Richmond Journal of Law and Technology

Volume 18 | Issue 1 Article 3

2011

Do Not Track: Revising the EU's Data Protection Framework to Require Meaningful Consent for Behavioral Advertising

Matthew S. Kirsch

DO-NOT-TRACK: REVISING THE EU'S DATA PROTECTION FRAMEWORK TO REQUIRE MEANINGFUL CONSENT FOR BEHAVIORAL ADVERTISING

By Matthew S. Kirsch*

Cite as: Matthew S. Kirsch, *Do-Not-Track: Revising the EU's Data Protection Framework to Require Meaningful Consent for Behavioral Advertising*, XVIII RICH. J.L. TECH. 2, http://jolt.richmond.edu/v18i1/article2.pdf

I. INTRODUCTION

[1] The advertisements you see while browsing the Internet are rarely accidental. For instance, Alliance Data, one of many new companies in the booming data-marketing industry, can instantaneously recognize that a user visiting their client's website is Joel Stein, a thirty-nine year-old, college educated male, who makes over $125,000 a year.[1] Alliance Data also knows that Joel is likely to make purchases online, but only spends about $25 dollars a purchase.[2] Using this information, and the specifics of

*Matthew Kirsch, J.D. Candidate, 2012, The George Washington University Law School; Member, The George Washington International Law Review; BBA, Emory University, 2009, Cum Laude.

[1] *See* Joel Stein, *Data Mining: How Companies Now Know Everything About You*, TIME MAGAZINE BUSINESS (Mar. 10, 2011), http://www.time.com/time/business/article/0,8599,2058114,00.html.

[2] *See id.*

over 100 of Joel's past online purchases, Alliance Data creates advertisements specifically tailored to Joel and displays them as he continues to browse the Internet.[3]

[2] Unlike the majority of Internet users, Joel Stein, as a reporter, discovered the extent to which new data mining companies tracked him online.[4] During his investigation, Joel found various data marketing companies that held detailed profiles about him, compiled from his online behavior.[5] With varying degrees of accuracy, these profiles "knew" about Joel's mortgage, car, hobbies, travel desires and more.[6] Some of Joel's discoveries were comical, such as the BlueKai profile that "knew" Joel was a nineteen year-old woman; most likely based on a recent splurge for his wife at an online lingerie website.[7] Other revelations raised more serious concerns, such as when the CEO of Reputation.com found Joel's social security number in a matter of hours.[8] What these data mining companies know, or think they know, about Joel, highlights some of the concerns raised when corporations own, trade, and sell profiles filled with the intimate and private details of citizen's lives.

[3] This Article will argue that the upcoming revision of the European Union's ("EU") Data Protection Directive should require advertisers to utilize and respect a "Do-Not-Track" mechanism in order to provide consumers with a meaningful mechanism to consent, or refuse to consent, to the online collection of their data for use in behavioral advertising. In Part II, the Article will provide an overview of the EU's current data protection framework. This Part will also look at the status of consent

[3] *See id.*

[4] *See id.*

[5] *See id.*

[6] *See* Stein, *supra* note 1.

[7] *See id.*

[8] *See id.*

under the current framework. It will then explain the EU's motivations for the upcoming revision of the Data Protection Directive. Next, this Part will explore the emergence of the behavioral advertising industry, followed by a discussion of some concerns this growth raises. It will then examine Privacy by Design and Privacy Enhancing Technologies, broad categories of technologies designed to enhance electronic privacy. Finally, this Part will consider the sufficiency of industry self-regulation. Part III will argue for the implementation of a "Do-Not-Track" mechanism to provide citizens in the EU with a meaningful way to express informed consent to the online collection of their personal information for the purposes of behavioral advertising.

II. BACKGROUND

A. Data Protection in the European Union

[4] In the 1970's, the growing use of computers to process personal information led to the first calls for comprehensive data protection legislation.[9] As a result, in 1995, the European Commission ("EC" or "the Commission") adopted Directive 95/46 (the "Data Protection Directive" or "Directive"), which established a compressive framework for the processing of personal data.[10] The Data Protection Directive derives its legal authority from Article 95 of the European Community Treaty, which allows for the creation of legislation designed to harmonize the internal market within the EU.[11]

[9] *See* PETER CAREY, DATA PROTECTION: A PRACTICAL GUIDE TO UK AND EU LAW 1 (3d ed. 2009).

[10] *See* Council Directive 95/46, 1995 O.J. (L 281) 31 (EU) [hereinafter Data Protection Directive]; CAREY, *supra* note 9, at 5.

[11] *See* Treaty Establishing the European Community art. 95, Dec. 29, 2006, 2006 O.J. (C 321E) 37 (consolidated version); Alfonso Scirocco, *The Lisbon Treaty and the Protection of Personal Data in the European Union*, DATAPROTECTIONREVIEW.EU (Aug. 8, 2008), http://www.madrid.org/cs/Satellite?c=CMRevistaFP&cid=1142425661164&esArticulo=true&idRevistaElegida=1142398920499&language=en&pag=1&pagename=RevistaDatos

[5] The Data Protection Directive has two principal aims.[12] The first is the preservation of the fundamental right to data protection, and the second is to facilitate the free flow of personal data between and within EU member states.[13] To accomplish its twin aims the Directive sets out a general framework for the processing of personal data.[14] Article 6 describes one of the central tenants of this framework, that "the processing of personal data must . . . be carried out with the consent of the data subject . . . ."[15] Further, certain categories of data, such as religious, racial or health information are considered sensitive, and the Directive prohibits processing this data without the explicit affirmative consent of the data subject.[16] The Directive also attempts to ensure the fair collection of data by requiring that data subjects receive notice of the "identity of the [data] controller[,] . . . the purposes of the processing . . . [and] any further information such as the recipients . . . [or whether the data subject has a] right of access to and the right to rectify the data concerning him … ."[17]

PersonalesIngles%2FPage%2FRDPI_home_RDP&siteName=RevistaDatosPersonalesIngles.

[12] *See* CAREY, *supra* note 9, at 6.

[13] *See Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: A Comprehensive Approach on Personal Data Protection in the European Union*, at 4, COM (2010) 609 final (Nov. 4, 2010), *available at* http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf [hereinafter *Call for Revision*]; *see also* CAREY, *supra* note 9, at 6.

[14] *See* CAREY, *supra* note 9, at 5-6.

[15] Data Protection Directive, *supra* note 10, Preamble, para. 30.

[16] *See id.* art. 8, paras. 1, 2(a). Certain narrow exceptions apply. *See id.* art. 8, para. 2(b)-(e).

[17] *Id.* art. 10.

[6] A landmark aspect of the Data Protection Directive is its formal recognition of the fundamental right to the protection of personal data, as set out in Article 8 of the EU Charter of Fundamental Rights.[18] Article 8 provides that:

> 1. Everyone has the right to the protection of personal data concerning him or her.
> 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person 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.[19]

However, the Directive's recognition of this right does not give Article 8 binding legal effect; for many years, the Charter of Fundamental Rights operated merely as a political commitment.[20] This changed in 2007 when the Treaty of Lisbon explicitly included the right to the protection of personal data in Article 16b, resulting in the constitutional recognition of Article 8 of the Charter of Fundamental Rights.[21] When the Treaty of

[18] *See* Charter of Fundamental Rights of the European Union art. 8, Dec. 18, 2000, 2000 O.J. (C 364) 1 [hereinafter EU Charter of Fundamental Rights]; Data Protection Directive, *supra* note 10, Preamble, paras. 2,7.

[19] EU Charter of Fundamental Rights, *supra* note 18, art. 8.

[20] *See* Press Release, Charter of Fundamental Rights: The Presidents of the Commission, European Parliament and Council Sign and Solemnly Proclaim the Charter in Strasbourg (Dec. 12, 2007), *available at* http://europa.eu/rapid/pressReleasesAction.do?reference=IP/07/1916&format=HTML&aged=0&language=EN&guiLanguage=en.

[21] *See* Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community, art. 16 B & Declaration 20, Dec. 13, 2007, 2007 O.J. (C 306) 1, 51, 257 [hereinafter Treaty of Lisbon]; *see also Call for Revision*, *supra* note 13, at 4; Press Release, Charter of Fundamental Rights, *supra* note 20.

Lisbon entered into force in 2009, the right to the protection of personal data finally had an independent, constitutional, and binding legal basis.[22]

B. Consent in the EU Data Protection Framework

[7] As will be discussed in more detail in Part II(C), the EU is in the process of revising the Data Protection Directive.[23] A major reason for the revision of the Directive is the non-uniform implementation by EU Member States of what constitutes informed and free consent, especially in the context of behavioral advertising.[24] This Part will begin by examining the meaning of consent within the data protection framework, with a focus on the new e-Privacy Directives. It will then examine the Article 29 Working Party's 2010 opinion on informed consent to behavioral advertising under the existing data protection framework.[25] Finally, it will attempt to derive the meaning of consent from relevant enforcement actions and case law.

i. Consent in the e-Privacy Directives

[8] In 2002, as a supplement to the Data Protection Directive, the EU adopted the e-Privacy Directive to address "the processing of personal data and the protection of privacy in the electronic communications sector."[26] In 2009, the e-Privacy Directive was amended to further

[22] *See Call for Revision*, *supra* note 13, at 4; Press Release, Charter of Fundamental Rights, *supra* note 20.

[23] *See infra* Part II.C.

[24] *See Call for Revision*, *supra* note 13, at 8-9. *See generally infra* Part II.D (discussing behavioral advertising in detail).

[25] *See infra* Part II.B.ii.

[26] *See* Council Directive 2002/58, 2002 O.J. (L 201) 37 (EU) [hereinafter e-Privacy Directive].

address the changing landscape of the Internet.[27] The e-Privacy Directive and its amending Directive do not change or amend the Data Protection Directive itself, rather the new directives provide an extra set of regulations specific to electronic communications.[28] Because the amended e-Privacy Directive addresses many of the same issues the revision of the Data Protection Directive intends to address, it is important that the two directives complement each other.[29]

[9] A major provision added by the amended e-Privacy Directive requires data controllers to inform data subjects when placing cookies or similar tracking devices on a user's terminal equipment.[30] Data subjects must have the right to object to the use of cookies and other tracking devices.[31] Unfortunately, despite its emphasis on cookies and consent, the amended e-Privacy Directive failed to clear up the confusion over implicit consent with respect to browser settings.[32] For example, a recent draft of Finland's implementing legislation for the amended e-Privacy Directive

[27] *See* Council Directive 2009/136, art. 4, 2009 O.J. (L 337) 11, 22 (EU) [hereinafter Amended e-Privacy Directive] (noting that the 2009 amendment of the e-Privacy Directive must be implemented by May 25, 2011).

[28] *See* CAREY, *supra* note 9, at 12.

[29] *See Call for Revision*, *supra* note 13, at 7.

[30] *See* Amended e-Privacy Directive, *supra* note 27, Preamble, para. 66. For purposes of this Article "terminal equipment" is a term meant to include a person's personal computer.

[31] *See id.*

[32] *See* Eija Warma & Vilja Kemppainen, *Implementation of E-Privacy Directive in Finland: Will User-Friendliness Override Privacy in the Use of Cookies in Internet Services?*, CASTREN & SNELLMAN (Feb. 18, 2011), http://castrensnellman.meteoriitti.com/Page/c1ccbac8-1bad-436e-bb79-e1ffaa00df14.aspx?groupId=cdeed881-8278-43d3-9994-ccf6a6a633e7&announcementId=b841f3d0-0d3a-4c72-b9b3-3f036b00332e ("Recital 66 of the Directive states that the user's consent may be received through browser settings. As default settings of major browsers generally allow cookies, this standpoint would make the Directive's impact on business quite minor.").

specifically allows for a user's browser settings to provide consent.[33] Contrast Finland's approach with the UK's, where Parliament is considering simply "copying and pasting" the language of the amended e-Privacy Directive into national law and letting the courts figure out any ambiguities regarding the meaning of consent.[34] Also, both France and the Netherlands have passed similar laws requiring prior opt-in consent for cookies.[35]

ii. The Article 29 Working Party's Opinion

[10] Despite the present ambiguities regarding consent in the data protection framework, a 2010 opinion issued by the Article 29 Working Party may still present a comprehensive definition of consent.[36] The newly amended e-Privacy Directive and the May 2011 deadline to implement the Directive into each Member State's national laws prompted

---

[33] *See id.*

[34] *See* Out-Law.com, *UK Passes Buck on Europe's Cookie Law with Copy-Paste Proposal: You Sort It out*, THE REG. UK (Sept. 17, 2010), http://www.theregister.co.uk/2010/09/17/eu_cookie_law/print.html.

[35] Hunton & Williams LLP, *France Introduces Prior Opt-in Consent for Cookies*, PRIVACY AND INFORMATION SECURITY LAW BLOG, http://www.huntonprivacyblog.com/2011/08/articles/european-union-1/france-introduces-prior-optin-consent-for-cookies/ (specifying that opt-in consent may be given "via user controlled settings on the relevant device"); Nicole Wolters Ruckert and David Korteweg, *New Dutch Cookie Law Requires Prior Consent from Internet Users*, INT'L ASS'N OF PRIVACY PROF'LS., https://www.privacy association.org/public ations/2011_06_28_new_du tch_cookie_law_requires_prior_consent_from_Internet_users (defining consent as "freely given, specific and well-informed").

[36] *See Opinion 2/2010 of the Article 29 Data Protection Working Party on 'Online Behavioural Advertising,'* WP 171 (June 22, 2010) 3, *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf [hereinafter *WP29 Opinion on Online Behavioural Advertising*]; CAREY, *supra* note 9, at 9 ("Article 29 of the Directive set up a Working Party . . . to act as an independent advisory body . . . . Thus when considering the meaning of . . . the Directive . . . regard should be had to any relevant opinion that has been issued by the Working Party.").

the issuance of the Working Party's *Opinion on Online Behavioural Advertising*.[37] While the Working Party's opinions do not hold the force of law, they are still considered important in interpreting the data protection framework.[38]

[11] The *Opinion* begins by noting that where the e-Privacy Directive addresses a specific subject matter, such as the use of cookies, its clauses should be read as controlling over a conflicting general clause in the original Data Protection Directive.[39] However, if a cookie collects information that also fits the definition of personal data under the Data Protection Directive, then that Directive will apply *in addition to* the e-Privacy Directive.[40] Consequently, the behavioral advertising industry will be subject to both the Data Protection Directive and the e-Privacy Directive because the majority of data collected by third-party cookies will fall within the Data Protection Directive's broad definition of personal data.[41]

---

[37] *See WP29 Opinion on Online Behavioural Advertising*, *supra* note 36, at 3, 7-8.

[38] *See* CAREY, *supra* note 9, at 9.

[39] *See WP29 Opinion on Online Behavioural Advertising*, *supra* note 36, at 10.

[40] *See id.* at 9. The Directive defines personal data as:

> any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity . . . .

Data Protection Directive, *supra* note 10, art. 2. More information on the subtleties and scope of personal data, as interpreted by the Article 29 Working Party may be found in *Opinion 4/2007 on the Concept of Personal Data*. *See generally Opinion 4/2007 of the Article 29 Data Protection Working Party on the 'Concept of Personal Data,'* WP 136 (June 20, 2007), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf.

[41] *See WP29 Opinion on Online Behavioural Advertising*, *supra* note 36, at 9 ("If as a result of placing and retrieving information through the cookie or similar device, the

[12] The *Opinion* also finds that Article 5(3) of the amended e-Privacy Directive generally restricts the use of cookies in behavioral advertising.[42] Article 5(3) provides in pertinent part:

> Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information, in accordance with Directive 95/46/EC, *inter alia* about the purposes of the processing . . . .[43]

However, an additional explanation in Recital 66 of the amending Directive tempers this seemingly strong language.[44] Recital 66 states:

> Third parties may wish to store information on the equipment of a user, or gain access to information already stored . . . . The methods of providing information and offering the right to refuse should be as user-friendly as possible. . . . Where it is technically possible and effective, in accordance with the relevant provisions of Directive 95/46/EC, the user's consent to processing may be

information collected can be considered personal data then, in addition to Article 5(3), Directive 95/46/EC will also apply."). Third party cookies will be discussed in more detail in Part II.D.

[42] *See id.* at 8.

[43] e-Privacy Directive, *supra* note 26, art. 5(3).

[44] A Recital is a part of an act or directive whose purpose "is to set out concise reasons for the chief provisions of the enacting terms, without reproducing or paraphrasing them." *Joint Practical Guide: Guide of the European Parliament, the Council and the Commission*, EUR-LEX, http://eur-lex.europa.eu/en/techleg/10.htm (last visited Aug. 21, 2011).

> expressed by using the appropriate settings of a browser or other application.[45]

Article 5(3) will often implicate behavioral advertisers, as it expressly applies to any party who places cookies or collects information from existing cookies stored on a data subject's computer.[46] Thus, most ad-networks, due to their use of cookies, must operate within the confines of the e-Privacy Directive.[47] Under the Working Party's interpretation of the current framework, advertising networks must obtain informed consent from a data subject.[48] The Working Party claims that consent under Article 5(3) requires an advertising network to: 1) give the user sufficient information about the data to be collected, as well as the purpose of the cookie, before asking a user for consent; 2) obtain consent before ever placing a cookie or collecting information from a user's computer; and 3) allow for a user to revoke their consent.[49]

[13] In response to varying interpretations among EU Member States, the Working Party addresses the question whether a user who fails to change default browser settings that allow cookies has given sufficient consent under the aforementioned test.[50] The *Opinion* states that although advertising networks and content providers often inform users about third-party cookies in their privacy policies, this practice, supported only by default browser settings, is unlikely to meet the requirements of informed

[45] Amended e-Privacy Directive, *supra* note 27, at 34.

[46] *See WP29 Opinion on Behavioural Advertising*, *supra* note 36, at 10.

[47] *See id.*

[48] *See id.*

[49] *See id.* at 13.

[50] *See id.*

consent under the data protection framework.[51] The Working Party gives three rationales for this conclusion.

[14] First, it concludes that under Article 2(h) of the Data Protection Directive, a browser cannot give valid consent for the collection and processing of a user's information by default.[52] The Working Party bases this finding on the average data subject's ignorance of the extent to which companies track online behavior for marketing purposes.[53] Further, if a company's privacy policy instructs a data subject to change his browser settings to avoid tracking, the average Internet user may not have the technological savvy to properly change the settings.[54] Second, even if browser settings could convey a user's informed consent, the Working Party argues against the ability to bypass a user's wishes through emerging technologies to track a user who has actively set his browser to block third-party cookies.[55] Third, browser settings cannot accurately discern user consent and may construe initial or partial acceptance of cookies as sufficient to allow the placement of all future cookies, whether by different companies or for purposes unrelated to that prior consent.[56]

[15] The Working Party also addressed the efficacy of an alternative consent mechanism, namely the opt-out programs offered by individual websites, ad-networks, and self-regulatory initiatives.[57] While the

[51] *See WP29 Opinion on Online Behavioural Advertising*, *supra* note 36, at 13.

[52] *See id.* at 14.

[53] *See id.*

[54] *See id.* (noting that only one of the four major browsers currently blocks third-party cookies by default upon installation).

[55] *See id.* Examples of emerging technologies would include flash cookies, tracking beacons, or deep packet inspection. *Id.*

[56] *See WP29 Opinion on Online Behavioural Advertising*, *supra* note 36, at 14.

[57] *See id.* at 15.

Opinion recognizes that these mechanisms attempt to complement or fix the problems created by securing consent through browser settings, it concludes they are insufficient.[58] This is primarily because the average user will not know where or how to access the opt-out.[59] Few users realize that, by not actively seeking the opportunity to opt-out, they are actually opting-in and offering their informed consent to be tracked.[60] Additionally, the failure to opt-out is a non-reaction that, by its nature, happens after data collection has already begun.[61] A failure to opt-out is not prior-informed consent as required by Article 5(3).[62]

[16] Finally, the Working Party expresses the view that prior opt-in mechanisms better deliver informed consent.[63] The *Opinion* suggests that a company should notify a user before receiving, storing, or sending a cookie, and the information should contain specific details about each cookie.[64] These details should include the identity of the advertising network, a disclaimer regarding what information will be collected, and a description of how the information will show the user targeted advertisements.[65] After a user receives this message, they should have the choice of whether or not to consent.[66] In order to address the practical problem of deciding to individually consent to an overwhelming number

[58] *See id.*

[59] *See id.*

[60] *See id.*

[61] *See WP29 Opinion on Online Behavioural Advertising*, *supra* note 36, at 15.

[62] *See id.* at 16.

[63] *See id.*

[64] *See id.*

[65] *See id.*

[66] *See WP29 Opinion on Online Behavioural Advertising*, *supra* note 36, at 16.

of cookies, the Working Party suggests that consenting to one cookie should validate all the data that cookie may collect and transmit for a limited time, such as one year.[67]

iii. Consent in Enforcement Actions and Case Law

[17] While enforcement actions under the data protection framework have remained relatively limited, it is useful to examine the few instances in which a Member State's Data Protection Authority ("DPA") have enforced a data protection directive with regard to a breach of the directive's consent requirements.[68] The largest penalty in the Data Protection Directive's history was levied over a consent violation in 2001.[69] The Spanish Data Protection Agency fined the television network Zeppelin TV one million euros for transmitting the personal data of television show participants to third-party advertisers without the participants' consent.[70] More recently in 2008, the Italian DPA fined GS, a supermarket chain, for using information collected from reward card applications and customer purchases to conduct targeted advertising without their customers' consent.[71] Finally, the German DPA brought the most recent enforcement action in 2010 against Deutsche Postbank AG for

[67] *See id.*

[68] *See* CAREY, *supra* note 9, at 183.

[69] *See* TECH., MEDIA & TELECOMM. GRP., LINKLATERS, DATA PROTECTED 102 (Nov. 2005), *available at* www.linklaters.com/pdfs/publications/tmt/dat aprotected05.pdf.

[70] *See* CAREY, *supra* note 9, at 183.

[71] *See Supermarket Chain Fined for Unlawful Use of Customer Data*, EUR. PRIVACY & E-COM. ALERT (Hunton & Williams, L.L.P., Brussels, Belg.), Aug. 2008, at 2, *available at* http://www.hunton.com/european_data_protection_and_privacy (follow "Alerts" hyperlink; then follow "More" hyperlink; and select "European Privacy & E-Commerce Alert: August 25, 2008" hyperlink).

allowing thousands of independent sales agents to use the Bank's customer records for sales purposes without the consent of its customers.[72]

[18] Of the preceding examples, the GS enforcement action proves most relevant to the analysis of consent in behavioral advertising. Unfortunately, few details of the enforcement action have been published and the requisite level of consent necessary to use consumer information for behavioral advertising purposes remains unclear.[73] However, even if interpretations of the GS enforcement establish the principle that targeted advertising requires explicit affirmative consent, it represents one enforcement action under one of the twenty-seven Member States' implementing legislation.[74]

[19] Case law addressing the issue of consent in a data privacy context is correspondingly thin, with only one such case heard by the European Court of Justice.[75] In that case, *Bavarian Lager Co.*, Bavarian Lager requested a copy of the minutes of a meeting during which various

[72] *See* Hunton & Williams, LLP, *German DPA Imposes €120,000 Fine on Deutsche Postbank AG*, PRIVACY & INFO. SECURITY L. BLOG (May 12, 2010, 10:49 AM), http://www.huntonprivacyblog.com.

[73] *See, e.g., Stop Alle Carte Fedeltà se Spiano nel Carrello Della Spesa [Stop the Loyalty Cards in the Shopping Cart if You Spy]*, GARANTE PER LA PROT. DEI DATI PERS. (Reg. Tribunale di Roma, Rome, Italy), May 21, 2008, *available at* www.garantepr ivacy.it/garante/doc.jsp?ID=1522432 (search engine translation from Italian to English).

[74] *See generally Declaration of the Article 29 Data Protection Working Party* on *'Recent Examples of Enforcement Actions Carried out by Data Protection Authorities'*, WP 101 (Nov. 25, 2004), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wp docs/2004/ wp101a_en.pdf (providing examples of data protection enforcement actions in various member states).

[75] *See* European Comm'n, European Anti-Fraud Office (OLAF), *Summary of Caselaw of EU Courts on Data Protection*, at 8, 12 (June 2010) (Laraine Laudati), *available at* http://ec.europa.eu/dgs/olaf/data/doc/Summary-caselaw-EU-courts.pdf (examining European Court of Justice decisions concerning data protection from 2001 to 2010 in which only one case mentions the issue of consent).

government officials and industry representatives determined the company's ability to sell its product in England.[76] The reply to the request stated that it would release the minutes with the names of five parties redacted, including two parties who expressly objected and three who could not be reached.[77] The Court held that the Commission properly refused to release the five names and established that, at least in these circumstances, silence or a failure to respond to a request for consent could not establish informed and free consent.[78]

[20] An earlier case, *British Gas Trading v. Data Protection Registrar*, also discusses the principle that silence does not amount to consent.[79] In that case, "the British Data Protection Tribunal drew a distinction between new and existing customers for the purpose of determining when the requirement of consent would be satisfied."[80] The Tribunal held that new customers of British Gas consented to advertising if they had the chance to opt-out in their initial contract for service.[81] However when British Gas sent existing customers an additional opt out form, their failure to return the form could not qualify as consent.[82]

[21] Given the dearth of enforcement actions and case law on the requirement of consent in the context of data protection, it is hard to draw

[76] *See* Case C-28/08 P, Comm'n v. Bavarian Lager Co., 2010 ECJ EUR-Lex LEXIS 687, at *20 (June 29, 2010).

[77] *See id.*

[78] *See id.* at *40-42.

[79] *See* British Gas Trading Ltd. v. Data Prot. Reg., [1997/98] 1 Info. T.L.R. 393, at 415-16 (Eng.), *available at* http://www.informationtribunal.gov.uk/DBFiles/Decision/i162/british_gas.pdf.

[80] CAREY, *supra* note 9, at 67; *see British Gas*, [1997/98] 1 Info .T.L.R. at 415-16.

[81] *See British Gas*, [1997/98] 1 Info. T.L.R. at 415-16.

[82] *See id.* at 416.

a general picture of the status quo from either of these sources. This ambiguity, combined with the wide variety of implementing legislation, is what the European Commission hopes to clarify by updating the Data Protection Directive.[83]

C. Revising the Data Protection Directive

[22] On November 4, 2010, the Commission explained the need to revise and update the original Data Protection Directive as a way to meet various challenges that have emerged over the past fifteen years.[84] One such challenge is the threat posed by newer and increasingly sophisticated methods of collecting and analyzing personal data that have allowed for more effective targeting of individuals based on their behavior.[85] Another major concern is the lack of uniformity between EU Member State's implementing legislation, despite the common regulatory framework provided by the directives.[86] The European Data Protection Supervisor (EDPS) views the resolution of these ambiguities as necessary "to enhance legal certainty, reduce the administrative burden and ensure a level playing field for economic operators."[87]

---

[83] *See Call for Revision*, *supra* note 13, at 2, 8-9.

[84] *See id.* at 2.

[85] *See id.*

[86] *See id.* at 3-4.

[87] PETER HUSTINX, OPINION OF THE EUROPEAN DATA PROTECTION SUPERVISOR ON THE COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS - "A COMPREHENSIVE APPROACH ON PERSONAL DATA PROTECTION IN THE EUROPEAN UNION" 12 (2011), *available at* http://www.edps.europa.eu/ EDPSWEB/webdav/site/mySite/shared/Documents/ Consultation/Opinions/2011/11-01-14_Personal_Data_ Protection_EN.pdf [hereinafter EDPS ON DATA PROTECTION REVISION].

[23] One specific area of ambiguity between Member State's legislation is the requirement of informed and free consent.[88] For example, the requirements found in various Member States vary widely, from the need for written consent, to the acceptance of implicit consent derived from a user's browser settings.[89] EDPS argues that "[c]onsent that has been inferred by an action and more particularly by silence or inaction is often not an unambiguous consent. However, it is not always clear what constitutes true, unambiguous consent."[90] EDPS further argues that this ambiguity prohibits effective consideration of citizens' rights to the protection of personal data under the law.[91] The Commission has stated that any revision of the Directive should clarify the conditions for a data subject's ability and right to consent.[92] The Commission also noted that the framework should strengthen the data subject's ability to actively refuse consent.[93] The problems stemming from an ambiguous conception of informed and free consent are nowhere more apparent than in the context of behavioral advertising.

D. Emergence of Behavioral Advertising

[24] Online advertising is big business. In 2009, in the twenty-three EU Member States for which data is available, advertisers spent over 4.4 Billion euros on display advertising.[94] In the UK, approximately a third of

[88] *See Call for Revision*, *supra* note 13, at 9.

[89] *See id.* at 8.

[90] EDPS ON DATA PROTECTION REVISION, *supra* note 87, at 18.

[91] *See id.* at 12.

[92] *See Call for Revision*, *supra* note 13, at 9.

[93] *See id.* at 14.

[94] *See* IAB, ADEX 2009 EUROPEAN ONLINE ADVERTISING EXPENDITURE 36 (Sept/ 2010), http://www.iab.fi/assets/Tiedotteet/Adexsyyskuu2010.pdf. The IAB defines Display Advertising as when "an advertiser pays an Internet company for space to display a static or hyper-linked banner or logo on one or more of the Internet company's pages." *Id.*

display advertising utilized behavioral targeting.[95] Assuming this trend represents other EU Member States with mature advertising markets, advertisers spent billions of euros on behavioral advertising in 2009.[96]

[25] The Article 29 Working Party defines behavioral advertising as the practice of tracking a data subject's behavior online, in order to build profiles which deliver more relevant advertising during future browsing sessions.[97] The parties involved in behavioral advertising take on three different roles. The first is the advertising network provider ("ad-network") who performs the tracking, analyzes the data, and connects content publishers with advertisers.[98] The second are advertising companies that want to promote a product or service to a specific

This type of advertising can be contrasted to the other dominant category, Paid Search, which the IAB defines as "[f]ees advertisers pay Internet companies to list and/or link their company site domain name to a specific search word or phrase." *Id.*

[95] *See There's No Need to Talk to Strangers*, MARKETINGWEEK (June 2010), http://www.marketingweek.co.uk/ disciplines/digital/digital-strategy-supplement/theres-no-need-to-talk-to-strangers/3015004.article.

[96] Specific behavioral advertising data for many Member States is unavailable and its use may be lower in less mature or sophisticated markets than in the UK. However, the top three mature markets (the UK, Germany and France) account for 64% of total advertising revenue in the EU. *See* IAB, *supra* note 94, at 5. Thus even if this trend only applies to the top three mature markets, almost a Billion Euros was still spent on behavioral advertising in 2009. *Id.* at 8. Since 2007, venture firms have invested $4.7 billion in 356 online-ad firms, many based on a company's ability to create a more detailed profile of individual users than the next company is capable of providing. *See* Scott Thurm, *Online Trackers Rake in Funding*, WALL ST. J., Feb. 25, 2011, at B1.

[97] *See WP29 Opinion on Online Behavioural Advertising*, *supra* note 36, at 3; *see also* MIREILLE HILDEBRANDT, *Who is Profiling Who? Invisible Visibility*, *in* REINVENTING DATA PROTECTION? 239, 243-44 (Serge Gutwirth et al. eds., 2009) (providing a fictional example of how online profiling operates).

[98] *See WP29 Opinion on Online Behavioural Advertising*, *supra* note 36, at 5.

audience.[99] The third role belongs to content publishers, who earn revenue by displaying the ads on their website.[100]

[26] Behavioral advertising companies glean information from a variety of sources, including what websites a user visits, how the user interacts with those sites, and content created by the user that is posted on publicly accessible websites or social networks.[101] This information is then supplemented with information voluntarily provided by the user to websites.[102] For instance, by entering your date of birth to verify your age on an alcohol company's website, you could add your birthday to your profile.[103] Similarly, a user's physical location, as determined from their IP address, can become part of a user's profile.[104] Profiles created from these online sources can combine with traditional offline data to create a more comprehensive profile.[105]

[27] The primary technology used by the behavioral advertising industry is the tracking cookie.[106] Specifically, ad-network providers

[99] *Id.*

[100] *Id.*

[101] *See id.* at 4.

[102] *See, e.g., Ad Specifications*, HULU (June 15, 2011), http://assets.huluim.com/downloads/hulu_ad_specs.pdf.

[103] *See, e.g., Age Verification*, LAPHROAIG, http://www.laphroaig.com (last visited Sept. 25, 2011) (showing that when prompted to become a Friend of Laphroaig, the user's age is automatically imported into the user's profile).

[104] *See, e.g., id.*

[105] *See* BUREAU OF CONSUMER PROT., FED. TRADE COMM'N, ONLINE PROFILING: A REPORT TO CONGRESS 5 (2000), *available at* http://www.ftc.gov/os/2000/06/onlineprofilingreportjune2000.pdf [hereinafter ONLINE PROFILING: A REPORT TO CONGRESS].

[106] *Id.* at 3.

begin the profiling process by tracking users through some form of "client-side processing" that consists of the physical storage of a file—such as a cookie—on a data subject's computer.[107] It is crucial to distinguish tracking cookies, or third-party cookies, from standard first-party cookies used by almost every website.[108] While tracking cookies are a controversial tool used by the behavioral advertising industry, standard cookies are innocuous and currently essential to the functionality of the modern Internet.[109]

[28] First-party cookies are small text files placed on a computer by websites that a user visits that allow content providers to enhance basic functionality with features such as the storage of login information, layout preferences, and preferred payment methods or shipping addresses.[110] While the discussion of behavioral advertising often includes first-party cookies, the use of first-party cookies is widely accepted even without a user's consent.[111] To avoid confusion, the debate over the use of third-

[107] *See WP29 Opinion on Online Behavioural Advertising*, *supra* note 36, at 6.

[108] *See* Lori Eichelberger, *The Cookie Controversy: Cookies and Internet Privacy*, COOKIECENTRAL.COM, http://www.cookiecentral.com/ccstory/cc3.html (last visited Sept. 16, 2011) (explaining the dangers between first and third party cookies).

[109] *See What Went Wrong?*, COOKIECENTRAL.COM, http://www.cookiecentral.com/cookie5.htm (last visited Sept. 17, 2011).

[110] See Lori Eichelberger, *The Cookie Controversy: Introduction*, COOKIECENTRAL.COM, http://www.cookiecentral.com/ccstory/index.html (last visited Sept. 17, 2011); Lori Eichelberger, *The Cookie Controversy: The Purpose of Cookies*, COOKIECENTRAL.COM, http://www.cookiecentral.com/ccstory/index.html (last visited Sept. 17, 2011); *Implementing Machine Language Privacy Requirements – User: First-Party Cookie*, DEPARTMENT OF COMMERCE WEB ADVISORY COUNCIL, http://www.osec.doc.gov/webresources/P3P_User_Admin_files/TextMostly/Slide17.html (last updated May 14, 2010).

[111] *Implementing Machine Language Privacy Requirements – User: Cookies*, DEP'T OF COMMERCE WEB ADVISORY COUNCIL, http://www.osec.doc.gov/webre sources/P3P_User_Admin_files/TextMostly/Slide10.html (last updated May 14, 2010); *see* Eichelberger, *The Cookie Controversy: Cookies and Internet Privacy*, *supra* note 108.

party tracking cookies, discussed in more detail below, should not consider first-party cookies.

[29] Typically, an ad-network places a tracking cookie on a user's computer when a user first visits the website of one of the ad-network's clients.[112] Once the ad-network places the cookie, it can recognize it anytime the same user browses to a webpage where the ad-network may operate.[113] By re-accessing the cookie at each new site the user visits, the ad-network builds a profile based on the user's online behavior.[114] Some of the Internet's most visited websites allow multiple ad-networks to place tracking cookies on a user's computer, a practice that can result in as many as 200 separate cookies being placed on a user's computer in a single visit.[115]

[30] As technologies emerge to help users exercise their privacy rights regarding cookies, ad-networks develop new technologies at an even faster pace.[116] While older versions of cookies had expirations after which they no longer functioned, persistent cookies may remain active until deleted by the user.[117] Ad-networks are also experimenting with hard to erase tracking technologies, such as flash cookies, tracking beacons, biometric profiling and deep packet inspection.[118] These technologies can track

[112] *WP29 Opinion on Online Behavioural Advertising*, *supra* note 36, at 6.

[113] *Id.*

[114] *Id.*

[115] *See* Julia Angwin, *The Web's New Gold Mine: Your Secrets*, WALL ST. J., July 31, 2010, at W1; *What They Know*, WALL ST. J. L. BLOG, http://blogs.wsj.com/wtk/ (last visited Sept. 14, 2011) (finding that dictionary.com places 234 tracking files in a single visit, comcast.net places 151, careerbuilder.com places 118, and msn.com places 207).

[116] *See, e.g.*, *WP29 Opinion on Online Behavioural Advertising*, *supra* note 36, at 6.

[117] *See id.*

[118] *See id.*; Julia Angwin, *Latest in Web Tracking: Stealthy 'Supercookies,'* WALL ST. J., Aug. 18, 2011, at A1; Steve Stecklow & Paul Sonne, *What They Know: A Wall Street*

users outside of the controls built into today's web-browsers, thus depriving users of the already limited ability to control their privacy settings.[119] While the details of these new methods are technologically complex, the goal is the same: to create a tracking device that is not easily deleted, and, if deleted, has the ability to 're-spawn' or 'un-delete' itself.[120]

E. Concerns Regarding Behavioral Advertising

[31] A recent study by England's consumer protection agency, the Office of Fair Trading ("OFT"), found that 40% of consumers hold neutral views towards behavioral advertising, 28% percent dislike the practice, and 24% percent welcome it.[121] Additionally, the OFT found that

Journal Investigation: Shunned Profiling Method on the Verge of Comeback, WALL ST. J., Nov. 24, 2010, at A1 ("[D]eep packet inspection [technology] . . . can be far more powerful than 'cookies' . . . because it can be used to monitor all online activity, not just Web browsing. Spy agencies use the technology for surveillance.").

[119] *See* Rodica Tirtea et al., *Bittersweet Cookies: Some Security and Privacy Considerations*, EUROPEAN NETWORK & INFO. SEC. AGENCY 8 (2011) [hereinafter ENISA Cookie Report], *available at* http://www.enisa.europa.eu/act/it/library/pp/cookies/.

[120] *See WP29 Opinion on Online Behavioural Advertising*, *supra* note 36, at 6-7.

[121] OFFICE OF FAIR TRADING, ONLINE TARGETING OF ADVERTISING AND PRICES: A MARKET STUDY 7 (2010), *available at* http://www.oft.gov.uk/shared_oft/business_leaflets/659703/OFT1231.pdf. Similar studies in the United States and Canada have found consumers are not in favor of behavioral advertising. *See* JANET LO, PUB. INTEREST ADVOCACY CTR., A "DO NOT TRACK LIST" FOR CANADA 11 (2009), *available at* www.piac.ca/files/dntl_final_ website.pdf ("The majority of respondents (54%) [in a recent Canadian study] strongly supported the creation of a 'Do Not Track List', and an additional 27% of respondents somewhat supported a 'Do Not Track List' . . . ."); JOSEPH TUROW ET AL., CONTRARY TO WHAT MARKETERS SAY, AMERICANS REJECT TAILORED ADVERTISING AND THREE ACTIVITIES THAT ENABLE IT 15 (2009), *available at* http://ssrn.com/abstract=1478214 (finding that 66% percent of American adults do not want to be shown targeted advertising and that when told of how behavioral marketers gather their information, this percentage jumped to between 73% and 86%).

concerns over behavioral advertising decreased when consumers could, if they desired, opt-out of behavioral advertising and its related tracking activities.[122]

[32] While individual concerns about behavioral advertising vary, many people simply feel violated upon learning that ad-networks compile and sell their personal details without their knowledge or consent.[123] For instance, in the weeks leading up to a U.S. primary election last October, a sixty-seven year old woman named Linda Twombly was bombarded with advertisements urging her to donate and vote for a specific Republican candidate.[124] The ads were eerily omniscient; Ms. Twombly *was* a Republican and *did have* a history of donating to political campaigns.[125] However, the ads were not based on information Ms. Twombly had volunteered to the candidate or the party.[126] Rather, they were based on information *sold* to the candidate by a company whose algorithms determined these facts from Ms. Twombly's online behavior.[127]

[33] Another recent example of such behavior is a teenage girl who saw weight-loss ads every time she went on the Internet after an ad-network identified her as falling within a category of people desiring to lose weight.[128] There is also the infamous example of a man who bought his

[122] OFFICE OF FAIR TRADING, *supra* note 121, at 36.

[123] *See* HILDEBRANDT, *supra* note 97, at 242-43.

[124] *See* Emily Steel, *What They Know: A Wall Street Journal Investigation: A Web Pioneer Profiles Users by Name,* WALL ST. J., Oct. 25, 2010, at A1.

[125] *See id.*

[126] *See id.*

[127] *See id.*

[128] Angwin, *Gold Mine*, *supra* note 115; *see also* Nicholas Carr, *The Great Privacy Debate -- Tracking Is an Assault on Liberty, with Real Dangers*, WALL ST. J., Aug. 6, 2010, (Weekend Journal), at W1; Transcript of Workship at 61:5-15, Fed. Trade Comm'n Roundtable Series 1 on: Exploring Privacy (Dec. 7, 2009) (Matter No. P095416),

wife a ring on Overstock.com only to have the purchase, complete with his 51% discount, broadcast on his Facebook newsfeed.[129]

[34] Furthermore, behavioral advertising has practical and economic consequences. The European Network and Information Security Agency ("ENISA") identified various technological threats presented by behavioral advertising, including network threats, end-system threats, and cookie-harvesting threats.[130] These techniques can modify the information returned by cookies from a user's computer to the ad-networks, secretly collect a user's information by impersonating cookies of legitimate websites, or recreate a user's full search history from search engines such as Google.[131]

[35] Other threats revolve around the claim of anonymity for behavioral profiles. While most companies insist any data collected remains anonymous, newly created algorithms can "de-anonymize" these profiles by adding names, addresses, and phone numbers.[132] A recent study found that third-party trackers increasingly link "anonymous" profiles to

available at http://www.ftc.gov/bcp/workshops/privacyroundtables/PrivacyRoundtable_Dec2009_Transcript.pdf (describing the potential to target obese, anxious or other vulnerable market niches).

[129] *See* Sheppard Mullin, *Efficiency v. Privacy: Is Online Behavioral Advertising Capable of Self-Regulation?*, COVERING YOUR ADS BLOG, (Apr. 14, 2010), http://www.coveringyourads.com/2010/04/articles/advertising-law/efficiency-v-privacy-is-online-behavioral-advertising-capable-of-selfregulation/.

[130] *See* ENISA Cookie Report, *supra* note 119, at 7.

[131] *See id.*

[132] *See* Steel, *supra* note 124; *see also* Dennis D. Hirsch, *The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?*, 34 SEATTLE U. L. REV. 439, 450 (2007) (noting that offline sources used by data brokers include public records, the media and credit-reporting agencies and that data brokers "have been combining this off-line data, traceable to specific individuals, with online data that they can match to those same individuals").

personally identifiable information through the use of social networks.[133] One potential consequence of de-anonymization is the risk of identity theft if an individual hacks into an ad-network's database.[134] London Economics performed a case study that examined a recent incident involving TNS Infratest, a German marketing company engaged in behavioral profiling.[135] The company held profiles on 90,000 German households, many of which contained detailed information including individuals' names, addresses, dates of birth, education levels, marital status, household incomes, bank accounts, health insurance and even details on consumer purchases such as cars, mobile phones and computers.[136] Unfortunately, the hacking of this database exposed all 90,000 profiles.[137]

[36] Similarly, a recent study at Carnegie Mellon University showed that hacking is not even necessary for identity theft.[138] Using the same "anonymous" information generally found in behavioral advertising profiles such as place of birth and birth date, computer algorithms can determine Social Security numbers for "8.5% of people born in the United

[133] ENISA Cookie Report, *supra* note 119, at 8; Balachander Krishnamurthy & Craig E. Wills, *On the Leakage of Personally Identifiable Information Via Online Social Networks*, 40 COMPUTER COMM. REV. 112, 117 (2010).

[134] *See* LONDON ECON., STUDY ON THE ECONOMIC BENEFITS OF PRIVACY-ENHANCING TECHNOLOGIES (PETS) 204 (2010).

[135] *Id.* at 201-04.

[136] *Id.* at 201-02.

[137] *Id.* at 204 (discussing how the incentive to steal such data is high as a complete consumer profile that includes bank credentials can sell for as much $1,000 a person).

[138] Alessandro Acquisti & Ralph Gross, *Predicting Social Security Numbers from Public Data*, 106 PROC. NAT'L. ACAD. SCI. 10975, 10975 (2009); Steve Lohr, *How Privacy Vanishes Online*, N.Y. TIMES, Mar. 16, 2010, http://www.nytimes.com/2010/03/17/technology/17privacy.html?scp=9&sq=%22do%20not%20track%22&st=Search.

States between 1989 and 2003."[139] With access to the right software, almost five million Social Security numbers are potentially up for sale.[140]

[37] Widespread profiling also allows for price discrimination and social sorting.[141] Online price discrimination, or even the outright denial of service or products, is known as "weblining," an online version of traditional economic discrimination practices such as "redlining" and "reverse redlining."[142] Weblining can create pricing schemes to discriminate between individual customers and can target especially vulnerable populations such as the poor or uneducated.[143] Some of these potential harms are already being realized. For example, British insurer Aviva recently used online data profiles in order to categorize potential insurance applicants in various risk profiles.[144]

[38] Lee Tien, a senior staff attorney for the Electronic Frontier Foundation, worries about what might happen if employers have access to profiles which allows them to see whether an employee is pregnant or considering trying to become pregnant.[145] Tien raises similar concerns about other vulnerable populations that deserve anonymity, such as

[139] Acquisti & Gross, *supra* note 138, at 10975; Lohr, *supra* note 138.

[140] *See* Lohr, *supra* note 138.

[141] *See* HILDEBRANDT, *supra* note 97, at 244.

[142] *See* ONLINE PROFILING: A REPORT TO CONGRESS, *supra* note 105, at 13, n.45 (defining redlining and reverse redlining as "the practice of some financial institutions to not extend credit or to offer less favorable credit terms to prospecitve [sic] borrowers in predominantly minority areas").

[143] *See* LO, *supra* note 121, at 53.

[144] Leslie Scism & Mark Maremont, *Insurers Test Data Profiles to Identify Risky Clients*, WALL ST. J., Nov. 19, 2010, at A1.

[145] Stein, *supra* note 1.

political dissidents and battered women.[146] Other scholars worry about the use of inaccurate data sets in determining the outcome of employment, dating, or educational decisions.[147] Finally, as profiling becomes even more commonplace, a user's attempts to shield personal data will have consequences of their own.[148] For instance, a user who attempts to hide their data to remain anonymous may be discriminatorily denied service, forced to pay more, or simply categorized for their refusal.[149]

F. Privacy by Design and Privacy Enhancing Technologies

[39] The fundamental principal of Privacy by Design ("PbD") is that a system should address privacy concerns in its design, as opposed to addressing these concerns once the system has become vulnerable.[150] The collection-limitation principle, one of the core principals of PbD systems, requires that "the lawful collection of data" must take place with the informed "knowledge or consent of the data subject."[151] In this way, the principals of PbD compare remarkably to the consent requirements in the EU's data protection framework.[152]

[40] While the goal of PbD is technically possible today, few businesses attempt to implement its principles.[153] To the contrary, Daniel

[146] *See id.*

[147] *See id.*

[148] *See* LO, *supra* note 121, at 53 (claiming that online profiling may lead to a loss of consumer autonomy).

[149] *See id.*

[150] DANIEL LE MÉTAYER, *Privacy by Design: A Matter of Choice*, *in* DATA PROTECTION IN A PROFILED WORLD 323-24 (Serge Gutwirth et al. eds., 2010).

[151] *Id.* at 325.

[152] *See id.*

[153] *See id.* at 326.

Le Métayer, a leading expert in PbD systems, argues that most online systems actually fall into one of three categories, all of which fall short of PbD ideals.[154] The first category is "non-privacy by design" where the "system deliberately infringes privacy rights."[155] Such systems are common and include any online registration system that requires information outside of what is required to process the immediate transaction.[156] The next category is "non-privacy by non-design" where privacy issues are ignored throughout the design process.[157] Such systems include websites that do not offer opt-out mechanisms or lack internal policies to destroy data after a set expiration period.[158] The last category is "non-privacy by bad design" where the system's design considers privacy concerns but falls short in the end.[159]

[41] PbD attempts to provide users with a meaningful way to express their choices, despite the tendency of these choices to involve many subtleties or ambiguities, and for the system to respect those choices.[160] For example, a PbD system must take into account that routine consent does not have practical import.[161] Examples of the routinization of

---

[154] *See id.*

[155] MÉTAYER, *supra* note 150, at 326.

[156] *See id.*

[157] *Id.*

[158] *Id.*

[159] *See id.*

[160] *See* MÉTAYER, *supra* note 150, at 327.

[161] Roger Brownsword, *Consent in Data Protection Law: Privacy, Fair Processing and Confidentiality*, *in* REINVENTING DATA PROTECTION? 83, 90 (Serge Gutwirth et al. eds., 2009).

consent abound, as anyone who has clicked "I agree" when installing software without reading the fine print well knows.[162]

[42] Others argue for the use of Privacy Enhancing Technologies ("PET"). Unlike Privacy by Design, PETs are not necessarily designed into the systems that implement them.[163] A PET is defined as "[a] technology whose primary purpose is to enhance the privacy of a user."[164] A study for the Dutch Ministry of the Interior defined PETs as a mechanism of "translation of 'soft' legal standards into 'hard' system specifications."[165] Successful PETs generally have a number of properties in common, including usability, deployability, effectiveness, and robustness.[166]

[43] Many commentators suggest that PbD, PETs, or some combination of both, may provide an answer to the threat to privacy posed by behavioral advertising.[167] Such efforts are technologically feasible. For

---

[162] *See id.* (mentioning routinisation by directing an agent to "sign here and here" or "just tick the box").

[163] *See* LONDON ECON., *supra* note 134, at 14.

[164] Jane K. Winn, *Technical Standards as Data Protection Regulation*, *in* REINVENTING DATA PROTECTION? 191, 199 (Serge Gutwirth et al. eds., 2009).

[165] *Id.* (quoting KPMG ET AL., MINISTRY OF THE INTERIOR AND KINGDOM RELATIONS, THE NETH., PRIVACY–ENHANCING TECHNOLOGIES: WHITE PAPER FOR DECISION-MAKERS 51 (Dec. 2004), *available at* http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.101.7649&rep=rep1&type=pdf [hereinafter KPMG].

[166] *See* LONDON ECON., *supra* note 134, at 14.

[167] *See, e.g.*, FTC, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS 44-52 (December 2010), *available at* http://ftc.gov/os/2010/12/101201privacyreport.pdf (recommending that companies "assess the privacy impact of specific practices, products, and services to evaluate risks and ensure that the company follows appropriate procedures to mitigate those risks"); *Online Tracking and Behavioral Profiling*, EPIC.ORG, http://epic.org/privacy/consumer/online_tracking_and_behavioral.html (last visited Oct. 12, 2010).

instance, the browser Firefox recently announced it would implement a Do-Not-Track feature into the next version of its web browser, while Microsoft implements a similar initiative in Internet Explorer 9.[168] However, for these technologies to work, advertising networks must agree to respect users' settings.[169] To date, not a single company has agreed to participate in either of these programs.[170]

G. Attempts at Self-Regulation in the Behavioral Advertising Industry

[44] Recently, the behavioral advertising industry has begun a renewed attempt at self-regulation.[171] Each of the major efforts, one in the U.S. and one in the EU, offers consumers information regarding behavioral advertising, creates a framework of best practices which member ad-networks promise to abide by, and gives consumers the opportunity to opt-out of behavioral advertising from selected ad-networks.[172] Despite the apparent progress evidenced by these efforts, many commentators

---

[168] Julia Angwin, *Web Tool on Firefox to Deter Tracking*, WALL ST. J., Jan. 24, 2011, http://online.wsj.com/article/ SB10001424052748704213404576100441609997236.html; Cade Metz, *Google, MS, Mozilla: Three 'Do Not Tracks' To Woo Them All: So Many Ways to Do One Simple Thing*, THE REG. UK (Feb. 14, 2011), http://www.theregister.co.uk/2011/02/14/google_mozilla_and_microsoft_do_do_not_track/.

[169] *See* Angwin, *Web Tool*, *supra* note 168.

[170] *See id.*

[171] *See generally* Digital Adver. Alliance, *The Self-Regulatory Principles for Online Behavioral Advertising*, THE SELF-REG. PROGRAM FOR ONLINE BEHAV. PROGRAMMING, http://www.aboutads.info/ (last visited Sept. 25, 2011); *IAB Good Practice Principles*, YOUR ONLINE CHOICES, http://www.youronlinechoices.com/good-practice-principles (last visited Sept. 25, 2011).

[172] *See* Digital Adver. Alliance, *supra* note 171; *IAB Good Practice Principles*, *supra* note 171.

question whether self-regulation provides the entire answer, given the behavioral advertising industry's contrary incentives.[173]

[45] In *The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?*, Professor Dennis Hirsh outlines three broad critiques of self-regulation in online privacy. First, "firms will put their own profits before ahead of the public interest [in privacy]."[174] Second, self-regulatory programs generally lack the power or will to truly enforce the guidelines against its members.[175] Third, as long as membership in self-regulatory programs remains voluntary, most companies will choose to "free ride" on any good-will generated by the programs without restriction by the guidelines themselves.[176]

[46] The first critique argues that it is not in the best economic interest of the ad-networks to effectively enroll consumers because each enrollment hurts their bottom line.[177] As an illustration of this argument, the Electronic Privacy Information Center ("EPIC") points out that the telecommunication industry's self-regulatory efforts in the 1990's managed to enroll just about 5 million consumers, versus the over 200 million now registered in the FTC's Do-Not-Call list.[178] The trend will

[173] *See, e.g.*, CHRIS JAY HOOFNAGLE, ELEC. PRIVACY INFO. CTR., PRIVACY SELF REGULATION: A DECADE OF DISAPPOINTMENT 1, 15 (2005) [hereinafter EPIC], *available at* http://epic.org/reports/decadedisappoint.html; Scott Foster, *Online Profiling Is on the Rise: How Long Until the United States and the European Union Lose Patience with Self-Regulation?*, 41 SANTA CLARA L. REV. 255, 258, 277 (2000); Mullin, *supra* note 129.

[174] Hirsch , *supra* note 132, at 458.

[175] *Id.*

[176] *Id.* at 459.

[177] *See id.* at 468.

[178] *Compare* EPIC, *supra* note 173, at 1, *with* Nate Anderson, *Do Not Call List Tops 200 Million, Some Scammers Still Ignore It*, ARSTECHNICA.COM, http://arstechnica.com/tech-policy/news/2010/07/telemarketing-remember-just-how-bad-it-was.ars (last visited Sept.

most likely hold for behavioral advertising; in fact, the Network Advertising Initiative ("NAI"), the central mechanism for the new U.S. opt-out initiative, has offered a version of its new opt-out service, with little to no success.[179]

[47] The second critique argues that, in addition to the limitations imposed by its voluntary membership, initiatives such as the NAI opt-out cannot be entirely successful because they lack the accountability and enforcement opportunities offered by equivalent government regulation.[180] In this vein, some commentators argue that because consumers have no way to monitor a company's use of their information, they cannot discipline the company efficiently in the marketplace for violations.[181]

[48] Third, maintaining a significant membership in a voluntary program such as NAI or IAB is unlikely.[182] Critics point to NAI's previous attempts at self-regulation as evidence.[183] In 2000, NAI initiated a self-regulatory regime for online privacy and even appointed an independent organization to enforce violations.[184] However, while the program started with twelve of the largest ad-networks, by 2003, its membership dwindled to just two.[185] The independent enforcer slowly

15, 2011) (discussing how the Federal Trade Commission acknowledged the Do Not Call registry's passing 200 million in numbers).

[179] *See* EPIC, *supra* note 173, at 9-10.

[180] *See id.* at 10.

[181] *See* Foster, *supra* note 173 at 262, 266.

[182] *See* Hirsch, *supra* note 132, at 458-59.

[183] *Id.* at 462.

[184] *Id.*

[185] *Id.* at 463; *see* EPIC, *supra* note 173, at 9-10 ("Further contributing to the irrelevance of NAI is the fact that its membership has depleted to two: DoubleClick and Atlas DMT.").

stopped reporting compliance and enforcement statistics and, in 2006, scrapped the entire program.[186]

[49] Finally, some critics argue that scattered self-regulatory programs are ineffective because users have to find, learn about, and apply to a potentially large number of competing opt-out programs.[187] This is compounded in the behavioral advertising industry because the opt-out programs are generally limited to a small subset of ad-networks that choose to participate.[188] Additionally, opt-out programs vary in efficacy. DoubleClick, a large advertiser, will still show users targeted ads even if they opt-out.[189] DoubleClick only promises not to use what they themselves consider personal information to generate the ads.[190] Finally, self-regulated opt-out programs are generally temporary because they rely on the user to not clear their cookies, a task many users concerned about privacy regularly do.[191]

III. ANALYSIS

[50] This Part will argue that the EU's current legal framework is incapable of providing consumers with a meaningful method to consent or refuse to consent to behavioral advertising. It will then argue that

---

[186] *Id.*

[187] *See* Hirsch, *supra* note 132, at 455.

[188] *See generally* Digital Adver. Alliance, *supra* note 171 ("You can now visit the beta version of the Program's Consumer Opt Out Page, which allows users to conveniently opt-out from online behavioral ads served by some or all of our *participating* companies." (emphasis added)); *IAB Good Practice Principles*, *supra* note 171 (providing a list of companies that are complying with the IAB Good Practice Principles).

[189] LO, *supra* note 121, at 50.

[190] *Id.*

[191] *See id.*

requiring a "Do-Not-Track" mechanism in the revised Data Protection Directive satisfies the Treaty of Lisbon, meets the twin objectives of the original Directive, and fulfills the five applicable revision objectives as expressed by the Commission.[192] It will also consider and respond to various technological and economic criticisms of a Do-Not-Track mechanism. Finally, the Article will argue against alternative solutions, including self-regulation.

A. The Current Data Protection Framework

[51] The EU's data protection framework, as set out by the Data Protection Directive, e-Privacy Directives and the Treaty of Lisbon, purports to guarantee citizens the right to the protection of personal data.[193] Behavioral advertisers must operate within the confines of the data protection framework because behavioral advertising requires the collection and use of Internet users' personal data to track and target individuals based on their online activities.[194] Ad-networks who engage in behavioral advertising must secure informed consent from users *before* engaging in behavioral advertising, or they risk violating a user's right to the protection of personal data.[195]

[52] Today, many experts believe that behavioral advertising violates a citizen's right to the protection of personal data because ad-networks generally fail to secure informed consent from the user.[196] The failure to

[192] *Call for Revision*, *supra* note 13, at 5-10; *see* Treaty of Lisbon art. 16 B; Data Protection Directive, *supra* note 10, Preamble para. 7.

[193] Treaty of Lisbon art. 16 B; Data Protection Directive, *supra* note 10, Preamble para. 7; e-Privacy Directive, *supra* note 26.

[194] *See supra* Part II.D.

[195] *See id.* at 4.

[196] *See WP29 Opinion on Online Behavioural Advertising*, *supra* note 36, at 9; *infra* Part II.B.iii.

prevent such violations stems from the ambiguity surrounding the meaning of consent, which the data protection framework does not define.[197] The failure to sufficiently define consent in the directives has frustrated efforts to clarify the meaning of consent in case law, enforcement efforts, and national implementing legislation.[198] As a result of this ambiguity, ad-networks may act in violation of citizens' rights without consequence.[199] In 2010, the Commission called for an overhaul of the Directive, in part because of such ambiguities.[200]

[53] It is crucial to note that past attempts to rectify issues in the data protection framework, including the adoption of the e-Privacy Directive and its amending Directive, have failed to resolve the ambiguity over the meaning of consent under the framework.[201] By attempting to rectify the issue, the newer directives made similar mistakes as the original Data Protection Directive, namely, making ambiguous statements regarding informed and free consent and leaving the actual implementation and interpretation of its provisions to the twenty-seven EU Member States.[202] To meet the Commission's stated goal of a uniform regulation that provides users with a chance to effectuate informed and free consent to behavioral advertising, any revision of the Data Protection Directive will have to be clearer and more specific than its predecessor legislation.[203]

---

[197] *See* EDPS ON DATA PROTECTION REVISION, *supra* note 87, at 12 ("The Directive contains a number of provisions that are broadly formulated and that therefore leave significant room for diverging implementation.").

[198] *See id.*; *Call for Revision*, *supra* note 13, at 8-9; *supra* Part II.B.iii.

[199] This is evidenced by the size of the behavioral advertising industry and the lack of enforcement actions over potential violations. *See supra* Part II.B.iii.

[200] *See Call for Revision*, *supra* note 13, at 8-9.

[201] *See id.*

[202] *See generally id.*

[203] *See id.* at 7-8.

B. Proposal

[54] A universal "Opt-Out" or "Do-Not-Track" mechanism satisfies the right to the protection of personal data, including the requirement of informed and free consent, under the Treaty of Lisbon and EU Charter of Fundamental Rights.[204] The mechanism also meets the twin aims of the original Data Protection Directive, as well as each of the five applicable objectives outlined by the European Commission for the Data Protection Directive's revision.[205]

i. Framework for Potential Solutions

[55] Any proposal for the revision of the Data Protection Directive must satisfy a variety of parameters. First, any solution must, at its most basic level, satisfy the EU Charter of Fundamental Rights in that "data must be processed fairly for specified purposes and on the basis of the consent of the person concerned . . . ."[206] As discussed above, in the case of behavioral advertising, the current framework fails to secure this right.[207] Second, any proposal should attempt to meet the twin aims of the original Data Protection Directive: the protection of personal data and the free flow of information in commerce.[208] Furthermore, since the adoption of the Treaty of Lisbon, the protection of personal data is more than an aim—it is

[204] *See generally* Treaty of Lisbon art. 68; EU Charter of Fundamental Rights, *supra* note 18, at 10 (explaining rights of protection for personal data).

[205] S*ee generally Call for Revision*, *supra* note 13, at 5-10 (outlining twin aims and five objectives).

[206] EU Charter of Fundamental Rights, *supra* note 18, at 10; s*ee Call for Revision*, *supra* note 13, at 11.

[207] *See generally supra* Part II.B.ii (discussing problems with the current framework).

[208] *Call for Revision*, *supra* note 13, at 2; Data Protection Directive, *supra* note 10, paras. 2-3.

a constitutionally guaranteed right.[209] Finally, the Commission has outlined additional objectives for the revised legislation. Five of these objectives are applicable to, and resolved by, the current proposal: (1) ensuring a coherent application of data protection rules; (2) providing a mechanism for users to effectuate informed and free consent; (3) strengthening individuals' rights in the face of new technologies; (4) increasing transparency; and (5) providing users increased control over their data.[210]

ii. The Do-Not-Track Mechanism

[56] A Do-Not-Track mechanism would utilize PbD and PET principles to build a tool that allows a user to provide informed and free consent through their web browser.[211] As suggested by the Dutch Ministry of the Interior, the use of PETs would "[translate] the 'soft' legal standards" of the data protection directives "into 'hard' system specifications" that create a unified mechanism for informed and free consent for every citizen in the EU.[212]

[57] The Do-Not-Track mechanism could work as follows: every browser would have an initial settings wizard where the user could choose their level of exposure to targeted advertisements while using the Internet.[213] Users would receive information on behavioral advertising generally, and could read in greater detail about specific ad-networks, including their methods of data collection and types of analysis employed.

---

[209] *See* Treaty of Lisbon, *supra* note 21, at 68; Press Release, Charter of Fundamental Rights, *supra* note 20.

[210] *Call for Revision*, *supra* note 13, at 5-10.

[211] *See* Angwin, *Web Tool*, *supra* note 168; Metz, *supra* note 168; Winn, *supra* note 164, at 199; *see also supra* Part II.F.

[212] Winn, *supra* note 164, at 199; KPMG, *supra* note 165.

[213] *See* Angwin, *Web Tool*, *supra* note 168; Metz, *supra* note 168.

This wizard would be legally mandatory for a browser to offer to a user before the user is allowed to use a browser for the first time.[214] Finally, the mechanism would never exclude first-party cookies so basic Internet functionality remains undisturbed.[215] After a user sets their choices, ad-networks could request permission from users to be added as an exception to a user's general preference set. This request should conform to the suggestions for transparency outlined by the Working Party.[216] Thus, any request would need to include the types of data collected, the purposes of the collection, and the potential uses of the data by third parties.[217]

iii. Satisfaction of Informed and Free Consent

[58] First, and most importantly, the mechanism would satisfy the Treaty of Lisbon by providing users with the chance to express informed and free consent to tracking and behavioral advertising.[218] While the Treaty of Lisbon uses general language regarding consent, the courts, enforcement authorities, and Article 29 Working Party have offered a limited degree of clarification.[219] A Do-Not-Track mechanism would satisfy the findings of the courts and enforcement authorities that silence does not indicate consent.[220] The principal that silence cannot equal

[214] *See generally supra* Part II.B.ii (discussing the current issues with user data protection, and the need for a better method of informing users of data protection options).

[215] *See supra* Part II.D (discussing how first party cookies allow storage of logins, layout preferences, payment methods or shipping addresses).

[216] *WP29 Opinion on Online Behavioural Advertising*, *supra* note 36, at 15.

[217] *See id.* at 12-13.

[218] *See* Treaty of Lisbon art. 16 B.

[219] *WP29 Opinion on Online Behavioural Advertising*, *supra* note 36, at 13-17.

[220] *See, e.g.*, Case C-28/08 P, Comm'n v. Bavarian Lager Co., 2010 EUR-Lex LEXIS 687, at *42 (June 29, 2010) ("By requiring that, in respect of the five persons who had not given their express consent, Bavarian Lager establish the necessity for those personal

consent, derived from the *Bavarian Lager* and *British Gas* cases, contrasts with the current norm in many EU Member States where browser settings, even if left on default, are sufficient evidence of a user's intent to provide consent.[221] Under the current proposal, users must make an informed, affirmative decision; eliminating the risk that a user's silence could suggest consent to an ad-network.[222]

[59] To qualify as informed consent, the Data Protection Directive mandates that data subjects should be notified of the "identity of the [data] controller . . . the purposes of the processing . . . [and] any further information . . . in so far as such further information is necessary . . . to guarantee fair processing in respect of the data subject."[223] The Working Party agrees that for truly informed consent, a user must receive transparent information regarding the placement of the tracking cookie.[224] The Do-Not-Track mechanism also satisfies this mandate. Under the proposal, Member States, national DPA's, or the Working Party could be

data to be transferred, the Commission complied with the provisions of Article 8(b) of Regulation No 45/2001.").

[221] *Compare id.*, *and* CAREY, *supra* note 9, at 66-67, *with* Warma & Kemppainen, *supra* note 32 (noting that Recital 66 of the E-Privacy Directive permits consent to be obtained via browser settings, the defaults of which generally allow cookies).

[222] *See* Data Protection Directive, *supra* note 10, art. 7(a); *see also*, *WP29 Opinion on Online Behavioural Advertising*, *supra* note 36, at 13 ("[F]or consent to be valid . . . it must be freely given, specific and constitute an informed indication of the data subject's wishes . . . before the personal data are collected, as a necessary measure to ensure that data subjects can fully appreciate that they are consenting and what they are consenting to.").

[223] Data Protection Directive, *supra* note 10, art. 10.

[224] *WP29 Opinion on Online Behavioural Advertising*, *supra* note 36, at 17-18 ("The data subject should be clearly informed that the cookie will allow the advertising provider to collect information about visits to other websites, the advertisements they have been shown, which ones they have clicked on, timing etc.," in such a manner that is "clear and comprehensive" and "as user friendly as possible") (quoting Data Protection Directive, *supra* note 10, art. 10) (emphasis omitted).

tasked with creating the information presented to a user during the setup process in each user's browser. A user may consider the choice of whether and to what extent to consent to behavioral advertising, utilizing objective information provided by a trustworthy source. This proposal represents a stark contrast from the status quo, in which consent appears to be sufficient no matter how uninformed the user happens to be.[225]

[60] Finally, the Working Party's interpretation of informed and free consent mandates that consent be easily revocable.[226] Under the Do-Not-Track proposal, by using a universal setting through the browser, a user could switch between allowing third-party tracking for all purposes, to allowing tracking for certain narrow purposes, to never allowing tracking at all, simply with the click of a button.

iv. Satisfaction of the European Commission's Objectives for Revision

[61] The proposal for a Do-Not-Track mechanism also elegantly meets the stated objectives of the European Commission for the revision of the Data Protection Directive.[227] First, the mechanism would ensure a coherent application of data protection rules, because the Do-Not-Track mechanism would be consistently implemented throughout the EU.[228] Under the proposal, ad-networks would have to respect a user's decision to opt-out of all behavioral tracking, no matter what country the user is from, or what country the ad-network operates in.[229]

---

[225] *See, e.g.*, *WP29 Opinion on Online Behavioural Advertising*, *supra* note 36, at 11 ("[T]he visitor's browser . . . automatically transfers such information to the ad network provider . . . because the publisher . . . set[s] up its web site in such a way that the visitor to its own web site is automatically redirected to the ad network provider web site.").

[226] *Id.* at 13 ("[C]onsent must be revocable.").

[227] *See Call for Revision*, *supra* note 13, at 5, 10, 13, 15, 17.

[228] *See id.* at 10.

[229] *See id.*; *WP29 Opinion on Online Behavioural Advertising*, *supra* note 36, at 23.

[62] The proposal would not only benefit Internet users, but also ad-networks and other economic stakeholders, because the proposal would provide ad-networks and content providers with the certainty of whether they may engage in behavioral advertising with regard to a given user. Further, the proposal will enhance the free flow of information because resolving ambiguities over the definition of consent will "enhance legal certainty, reduce the administrative burden, and ensure a level playing field for economic operators."[230]

[63] Second, the Do-Not-Track proposal would provide a mechanism for a user to effectuate their informed and free consent.[231] Part III(B)iii, above, discusses in detail the sufficiency of a Do-Not-Track mechanism to provide informed and free consent under the law. A Do-Not-Track proposal would inform individuals of their rights and make them fully aware they are consenting. Third, the Do-Not-Track platform would increase transparency by providing objective information to the user before making a choice.[232] So long as the language used is "easy to understand . . . and plain language is used" the Do-Not-Track mechanism will satisfy the Commission's recommendations.[233]

[64] Fourth, the mechanism would strengthen individuals' rights in the face of new technologies because the Do-Not-Track platform would be technologically neutral. A Do-Not-Track mechanism is technologically neutral because it would avoid banning certain technologies over others. Instead, it would alert ad-networks *not* to track a specific user, no matter what technology was used. The Do-Not-Track mechanism would also strengthen a user's individual rights by alerting a user that an ad-network

---

[230] EDPS ON DATA PROTECTION REVISION, *supra* note 87, at 12.

[231] *See Call for Revision*, *supra* note 13, at 8-9.

[232] See *id.* at 6-7.

[233] *Id.* at 6.

had violated its privacy choices. The browser technology could automatically check for cookies placed without the permission of the user, and the technology could be updated as needed to recognize new technologies as they were invented.[234] These alerts could also help increase enforcement actions by documenting violations of the data protection rules.[235]

[65] Fifth, a Do-Not-Track mechanism would provide users increased control over their own data in a variety of ways. Not only could users specifically choose with whom they shared their information and how it should be used, the user could also choose to implement a strategy of data minimization. This strategy could allow the user to decrease their risk of identity theft through hacking or fraud, or simply provide a user with the feeling of autonomy that comes from the control of their own personal information.

C. Challenges to a Do-Not-Track List

[66] Critics commonly offer four main challenges to the implementation of a Do-Not-Track mechanism. First, critics assert that a Do-Not-Track mechanism would destroy the basic functionality of the Internet.[236] Second, that a mechanism placing users on a Do-Not-Track

[234] *See Call for Revision*, *supra* note 13, at 6 ("The Commission will consider how to ensure a coherent application of data protection rules, taking into account the impact of new technologies on individuals' rights and freedoms . . . .").

[235] *See id.* at 9.

[236] *See* Jack Marshall, *Feasibility of FTC 'Do-Not-Track' Option in Doubt*, CLICKZ.COM (Dec. 6, 2010), http://www.clickz.com/clickz/news/1930130/feasibility-ftc-track-option-doubt (statement of Pam Horan, president of Online Publishers Association) ("We're concerned about the concept of do-not-track if it specifically impacts the first party [publisher sites] . . . . Cookies are really critical to the operation of publishers' websites to do a variety of things.").

list would in-itself place users' privacy at risk.[237] Third, that by destroying a premium income stream, many websites will not be able to stay in business, or will be forced to bombard users with generic ads.[238] And fourth, that a Do-Not-Track mechanism is technologically infeasible.[239]

[67] The first argument is misguided in that it assumes a Do-Not-Track mechanism would simply block all cookies, thus removing functionality such as saved logins, favorite shipping addresses or customized page layouts.[240] However, as discussed above, the Do-Not-Track mechanism would simply alert ad-networks not to track a user; the mechanism would not block cookies on its own. Furthermore, the system would not ban or even discourage the use of first party cookies. Consequently, under the current proposal, the concerns of the first critique are moot.

---

[237] *See* Heather Osborn Ng, *Targeting Bad Behavior: Why Federal Regulators Must Treat Online Behavioral Marketing as Spyware*, 31 HASTINGS COMM. & ENT. L.J. 369, 386-87 (2009) ("[A] 'do not track' registry could cause more privacy problems than it fixes . . . . [A] 'do not track' program would allow the government to collect too much personally identifiable information from the public . . . .").

[238] *See* Catherine Holahan, *'Do Not Track' Could Backfire*, BLOOMBERG BUSINESSWEEK (Nov. 5, 2007, 12:01 AM), http://www.businessweek.com/technology/content/nov2007/tc2007114_372892.htm (discussing how the adoption of Do-Not-Track could lead to a barrage of extra advertising because of the lost value in showing behavioral ads); Edward Wyatt, *Legislators Support Internet Privacy, but Question How to Achieve It*, N.Y. TIMES, Dec. 2, 2010, at B3 (statement of Joan Gillman, executive vice president of Time Warner Cable) ("[D]o-not-track could hinder job creation within the advertising industry and by Web sites that rely on advertising revenues, [as well as] inhibit innovation and the development of new services.").

[239] *See* Christopher Wolf, *We Don't Need 'Do Not Track'*, BLOOMBERG BUSINESSWEEK (Nov. 12, 2007, 12:01 AM), http://www.businessweek.com/technology/content/nov2007/tc2007119_029422.htm ("Compiling and applying a list of those who do not want tailored advertising will be a technological nightmare.").

[240] *See* Marshall, *supra* note 236.

[68] The second argument, that a Do-Not-Track mechanism creates its own privacy risks,[241] does not apply to the specifics of this proposal. Unlike the FTC's Do-Not-Call list,[242] users' IP addresses or other identifying information would not be placed in a central list accessible to advertisers. Here, rather than creating a central list, the browser itself alerts companies not to track and target an anonymous user.[243] This alert need not contain any personal information beyond the fact the user does not wish to be tracked.

[69] The third and most widely voiced critique is that a Do-Not-Track mechanism will end the Internet as we know it by eliminating a major source of premium advertising revenue.[244] This critique is premised on the notion that behavioral ads sell for multiple times that of a generic advertisement.[245] Critics argue that the option to opt-out will limit the number of behavioral advertisements shown to users, and therefore fewer ads will command premium pricing on any given website.[246] There are some important flaws and caveats to this line of reasoning.

[70] Under current EU Law, including the Directives and the Treaty of Lisbon, users already have the ability to consent or refuse to consent to the

---

[241] *See* Ng, *supra* note 237, at 386.

[242] *Cf.* Rebecca Bolin, Note, *Opting Out of Spam: A Domain Level Do-Not-Spam Registry*, 24 YALE L. & POL'Y REV. 399, 429 (2006).

[243] *See* Kristen J. Mathews & Margaret Dale, *What Do You Really Need to Know About the FTC's Recent Report on Privacy?*, 19 METRO. CORP. COUNS. 33 (2011).

[244] *See, e.g.*, Holahan, *supra* note 238; Wyatt, *supra* note 238.

[245] *See* Angwin, *Gold Mine*, *supra* note 115 ("Targeted ads command a premium. Last year, the average cost of a targeted ad was $4.12 per thousand viewers, compared with $1.98 per thousand viewers for an untargeted ad, according to an ad-industry-sponsored study in March.").

[246] *See, e.g.*, Holahan, *supra* note 238; Wyatt, *supra* note 238.

use of their personal data in the behavioral advertising context.[247] In this sense, the Do-Not-Track mechanism only changes the ease with which users can express their already existent legal rights. More effective enforcement of existing laws and regulations should not be framed as a negative, even if there is an economic impact. Because a Do-Not-Track mechanism would simply increase the efficiency with which consumers can express their legal rights, ad-networks have no right to complain about potential economic losses. Importantly, many users will choose to ultimately allow behavioral advertising.[248] In the most recent European study, almost 65% of respondents stated opinions either neutral to or in favor of targeted ads.[249] A majority of the premium income stream should remain viable after the implementation of a Do-Not-Track mechanism.[250] Finally, online advertising only accounts for 10% of total advertising expenditures, and this has only been the case for the past few years.[251] Websites provided free content supported by advertising revenue before behavioral advertising became a widespread phenomenon.

D. Alternative Solutions

i. Self-Regulation

[71] The advertising industry has had fifteen years since the adoption of the Data Protection Directive in which to institute meaningful self-regulation.[252] By all accounts, they have failed.[253] The recent and widely

[247] *See* EDPS ON DATA PROTECTION REVISION, *supra* note 87, at 12. *See generally* Treaty of Lisbon Declarations 20, 21; Data Protection Directive, *supra* note 10, Preamble, para. 9; e-Privacy Directive, *supra* note 26.

[248] *See* OFFICE OF FAIR TRADING, *supra* note 121, at 7.

[249] *Id.*

[250] *Cf.* Wyatt, *supra* note 238.

[251] *See* IAB, *supra* note 94, at 10.

[252] *See Call for Revision*, *supra* note 13, at 2.

publicized initiative by the Internet Advertising Bureau UK must be viewed with a certain amount of skepticism.[254] Rather than viewing this latest attempt as the industry finally deciding to address the privacy concerns created by behavioral advertising, it represents the industry's last-ditch attempt to avoid stricter regulation.

[72] As discussed above in Part II(G), self-regulation fails at providing the rights and protections guaranteed by the data protection framework and Treaty of Lisbon for three key reasons.[255] First, ad-networks have no economic incentive to succeed at self-regulation beyond the level necessary to delay or prevent actual regulation.[256] Second, self-regulation programs generally lack meaningful enforcement mechanisms.[257] Third, self-regulation initiatives are voluntary and result in scattered systems that fail to present a single and easily usable consent mechanism for the consumer.[258] Historical analogs also suggest that self-regulatory efforts are doomed to be insufficient, while eventual governmental regulations, such as the Do-Not-Call list in the U.S., have found vast success.[259]

---

[253] *See* EPIC, *supra* note 173, at 9; Foster, *supra* note 173, at 281; Hirsch, *supra* note 132, at 460.

[254] *See IAB Good Practice Principles*, *supra* note 171.

[255] *See* Hirsch, *supra* note 132, at 458-59.

[256] *See id.* at 458.

[257] *See id.*

[258] *See id.* at 458-59.

[259] *See* EPIC, *supra* note 173, at 2; Anderson, *supra* note 178 ("Today, 200 million numbers are on the US Do Not Call list, and the government has generally forbidden all telemarketing calls. Taken together, these two rules fundamentally changed the telemarketing business.").

ii. Suggestions of the Article 29 Working Party

[73] The Article 29 Working Party's primary recommendation, that a user give their informed consent upon the placement of any third-party cookie is impractical.[260] A user would have to decide to accept or reject every third-party cookie an ad-network attempted to place on their computer, a task, which could easily tally in the thousands during everyday browsing.[261] Many of the Internet's most visited websites install over one hundred third-party cookies during a single visit.[262] To require a user to make an individual decision regarding each cookie is impossible without destroying the usability of the Internet.[263] Even if this solution has the advantage of allowing users to exactingly distinguish between an ad-network with moderate tracking practices and those with extreme or experimental practices, it is impractical to design a system that requires such repeated consent from the user.

[74] To combat this flaw, the Working Party suggests that consent to a third-party cookie should last for a full year.[264] This does not solve the problem, however, because each visit to a *new* website would still be painful or impossible for the user.[265] Finally, even if a user was forced to go through a yes/no decision based on unique information for each ad-network, the challenges of "consent fatigue" and general apathy will

[260] *See WP29 Opinion on Online Behavioural Advertising*, *supra* note 36, at 16.

[261] *Cf. What They Know*, *supra* note 115 (illustrating the number of tracking files installed on computers by popular websites).

[262] *Cf. id.*

[263] *See, e.g.*, *WP29 Opinion on Online Behavioural Advertising*, *supra* note 36, at 3.

[264] *See id.* at 16.

[265] *See* Jeff Atwood, *Your Session has Timed Out*, CODING HORROR (Apr. 15, 2008), www.codinghorror.com/blog/2008/04/your-session-has-timed-out.html (explaining the creation of cookies for individual browser requests).

render the choices meaningless, thus destroying the possibility of meaningful consent that the mechanism should provide.[266]

IV. CONCLUSION

[75] This Article argues for a wide reaching and comprehensive proposal, yet some additional steps remain. First, the browser technology will need to be perfected. Currently Firefox and Internet Explorer are developing technologies that could provide the basis for a Do-Not-Track mechanism.[267] Under this proposal, the Do-Not-Track technology would need to be uniform across browsers and be technologically capable of functioning in the manner outlined by this Article.[268] This process will take both time and money, and the question remains of who should pay for this development.[269]

[76] Second, Member States, DPA's, the Article 29 Working Party, the European Data Protection Supervisor, or some combination thereof, would need to conduct a public awareness campaign before implementing the Do-Not-Track platform.[270] Alerting users of their privacy choices and explaining them beforehand would minimize the risk of users simply clicking through the consent wizard upon installation.[271] It is important to

[266] *See* Brownsword, *supra* note 161, at 90 (warning against the "routinisation" of consent).

[267] *See* Metz, *supra* note 168.

[268] *Id.*

[269] *See* Stephen Shankland, *Mozilla Offers Do-Not-Track Tool to Thwart Ads*, CNET NEWS (Jan. 24, 2011, 1:03 AM PST), news.cnet.com/8301-30685_3-20029284-264.html.

[270] Press Release, Fed. Trade Comm'n, FTC Testifies on Consumer Privacy and Protection in the Mobile Marketplace (May 19, 2011), *available at* www.ftc.gov/opa/2011/05/mobiletestimony.shtm (mentioning the protection of consumer privacy rights through "consumer and business education campaigns").

[271] *See WP29 Opinion on Online Behavioural Advertising*, *supra* note 36, at 13.

alert consumers to the benefits of targeted advertising, including increased relevancy of advertisements and coupons, so that consumers can make objective choices.[272]

[272] *See* Metz, *supra* note 168.