufficient.[36] Fortunately, as we will discuss further below, the technical mechanisms of Do Not Track do allow proactive consent.

4 Do Not Track

In this section we introduce a potential mechanism for users to indicate their consent to tracking prior to even visiting a website, or to decline consent to tracking.

4.1 Short History of Do Not Track

Do Not Track (DNT) allows users to request online privacy. The idea evolved from the "Do Not Call" list in the United States, where people list their phone number in a registry to stop receiving telemarketing calls.[37] Starting in early 2011, users of the Mozilla Firefox browser users could send a "do not track" signal (via an HTTP header of "DNT:1" in technical parlance) to signify that the user enabled Do Not Track.[38] In short order, all major browsers offered a way for users to express a Do Not Track preference.[39] It was

[36] "It follows from the literal wording of Article 5.(3) that: i) consent must be obtained before the cookie is placed and/or information stored in the user's terminal equipment is collected." (Article 29 Working Party 2010, 'Opinion 2/2010 on online behavioural advertising' (WP), 22 June 2010, p. 13. See also Article 29 Working Party 2013, 'Working Document 02/2013 providing guidance on obtaining consent for cookies' (WP 208) 2 October 2013: "As a general rule, consent has to be given before the processing starts" (p. 3, emphasis original); Article 29 Working Party 2011, 'Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising' (WP 188) 8 December 2011, p. 5.

[37] For additional background on Do Not Track, see Christopher Soghoian, "The History of the Do Not Track Header," Slight Paranoia blog, January 21, 2011.

[38] Sean Michael Kerner, "Mozilla Details Firefox 4's Do Not Track," InternetNews (March 10, 2011).

[39] Geoff Duncan, "Google Chrome with adopt Do Not Track," Digital Trends (February 24, 2012).

estimated that by 2014, "Do Not Track is already set in about 20% of browser requests to European websites."[40]

In 2011, the World Wide Web Consortium (W3C) convened the Tracking Protection Working Group (we refer to this as the "DNT Group" in this paper.)[41] The DNT Group has been engaged in a discussion about a Do Not Track standard ever since.[42] The W3C is an international organisation where member organisations cooperate to develop technical web standards.[43] As of 2015, the DNT Group mainly consists of representatives from companies, with some of the participants having quit in frustration.[44] A handful of non-governmental organisations and academics continue to participate in the discussion, as does a representative of the Article 29 Working Party in his capacity as a scholar. The DNT Group could thus be seen as a multi-stakeholder negotiation.[45] W3C standards are not legally binding; the success of a W3C standard is measured by its rate of adoption.[46]

Do Not Track is not a technical mechanism that fundamentally changes how web browsers work. Instead, Do Not Track enables people to send a request into the world, with the hope someone will listen and do something. Do Not Track can be compared to hotel doorknob signs requesting privacy. A sign on a doorknob does not in any way hinder hotel staff from entering the room, but our social conventions hold that travelers can expect more privacy than if they did not hang the doorknob sign. This idea is central

---

[40] Baycloud Systems. 'E-Privacy, Data Protection Law, and the Do Not Track signal' (17 February 2014) <http://cloudclinic.com/cloudclinic-news/privacy-and-data-protection-law-and-the-do-not-track-signal> accessed on 11 May 2015.

[41] On of the authors on this paper (McDonald) was one of the original co-chairs of the W3C Tracking Protection Working Group. We are quite aware of the proper name, but feared TPWG is an impenetrable acronym for most readers. Throughout this paper, where formal citations regarding Do Not Track are light, we rely upon direct experience.

[42] W3C Tracking Protection Working Group (website). <http://www.w3.org/2011/tracking-protection/>

[43] W3C prefers to refer to their output as "recommendations" rather than "standards." We use the word standards to improve readability.

[44] As one public example, see Jonathan Mayer, "Resignation from the Tracking Protection Working Group," July 30, 2013. Available from <https://lists.w3.org/Archives/Public/public-tracking/2013Jul/0601.html>.

[45] See: Doty N and Mulligan DK, 'The Technology of Privacy: Internet Multistakeholder processes and techno-policy standards. Initial reflections on privacy at the World Wide Web Consortium.' (2013) 11 Journal on Telecommunications & High Technology Law 135.

[46] See: Doty N and Mulligan DK, 'The Technology of Privacy: Internet Multistakeholder processes and techno-policy standards. Initial reflections on privacy at the World Wide Web Consortium.' (2013) 11 Journal on Telecommunications & High Technology Law 135.

to Do Not Track. Do Not Track is a user's request for privacy – nothing more but also nothing less. The question then becomes: what additional privacy should users be able to expect when they send a Do Not Track request?

4.2 A Do Not Track Signal: What Should Companies Do?

As of 2015, there is a nearly completed W3C recommendation to standardize the technical communications protocols.[47] This document primarily specifies how users indicate they would prefer not to be tracked, and how companies can signal if they honour or ignore the request. There is also a nearly completed consensus publication from W3C as to what companies ought to do when receiving a user's Do Not Track request.[48] Both of these documents are in Last Call status, meaning this is the final chance for public comments prior to formal publication.

Getting these documents to a consensus draft involved a great deal of negotiation. At times, some DNT Group members thought there might only be agreement on the technical aspects. There is an optional way for companies to point to their own (or someone else's) document that explains what the company means when they send back a signal that they honour DNT.[49] This creates the possibility of many different DNT approaches other than the approach from W3C, potentially including a Do Not Track system designed specifically for Europe. Moreover, the DNT Group itself agreed that a European standard would be helpful, as discussed below.

4.3 Global Considerations for Do Not Track

Concerns about creating a standard that could both fulfill European regulations yet still be voluntary adopted by US companies surfaced during the very first in person meeting

---

[47] Roy T. Fielding and David Singer (editors.) Tracking Preference Expression (DNT;) W3C Last Call Working Draft (24 April 2014.) The most current published consensus document is available from http://www.w3.org/TR/tracking-dnt/

[48] Nick Doty (editor.) Tracking Compliance and Scope; W3C Last Call Working Draft (14 July 2015.) The most current published consensus document is available from http://www.w3.org/TR/tracking-compliance/

[49] See section 6.5.3 Compliance Property, in Tracking Preference Expression (DNT) (24 April 2014.) http://www.w3.org/TR/2014/WD-tracking-dnt-20140424/

of the DNT Group. Some participants were interested in a standard that would facilitate European compliance. Many participants could not abide by a Do Not Track standard that required no tracking by default, in which users must consent (that is, opt in to tracking.) Doing so would be detrimental to some, though not all, online business models. Yet in order to fulfill European regulations, tracking must not happen prior to user consent. To complicate matters further, it takes time before users upgrade to new browsers that offer Do Not Track options, meaning at least initially most websites would not receive any Do Not Track singles from users who had not yet upgraded to newer web browsers. The group consensus was one that allowed all requirements to be fulfilled:

- For United States users, the absence of a Do Not Track signal means users have not made a choice for privacy, and it is acceptable to continue to track them.
- For European users, the absence of a Do Not Track signal means they have not consented to tracking, and it is not acceptable to track them.

The language to capture this agreement could be clearer, but the W3C text reads: "In the absence of regulatory, legal, or other requirements, servers may interpret the lack of an expressed tracking preference as they find most appropriate for the given user, particularly when considered in light of the user's privacy expectations and cultural circumstances."[50]

In short, United States users opt out of tracking, and European users opt in to tracking. This allows companies to comply with European laws where they must, yet continue current business practices in other nations.

The decision detailed above was necessary, but not sufficient, to meet European regulatory requirements. Members of the DNT Group understood this and expected that European Do Not Track implementations would need to be more privacy protective than implementations in the United States. The DNT Group focused on creating a minimum floor for companies to comply with, while allowing companies to do more for privacy if

---

[50] See section 5.1, Expression Format, in Tracking Preference Expression (DNT) (24 April 2014.) http://www.w3.org/TR/2014/WD-tracking-dnt-20140424/

they so choose. A committee formed within the DNT Group with the goal of publishing a Global Considerations document.[51] The document was not designed as a formal part of the W3C standard, but rather a set of guidelines for companies with European visitors who look to reduce their legal liability. There were several committee meetings with good progress, but the document was never published. Due to personnel changes within W3C it seems unlikely to be a major focus in the future, and unwise to await publication.

However, it is already well understood that European compliance will need to be some level of "DNT plus" in order to meet European regulations. What that "plus" entails could be defined nation-by-nation, but that would present a bit of an implementation nightmare for most companies. Or, the "plus" could stem from the intersection of the most privacy-protective national laws in order to have one implementation that works across all EU member countries. Either approach could work. Of the two, we note that having as few variants as possible of DNT would reduce user confusion as to what, exactly, it means when a company honours a Do Not Track request, and would also reduce implementation complexity for companies. We believe a single European standard that will comply across multiple countries is the most practical approach. Such a standard does not need to come from the W3C Do Not Track group.

4.4 Do Not Track and Territorial Scope of National Laws

The DNT Group discussions about Global Considerations followed the approach that a country's law is relevant for website visitors who live in that country. For example, if a German Facebook visitor requests not to be tracked, it does not matter that Facebook is based in the United States or that Facebook has their European headquarters in Ireland. Germany's privacy laws protect German citizens online, everywhere.

Within the United States, laws with similar territorial scope exist. For example, California's AB 370 requires websites to document how they respond to Do Not Track

---

[51] See the Tracking Protection Working Group Global Considerations Task Force, <http://www.w3.org/2011/tracking-protection/130311-gloco.html>

requests. This law protects people in California, regardless of where the webserver is located or the location of the company that owns the webserver.[52] Companies have a choice between trying to determine where each user is located and showing Do Not Track information just to Californians, or the far easier path of adding a paragraph to their privacy policy and informing all visitors about their DNT practices. As a result, CA AB 370 has become a de facto national law in the United States requiring Do Not Track disclosure in privacy policies, including mobile apps.[53]

The national laws implementing the e-Privacy Directive and the Data Protection Directive often apply to companies that are based outside the EU. For instance, several EU countries have applied national data protection laws to Google.[54] As a rule of thumb: European regulators will probably not complain if an Internet company complies with the national law of the country where an EU Internet user is based.

In reality, the territorial scope of EU privacy and data protection rules is more complicated. The two main rules in the Data Protection Directive regarding territoriality can be summarised as follows.[55] First, European data protection law applies when processing is carried out in the context of the activities of an establishment of a company on EU territory.[56] Several of the largest companies that use behavioural targeting are formally established in Europe, such as Facebook and Apple (Ireland). Furthermore, in the *Google Spain* case, the European Court of Justice said, in short, that European data

---

[52] Assembly Bill No. 370, An act to amend Section 22575 of the Business and Professions Code, relating to consumers (September, 2013.) https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140AB370

[53] Paul G. Martino and Dominique R. Shelton, California adopts do-not-track disclosure law: A.B. 370 amends the California Online Privacy Protection Act (CalOPPA) to require new privacy policy disclosures for websites, online services and mobile apps about behavioral tracking, Lexology (September 20, 2013) http://www.lexology.com/library/detail.aspx?g=4a16a991-0df9-48de-92b3-dfda2271dba9

[54] See: Article 29 Working Party, Letter to Google (signed by 27 national Data Protection Authorities), 16 October 2012 <www.cnil.fr/fileadmin/documents/en/20121016-letter_google-article_29-FINAL.pdf> Appendix: <www.cnil.fr/fileadmin/documents/en/GOOGLE_PRIVACY_POLICY-_RECOMMENDATIONS-FINAL-EN.pdf> accessed 1 August 2015.

[55] Article 4 of the Data Protection Directive. The Directive as such doesn't apply to companies outside the EU; rather the national provisions based on the Directive apply.

[56] Article 4(a) of the Data Protection Directive.

protection law applies when a search engine operator has a subsidiary in a member state, and that subsidiary sells and promotes advertising space offered by the search engine.[57]

Second, EU data protection law applies when the company is not established in the EU, but uses equipment situated on EU territory for personal data processing.[58] Many non-European behavioural targeting companies use equipment, such as data centres, in Europe. Such companies must comply with EU data protection law. Furthermore, the Working Party says that European data protection law applies to any company that uses tracking technologies on a device in Europe, because in such cases the company makes use of equipment (the user's device) in Europe.[59]

The territorial scope of the e-Privacy Directive is also complicated, but potentially very wide.[60] In the Netherlands for instance, the regulator suggests that the e-Privacy Directive's cookie consent requirement applies to anyone who stores a cookie on a device in the Netherlands.[61] In sum, in many situations, EU data protection and privacy rules apply to non-European companies.

4.5 Example issue: first and third parties

While we do not detail all differences between the current W3C documents and what might be required for a version that comports with European law, we offer one example to illustrate the sorts of issues involved.

---

[57] CJEU, C-31/12, Google Spain, 13 May 2014, dictum, 2).
[58] Article 4 of the Data Protection Directive.
[59] Article 29 Working Party, 'Opinion 1/2008 on data protection issues related to search engines (WP 148), 4 April 2008', p. 9-12.
[60] See 'ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation', Final Report (a study prepared for the European Commission DG Communications Networks, Content & Technology by Time.Lex and Spark legal network and consultancy ltd, 10 June 2015) http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=9962 (accessed 13 July 2015), p. 29-33.
[61] "The key principle here is that this norm's objective is to protect users in the Netherlands. The information obligation and the consent requirement thus apply to both Dutch and non-Dutch websites that (exclusively or partially) target Dutch users." Netherlands Authority for Consumers & Markets, Frequently asked questions about the Dutch cookie act (version June 2014), p. 3.

From the start, proposals for a Do Not Track standard have few requirements for tracking within one website.[62] There was agreement within the DNT Group that tracking within one website should not be greatly affected by Do Not Track signals.[63] This would imply that companies such as Amazon or Facebook are allowed to analyse people's behaviour within their own website, regardless of whether people signal Do Not Track. In contrast, the e-Privacy Directive's consent rule also applies to first party tracking cookies.[64] Therefore, a European Do Not Track standard designed to help companies to comply with the e-Privacy Directive would need additional requirements on first parties. Companies can, of course, choose to implement a more privacy protective version of Do Not Track on their own, without a European Do Not Track standard. This would leave each company to work through these issues on their own, which seems inefficient.

5 Current Implementations

Given the issues described above, an obvious question is whether Do Not Track can work as an expression of consent in Europe. We believe so. It is possible to implement Do Not Track in a way that abides by European regulations, and some companies appear to very nearly do so already today. In addition to companies' compliance, we also discuss consent considerations with regard to how web browsers[65] work as part of the larger Internet ecosystem.

---

[62] Schunter, Matthias and Peter & Swire. 'Explanatory Memorandum for Working Group Decision on "What Base Text to Use for the Do Not Track Compliance Specification"' (16 July 2013) <http://www.w3.org/2011/tracking-protection/2013-july-explanatory-memo/> accessed on 16 February 2015, p. 12. Some complain that Do Not Track helps larger companies such as Google and Facebook and hurts ad networks that do not offer consumer services (see Chapell, A. 'Do Not Track: Great For Internet Giants Like Google And Facebook' (29 May 2014) <www.adexchanger.com/data-driven-thinking/track-great-internet-giants-like-google-facebook/> accessed 29 May 2015).

[63] In *Tracking Compliance and Scope*, Section 3.2 First Party Compliance is all of five paragraphs, where Section 3.3 Third Party Compliance is several pages.

[64] See on article 5(3) of the e-Privacy Directive: section 3.2 of this paper.

[65] For ease of reading, we focus on web browsers. Do Not Track is not only set with web browsers. For example, anti-virus maker AVG changes Windows registry settings to enable Do Not Track which is then sent by web browsers and the Fennec operating system sets and sends Do Not Track on mobile phones. Do Not Track can work in any HTTP (or SPDY) environment, including Internet of Things devices, console games, and televisions. But these details get unwieldy to pull into discussion, and by far the most common use case is browser-based.

5.1 AP News

AP News was the first organisation to honour Do Not Track.[66] Prior to Do Not Track, AP News set cookies with unique identifiers for each user viewing an AP story anywhere on the web. This allowed AP to collect statistics on the popularity of stories, story placement, and clusters of readers' interests.

When AP News first implemented Do Not Track, they stopped storing new data tied to unique identifiers on their servers, but continued other forms of aggregated data collection for their Do Not Track users. This led to user confusion. A blogger noticed that even when he enabled Do Not Track he still had AP News cookies on his computer, and questioned the validity of the AP News implementation. In response, AP News changed their Do Not Track implementation to delete all AP News cookies for Do Not Track users.

AP News' practices, including their Do Not Track implementation, are not currently in line with European regulations. As discussed in section 3, EU law requires companies to obtain user consent before they track users.[67]

We believe AP News would need to make technically simple changes to comply with European regulations. As described in Appendix A on page 35, AP News would stop tracking all European visitors who do not signal an affirmative consent to tracking (in technical terms, send an HTTP header of DNT:0). This would turn AP News from a company that tracks Europeans by default to a company that only tracks Europeans with their consent. We believe this approach would go above and beyond what is required by European law. Therefore, using Do Not Track as a European consent mechanism is technically possible.

---

[66] Scott Gilbertson, "In Big Endorsement, AP Embraces Mozilla's 'Do Not Track' Header," *Wired*, (March 31, 2011).

[67] Article 29 Working Party 2013, 'Working Document 02/2013 providing guidance on obtaining consent for cookies' (WP 208) 2 October 2013: "As a general rule, consent has to be given before the processing starts" (p. 3, emphasis original).

5.2 Advertising Industry Opt Out

A number of behavioural targeting companies cooperating in the Interactive Advertising Bureau (IAB) and the European Advertising Standards Alliance (EASA) offer people the chance to opt out of targeted advertising on a centralised website: youronlinechoices.com.

However, participating companies merely promise to stop showing targeted ads, so they may (or may not) continue to track people who have opted out. The company may offer the equivalent of "do not target" rather than "do not collect." That is, the company continues to collect and use data, but does not show ads that are targeted based on the data. Companies may, and often do, continue to track people who have opted out.[68] The website's FAQ explains: "[d]eclining behavioral advertising only means that you will not receive more display advertising customised in this way."[69] But it seems plausible that people expect the website to offer an opt out that strongly reduces data collection.[70]

To add to the confusion, not all participating companies follow the bare minimum requirement of "do not target." Some actually do stop collection, particularly if their only business model is to show targeted ads. These companies have opt-out programs that go beyond what EU regulations require for people who do not consent. This suggests the opt-out program could, on an individual company basis, be used to establish consent and lack of consent to comply with European law. Sadly, no: the companies could not use the DAA opt-out system to obtain valid consent. Valid consent requires an expression of will, which generally calls for an opt-in procedure, rather than the current opt-out.

---

[68] Article 29 Working Party, Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising (WP 188), Brussels 8 December 2011.

[69] Interactive Advertising Bureau Europe -– Youronlinechoices (about). 'Your Online Choices. A guide to online behavioural advertising. About' <http://www.youronlinechoices.com/uk/about-behavioural-advertising> accessed on 17 February 2015..

[70] In the United States there is a similar website, networkadvertising.org/choices/. Research suggests that many people expect it to offer "Do not track" rather than "Do not target" (McDonald, AM and JM Peha. 'Track Gap: Policy Implications of User Expectations for the 'Do Not Track' Internet Privacy Feature (TPRC 39: The 39th Research Conference on Communication, Information, and Internet Policy) (2011) <http://ssrn.com/abstract=1993133> accessed on 10 May 2015; Hoofnagle, C. J., Jennifer M. Urban and S. Li. 'Most US Internet Users Want 'Do Not Track' to Stop Collection of Data about their Online Activities' (October 8, 2012) <http://ssrn.com/abstract=2152135> accessed on 10 May 2015.

Additionally, the website works with opt-out cookies. Hence, if somebody clears her cookies – a measure that is often suggested to limit tracking – the opt-outs are lost. Furthermore, in 2011 the Working Party noted that the youronlinechoices website included code that enables user tracking, while users were not informed about this.[71]

For the IAB opt-out program to be useful for European compliance it would need to become a system where users opt in to tracking, rather than opt out. It would need a uniform higher standard than "do not target" though it is not always necessary to stop all data collection. Even with these politically implausible changes, the IAB opt out system has the challenge of being cookie based. Since websites automatically set cookies as soon as the page is loaded, and because consent must occur before the first non-necessary personally identifiable data is stored, websites would need to have either only cookies without unique identifiers, or a more involved technical design.

5.3 The Electric Frontier Foundation's DNT

The Electronic Frontier Foundation (EFF) is a US-based NGO focused on online rights. The EFF is working on their own version of Do Not Track. EFF originally published a preliminary short document[72] with the relevant content of what companies must promise:

> This domain interprets DNT as a request for an opt out of collection and retention of visitors' reading habits, which we will respect, subject to reasonable exceptions that respect user privacy.

Very recently, the EFF published a several page document that details their standard for Do Not Track.[73] It is based primarily on limiting unique identifiers, with a few exceptions like technical debugging and security with a ten day retention period. The EFF's Do Not

---

[71] Article 29 Working Party, Opinion 16/ 2011 on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising (, WP 188), Brussels 8 December 2011, p.7.
[72] See https://www.eff.org/files/dnt-policy-preliminary.txt
[73] Electronic Frontier Foundation, "Do Not Track Compliance Policy Version 1.0," available from <https://www.eff.org/dnt-policy> (August, 2015.)

Track standard is designed to work with the W3C Do Not Track work, and provides a path for users to give consent for tracking using W3C Do Not Track mechanisms.[74]

This definition of Do Not Track would not comport with EU laws because it requires all users to opt out of tracking, rather than to consent to tracking. That said, EFF designed their Do Not Track specifically for use by web browser plugins, including their own, which is named Privacy Badger.[75] As described below, while EFF's Do Not Track might not be sufficient for compliance in a standard browser, it may well work as part of a European compliance solution in conjunction with web browser plugins.

5.4 Web browser Preferences

The Working Party has asked browser vendors since 1999 not to allow third party cookies by default.[76] At the time of writing most browser vendors allow third party cookies by default. This might partly be explained by the fact that the some browser vendors are connected to companies that do behavioural targeting. The browser users are not paying customers.[77]

In theory, web browsers could be used to express consent for data processing.[78] In practice, browsers setting cookies by default cannot point to a user allowing cookies and

---

[74] IBID, see 1.c in the "Exceptions" section.
[75] Most web browsers allow third parties to write code to extend the functionality of the browser. These are called different things, including plugins, addons, and extensions. While it does not take much technical sophistication to install plugins to a web browser, it takes a certain technical bent to even be aware that such a thing is possible.
[76] Article 29 Working Party 1999, 'Recommendation 1/99 on invisible and automatic processing of personal data on the Internet performed by software and hardware' (WP 17), 23 February 1999. "Cookies should, by default, not be sent or stored" (p. 3).
[77] See Kristol 2001, Kristol DM, 'HTTP Cookies: Standards, Privacy, and Politics' (2001) 1(2) ACM Transactions on Internet Technology (TOIT) 151, p. 169-170; Soghoian C, 'End the charade: Regulators must protect users' privacy by default' (December 2010) <www.priv.gc.ca/information/research-recherche/2010/soghoian_201012_e.asp> accessed 11 May 2015; Soghoian C, 'Why Private Browsing Modes Do Not Deliver Real Privacy' (Position paper for Internet Architecture Board, workshop on Internet Privacy, jointly organized with the W3C, ISOC, and MIT CSAIL, was hosted by MIT on 8-9 December 2010) <www.iab.org/wp-content/IAB-uploads/2011/03/christopher_soghoian.pdf> accessed 11 May 2015; Wingfield N, 'Microsoft quashed effort to boost online privacy' (Wall Street Journal) (2 August 2010) <http://online.wsj.com/article/SB10001424052748703467304575383530439838568.html> accessed 11 May 2015.
[78] Recital (66) of the Citizens' Rights Directive 2009/136.

say she has affirmatively consented; she may have even known there was a choice to make.

Apple's Safari browser takes an unusual approach to third party cookie defaults. Safari was designed based on the original technical specification for cookies, which did not allow third party cookies by default at that time.[79] It is not quite the case that Safari blocks third party cookies by default. Cookies are blocked from websites the user has not visited, which describes most, but not all, third party cookies. For example, if Alice visits a website (e.g. Facebook) and then encounters it in a third party setting (e.g. a Facebook Like button while on a different website,) cookies would set for Alice even though they are third party cookies. Safari comes closest of the major browsers, but Safari still does not work for an expression of consent:

> [O]nly browsers or other applications which by default reject 3d party cookies and which require the user to engage in an affirmative action to accept both the setting of and continued transmission of information contained in cookies by specific web sites are able to deliver valid and effective consent.[80]

Furthermore, Safari does not block or require consent for first-party cookies.

5.5 PrivacyBadger, Disconnect, Ad Block, and other Browser Plugins

Browser plugins extend the functionality of web browsers. The Electric Frontier Foundation offers a browser plugin, Privacy Badger.[81] Privacy Badger blocks some tracking by default, and will allow domains to unblock themselves by promising to

---

[79] D. Kristol and L. Montulli, "HTTP State Management Mechanism," (February 1997). https://tools.ietf.org/html/rfc2109

[80] See 'ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation', Final Report (a study prepared for the European Commission DG Communications Networks, Content & Technology by Time.Lex and Spark legal network and consultancy ltd, 10 June 2015) http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=9962 (accessed 13 July 2015), p. 12.

[81] Electric Frontier Foundation, "Privacy Badger," <https://www.eff.org/privacybadger>

honour EFF's version of Do Not Track. That means tracking only happens with a user's consent. Consequently, while EFF's Do Not Track is insufficient for European compliance, when used as designed with Privacy Badger it may be.[82] Similarly, Disconnect also blocks trackers but allows them if they adhere to EFF DNT, both as a browser plugin and as a standalone app on mobile devices.[83] AdBlock (though not AdBlock Plus) has also adopted EFF's Do Not Track for their browser plugin.[84] It appears that Disconnect and Privacy Badger currently offer the best chance for European users to have their legal rights upheld.

5.6 Article 29 Working Party Feedback on W3C Do Not Track

In their analysis of a draft of the initial Do Not Track document developed by W3C, the Article 29 Working Party highlighted six areas of particular concern.[85] The Do Not Track Group has published a subsequent document, but it does not address all of the Article 29 Working Party concerns. Presumably the Article 29 Working Party will update their analysis in light of recent developments, but here is a quick summary, combined with our absolutely subjective guess as to the likelihood that substantive changes will be adopted.

5.6.1 Terminology

Area of concern: a clear statement that W3C standards do not override EU law and policy. **Changes needed:** Adopt the Article 29 Working Party suggested text verbatim, perhaps in Section 7 of the *Tracking Compliance and Scope* document. It currently covers legal compliance in Section 7, reading in full, "Notwithstanding anything in this

---

[82] We are indebted to Rob van Eijk for this interesting and non-obvious perspective. Mr. van Eijk was, of course, considering this in his personal capacity and we have no knowledge of how the Article 29 Working Party would eventually evaluate Privacy Badger with the just published EFF DNT.
[83] Casey Oppenheim, "Coalition Announces 'New Do Not Track' Standard," Disconnect Blog, (August 3, 2015.) <https://blog.disconnect.me/press-release-coalition-announces-new-do-not-track-standard/>
[84] Wendy Davis, Ad-Blocking Companies And EFF Unveil New 'Do Not Track' Standards, Media Post, (August 3, 2015.)
[85] Isabelle Falque Pierrotin, 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) (June 6, 2004.) Available from <http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140606_wp29_ts_standardisation_letter_to_w3c.pdf>

recommendation, a party may collect, use, and share data required to comply with applicable laws, regulations, and judicial processes." This text was not evaluated by the Working Party. **Likelihood:** Plausible. What is in the newly published text could also be deemed close enough.

5.6.2 Automatic expiration of preferences

Area of concern: Over time, users must be reminded they can withdraw their consent. **Changes needed:** Currently, consent is expected to last indefinitely. An entirely new mechanism to record the date of consent and remind users of their ability to withdraw consent would have to be designed. **Likelihood:** Low. This is not an issue the Do Not Track Group is currently considering.[86] Furthermore, it is not the sort of thing companies are likely to think about implementing on their own.

5.6.3 Respecting a user tracking preference

Area of concern: (a) the purpose of consent must be clear, and consent limited to only what the user has actually agreed to, (b) when DNT is unset it does not mean the user consented, (c) consent should be managed by user agents. **Changes needed:** (a) The documents could provide examples of how to word requests for consent, or even requirements, (b) this is the case for European citizens today though, as noted in section 4.3 on page 17, it could be better worded to be made clearer, (c) most of the time consent is managed by user agents (mostly web browsers) already. **Likelihood:** (a) Low, but individual companies could comply when requesting consent, (b) High, (c) High.

5.6.4 Anonymisation

Area of concern: the definition of de-identified data does not align with how the term is used in European regulations. **Changes needed:** section 2.9 in the *Tracking Compliance and Scope* would need to mirror definitions in European regulations. **Likelihood:** Low.

---

[86] The list of issues is available from <http://www.w3.org/2011/tracking-protection/track/issues>

However, there is non-binding text that advises Do Not Track implementers to avoid some of the problems the Working Party likely envisioned.

5.6.5 Potential consent (P), disregarding (D)

Area of concern: companies may not know if a user has consented or not right away, and are able to report back to the user that there is "potential" consent, leaving the user unsure if they are being tracked or not. Companies may also send a signal that they are simply disregarding Do Not Track requests. **Changes needed:** eliminate these two status values as possible responses. **Likelihood:** Low. However, a non-binding note points out that the specification is designed for "disregarding" to be used in case of technical error, not in the normal course of operations.

5.6.6 Users with special needs

Area of concern: there must be no discrimination against users with visual disabilities, or users with devices that have limited or no user interface. **Changes needed:** the Working Group suggested specific language to add. **Likelihood:** Low.

6 Requirements for a European Consent Mechanism

The prior section took a detailed look at a particular point in time in the W3C process. Here we step back to a more general level, and contrast multiple possible approaches.

To enable websites to comply with European law, a consent mechanism should comply at least with the following four conditions, as set forth by the Article 29 Working Party.

First, companies must not collect data for behavioural targeting about Europeans that do not express a preference.[87] Silence is not consent after all. [88]

---

[87] The territorial scope is more complicated than the sentence above suggests; see section 4.4.
[88] See section 3.3 and 3.6.

Second, if somebody visits a website and signals Do Not Track, the website and its partners should not follow that person's activities. No tracking should generally mean no data collection of personally identifiable information, which includes unique identifiers.[89] Some minor exceptions may be allowed for this rule. For instance, in some cases website publishers may store the IP address of certain visitors for a short period, for security reasons for example.[90] This could fit under the balancing provision of data processing.[91] Note that first parties are not exempt.

Third, consent must occur before uniquely identifiable cookies are set, not just before data is collected or processed.

Fourth, users must have a way to revoke their consent at a later time. This could be as simple as reversing their Do Not Track preference in a web browser.

6.1 A Comparison of Potential Consent Mechanisms

Below, we summarize current approaches to consent and how they interact with these four requirements.

---

[89] See Kohnstamm J. 'Online tracking: to collect or not to collect, that's the question...' (October 2012) <www.cbpweb.nl/downloads_artikelen/art_2012_kohnstamm_online_tracking.pdf> accessed 31 July 2015.
[90] See on that topic: Soghoian, C. 'Security and Fraud Exceptions Under Do Not Track (Position Paper for W3C Workshop on Web Tracking and User Privacy 28/29 April 2011, Princeton, NJ, USA)' <www.w3.org/2011/track-privacy/papers/Soghoian.pdf> accessed on 28 May 2014.
[91] See section 3.5.

Requirement	DAA Opt Out	W3C DNT	EFF DNT alone	EFF DNT with Privacy Badger, Disconnect, AdBlock
1. Consent by opt in	No	Yes (varies by country)	No	Yes
2. Limits collection of PII	Maybe (varies by company)	Maybe (varies by company)	Yes	Yes
3. Consent sent before cookies set	No	Yes	Yes	Yes
4. Can revoke consent	Yes (inverted: revoke opt out)	Yes	Yes	Yes
Meets all four	X	?	X	✓

It is difficult to imagine any system that requires Europeans to affirmatively opt in for privacy could be seen as sufficient. Both the DAA Opt Out program (designed by the advertising industry) and the EFF Do Not Track standard (designed by privacy advocates) treat a user's silence as consent to tracking, and therefore neither approach seems likely to satisfy a European legal framework.

The W3C Do Not Track approach sets a minimum bar that falls below what is required for European compliance, but individual companies could provide additional privacy protections and meet European laws while also adhering to the W3C approach.

Privacy Badger, Disconnect, and AdBlock extend the functionality of web browsers and are built on top of the EFF Do Not Track standard. Crucially, they block trackers (including tracking by means other than cookies) unless (a) the trackers abide by EFF's Do Not Track standard, which includes provisions to limit data collection for unique identifiers in ways that appear to accord with European privacy law, or (b) users affirmatively consent to tracking. This leads us to an interesting possibility that if a company implements EFF's Do Not Track standard, and a user visits with any un-customized browser, that visit may not comply with European law. Yet if the same user visits with Privacy Badger or Disconnect, that visit may accord with European law.

7 Conclusion

Let us conclude. First, a Do Not Track system for Europe is possible, and the work of the World Wide Web Consortium (W3C) on the Do Not Track standard was originally designed to support European compliance. Second, a European Do Not Track standard could emerge from W3C, or from elsewhere. Third, implementers do not need to wait for a standard, and indeed, there are current DNT implementations that are likely very close to compliant with European law, as shown in Appendix A.

Interest in Do Not Track has been reaffirmed by California's AB 370, requiring Do Not Track transparency, along with publications this summer from the W3C and the Electronic Frontier Foundation setting out technical standards for Do Not Track. The Electronic Frontier Foundation version is more privacy preserving, and layers on top of work done by the W3C to work with their framework. One of the challenges for any consent system is that it requires coordination from multiple parties. Every major browser has a way to set a Do Not Track signal, as well as to signal consent to tracking. This empowers users to have a voice in expressing their preferences, and also provides companies with information about their website visitors. This differs from ad blocking where companies often do not know they have been blocked.

Individual companies are able to engineer their own European-compliant implementation of Do Not Track. There is no technical barrier to meeting even the most privacy-preserving national laws. That said, web browsers do not enforce Do Not Track policy, let alone to a level that would comply with European laws. Indeed, not one of the companies with a major browser – Apple, Google, Microsoft, Mozilla, Opera – implements Do Not Track on their own websites; they ignore the signals that come from their own browsers. Browser add ons or plugins, including Privacy Badger, Disconnect, and AdBlock, block tracking without consent for Do Not Track users. This approach inverts the model to one of requiring consent first, rather than putting the burden on users to know how to opt out, and may well provide a user experience that accords with European privacy law.

California's law for Do Not Track transparency has, in practice, primarily been used to document non-compliance with users' requests not to be tracked. As shown in Appendix B, most popular companies do not mention Do Not Track in their privacy policies at all. Of those that do, nearly all acknowledge they ignore users' request for privacy, and continue to collect and process personally identifiable information even when users attempt to opt out through Do Not Track. United States companies are not granting European citizens the same privacy rights they are entitled to at home, which seems at odds with the spirit of Safe Harbor.

Finally, while we believe all of the pieces are in place to enable individual companies to meet their regulatory responsibilities in Europe with Do Not Track, asking each company to devise their own European variant on Do Not Track is inefficient. We end with a call for a standard for a European variant of Do Not Track.

8 Acknowledgements

The authors thank Peter Eckersley, Casey Oppenheim, Lee Tien, Alan Toner, and Rob van Eijk for thoughtful discussions regarding the subject of this paper. All mistakes and opinions are, of course, our own.

* * *

Appendix A

In this Appendix, we present the basic logic for how AP News could modify their Do Not Track implementation to comply with European privacy laws. Note that not only are we aiming to fulfill the most stringent of European privacy laws, we also looked for the easiest path to implementation. The initial AP News Do Not Track implementation took one engineer an hour to code. We expect these modifications would take even less time.

Currently, AP News has two different code branches. For users sending a Do Not Track signal requesting not to be tracked, they delete all AP News cookies and do not log the contents of any AP News cookies. For all other users, they either read and log AP News cookies that contain a unique identifier, or create and set a new unique identifier if there is no cookie yet. They then perform various processing of that data.

Here is the rough logic of how AP News could modify their system to align with European privacy law:

```
IF user is in the EU
   THEN
      IF DNT:0    /* there is consent to track */
         THEN read, set, and process unique identifiers as today
         ELSE treat as DNT:1 is today; delete cookies

   ELSE           /* applies only to non-EU users */
      proceed exactly as today
```

This logic inverts from an opt-out system of data processing to an opt-in system for European users, but not for users who reside elsewhere. It would, of course, be simpler to treat all visitors with the same privacy protections EU law affords, but that seems unlikely in practice for financial reasons.

As written above, European users who have not consented to tracking are not tracked, but we can imagine several optional alternative approaches. Users could be asked to allow

tracking with an explanation of the AP News data collection and use policies; users could be asked to pay money to avoid being tracked; or users could be turned away from the website that hosts AP News stories. All three options are likely to be acceptable under the W3C vision of Do Not Track. However, the final option of blocking access to a website for users who do not consent to tracking could run into questions from European regulators of whether consent is "freely given" under such conditions.

Imagine that as an optional refinement, AP News prompts users to opt in to unique tracking, and explains their privacy choices. Not everyone will consent. It is poor practice to badger users into consenting by asking them to opt in again, again, and again. A better design might be to set a cookie with non-unique data, including the date the user elected not to opt in, to avoid unnecessary pestering. Users who block cookies could be guided on how to make an exception for this particular cookie, if they prefer doing so to continual bombardment.

As a final note, the logic we present here only deals with AP News cookies. AP News might also need to investigate any other forms of unique identifiers they collect. In particular, most web servers store a log line with the IP address by default. AP News could change their web server configuration to omit logging information about users not sending consent (it takes two lines of code for Apache servers to omit log lines from DNT:0 users) or with a very little more work, to omit logging specifically the IP address field.

This example illustrates that it is technically easy to implement Do Not Track in a way that, so far as we know, would be likely comply with privacy laws in all European countries. It is an example of extremely limited data collection that goes further than required by the W3C Do Not Track documents, further than the Electronic Frontier Foundation's Do Not Track, and further than European law. For example, all three would permit some uniquely identifiable information to be collected and used for fraud prevention even with a user who sends a Do Not Track signal, depending on the implementation details.

Appendix B

In accordance with California law AB 370, any commercial company that collects personally identifiable information from a California citizen must disclose how they respond to a Do Not Track request as part of their privacy policy. We examined the privacy policies of the top 20 most popular US websites, as of July 2015.[92]

In summary, 13 of the top 20 websites simply ignore California law and omit any mention of Do Not Track. Twitter is particularly interesting, since they garnered a great deal of press attention when they implemented Do Not Track[93] yet omit mention of it in their privacy policy. Only one website, Pinterest, publically claims to support Do Not Track, but they do not describe how they do so (which appears at odds with California law). Pinterest's statement supporting Do Not Track attempted to load three third-party trackers, despite a browser sending a Do Not Track request. Of the remaining six websites that document their Do Not Track policy, all state they ignore incoming Do Not Track signals.

For Wikipedia, they reason that since they already protect user privacy above and beyond what the W3C standard would require from first parties for *all* of their users, they have nothing further to do for Do Not Track requests. It appears that Wikipedia does not set cookies or use similar files, or only cookies that are necessary to deliver the website. Hence, the e-Privacy Directive does not require Wikipedia to ask user consent.[94] Presumably Wikipedia stores IP addresses (which must often be seen as "personal data") of visitors under certain conditions. It seems plausible that such storage, for security reasons for instance, can be based on the balancing provision, and thus does not require user consent.[95]

---

[92] Alexa Top Sites, <http://www.alexa.com/topsites/countries/US>
[93] Dozens of news articles, including e.g. Don Reisinger, CNet, "Twitter announces support for Do Not Track," May 17, 2012. <http://www.cnet.com/news/twitter-announces-support-for-do-not-track/>
[94] As mentioned in section 3.2, article 5.3 of the e-Privacy Directive does not require consent for, in brief, necessary cookies.
[95] See section 3.5 about the balancing provision.

Reddit, Microsoft, and Disney suggest that they ignore Do Not Track because there is not yet a W3C consensus standard. We are curious to see how, if at all, their privacy policies will change after W3C publishes final specifications for Do Not Track. We also note that the absence of a detailed W3C standard did not deter other companies from developing their own Do Not Track implementations.

Reddit, Netflix, and Imgur reassure their readers that while they do nothing in response to a Do Not Track request, they also do not allow third parties to collect personally identifiable information from their websites. This appears to run into confusion as to what constitutes personally identifiable information. Under at least California and Netherlands law, any persistent unique identifier is personally identifiable information, including IP address. Under this definition, it is extraordinarily likely that third parties do, in fact, collect and process personally identifiable information. Imgur even describes the technical measures they take that obscure user's names while providing persistent unique identifiers to third parties, which means they do provide personally identifiable information to third parties.

Site	Do Not Track policy	Privacy policy
1. Google.com	None	https://www.google.com/intl/en/policies/privacy/
2. Facebook.com	None	https://www.facebook.com/privacy/explanation
3. Amazon.com	None	http://www.amazon.com/gp/help/customer/display.html/ref=footer_privacy?ie=UTF8&nodeId=468496
4. Youtube.com (a Google company)	None	https://www.google.com/intl/en/policies/privacy/
5. Yahoo.com	None	https://policies.yahoo.com/us/en/yahoo/privacy/index.htm
6. Wikipedia.org	Ignored (see below)	https://wikimediafoundation.org/wiki/Privacy_policy#Our_Response_to_Do_Not_Track_.28DNT.29_signals links to https://wikimediafoundation.org/wiki/Privacy_policy/FAQ#DNTFAQ
7. Ebay.com	None	http://pages.ebay.com/help/policies/privacy-policy.html
8. Twitter.com	None	https://twitter.com/privacy
9. Craigslist.org	None	https://www.craigslist.org/about/privacy.policy

10. Reddit.com	Ignored (see below)	https://www.reddit.com/help/privacypolicy
11. Netflix.com	None	https://www.netflix.com/PrivacyPolicy
12. Linkedin.com	Ignored (see below)	https://www.linkedin.com/legal/privacy-policy has an obvious link to https://www.linkedin.com/legal/do-not-track
13. Live.com (a Microsoft company)	None	http://www.microsoft.com/privacystatement/en-us/core/default.aspx
14. Bing.com (a Microsoft company)	Ignored (see below)	https://www.microsoft.com/privacystatement/en-us/bingandmsn/default.aspx
15. Imgur.com	Ignored (see below)	https://imgur.com/privacy
16. Pinterest.com	Supports Do Not Track	https://about.pinterest.com/en/privacy-policy links to https://help.pinterest.com/en/articles/we-support-do-not-track
17. Tumblr.com (a Yahoo! company)	None	https://www.tumblr.com/policy/en/privacy
18. Go.com (a Disney company)	Ignored (see below)	https://disneyprivacycenter.com/privacy-policy-translations/english/ links to https://disneyprivacycenter.com/twdc-privacy-controls/online-tracking-and-advertising/
19. Instagram.com	None	https://help.instagram.com/155833707900388
20. Chase.com	None	https://www.chase.com/resources/consumer-privacy links to https://www.chase.com/content/dam/chasecom/en/resources/documents/Online_Privacy_Policy.pdf

We provide relevant excerpts from privacy policies directly below, again in order of website popularity.

From the **wikipedia** privacy policy: *We are strongly committed to not sharing nonpublic information with third parties. In particular, we do not allow tracking by third-party websites you have not visited (including analytics services, advertising networks, and social platforms), nor do we share your information with any third parties for marketing purposes. Under this Policy, we may share your information only under particular situations, which you can learn more about in the "When May We Share Your Information" section of this Privacy Policy.*

Because we protect all users in this manner, we do not change our behavior in response to a web browser's "do not track" signal.

For more information regarding Do Not Track signals and how we handle them, please visit our FAQ.

Excerpt from the Wikipedia FAQ: *...we protect everyone, and do not change our behavior in response to a web browser's DNT signal. We believe that, as of this writing, this approach is as or more protective than the obligations for "first parties" set out in the World Wide Web Consortium's Do Not Track specification. However, the specification is still being revised and changed, often in important ways. We will continue to monitor the specification as it moves towards completion and update our behavior and this FAQ consistent with the principles laid out in the Privacy Policy.*

From the **reddit** privacy policy: *reddit's website does not currently respond to a Do Not Track ("DNT") or similar signal as it awaits the results of efforts by the policy and legal community to determine the meaning of DNT and the proper way to respond. reddit does not allow other parties to collect personally identifiable information from users on reddit.*

LinkedIn provides well-written user education and context around Do Not Track. For brevity, we excerpt just their own practices: *How does LinkedIn respond to the signal? LinkedIn takes privacy and security very seriously, and strive to put our members first in all aspects of our business. With regard to DNT, LinkedIn currently does not respond to DNT signals in browsers because it doesn't track individual members across the web with the exception of proactive sharing of articles on LinkedIn (see below).*

What about JavaScript buttons like "Share on LinkedIn"? When members visit websites that contain JavaScript buttons ("plugins"), like LinkedIn's Share button, we receive plugin impressions that we de-personalize in a short period of time. When members interact with our plugins (for example, sharing articles on LinkedIn) we keep this

information to improve their and others' LinkedIn experience. See our Privacy Policy for details.

Does LinkedIn permit third parties to collect personally identifiable information about an individual consumer's online activities over time and across different Web sites when a consumer uses LinkedIn's site?

As the world's largest professional network, our 100s of millions of members come to LinkedIn to connect with other members, to find jobs, to be found by other members for any number of professional reasons. LinkedIn is, inherently, a public place, and there is a lot of personally identifiable information on LinkedIn that is viewable by any visitor. In other words, third parties can find out about you from the info you share on our services - like LinkedIn and SlideShare.

In the DNT context, however, LinkedIn does not authorize the collection of PII from LinkedIn members through advertising technologies deployed in ads that may appear on LinkedIn without separate consent.

Microsoft's **Bing** describes their practices as: *Because there is not yet a common understanding of how to interpret the DNT signal, Microsoft does not currently respond to the browser DNT signals on its own websites or online services, or on third-party websites or online services where Microsoft provides advertisements, content or is otherwise able to collect information. We continue to work with the online industry to define a common understanding of how to treat DNT signals.*

Imgur: *We may use cookies, web beacons, or other anonymous tracking information to improve our server's interaction with your computer, and we may partner with third party advertisers who may (themselves or through their partners) place or recognize a unique cookie on your browser. These cookies enable more customized ads, content or services to be provided to you. To trigger these cookies, we may pass an encrypted or*

"hashed" (non-human readable) identifier corresponding to your email address to a Web advertising partner, who may place a cookie on your computer. No personally identifiable information is on, or is connected to, these cookies. Although our servers currently don't respond to "do-not-track" requests, you can block these cookies in other ways, for example by going to http://www.privacychoice.org/choose.

Pinterest: *We support Do Not Track because we think it's really important that you have a simple way to control how your info gets used. That's why in addition to giving you a number of ways to choose how Pinterest uses your data, we honor DNT as a signal for how you want us to use data we collect outside of Pinterest.*

Disney's **Go**: *Do Not Track is a standard that is currently under development. As it is not yet finalized, we adhere to the standards set out in this privacy policy.*

* * *