EU Data Protection Law and Targeted Advertising

Consent and the Cookie Monster - Tracking the crumbs of online user behaviour

by **Damian Clifford**, Researcher ICRI/CIR KU Leuven*

Abstract: This article provides a holistic legal analysis of the use of cookies in Online Behavioural Advertising. The current EU legislative framework is outlined in detail, and the legal obligations are examined. Consent and the debates surrounding its implementation form a large portion of the analysis. The article outlines the current difficulties associated with the reliance on this requirement as a condition for the placing and accessing of cookies. Alternatives to this approach are explored, and the implementation of solutions based on the application of the Privacy by Design and Privacy by Default concepts are presented. This discussion involves an analysis of the use of code and, therefore, product architecture to ensure adequate protections.

Keywords: Data Protection, Targeted Advertising, E-Privacy Directive, Consent, EU Data Protection Framework

Recommended citation: Damian Clifford, EU Data Protection Law and Targeted Advertising: Consent and the Cookie Monster - Tracking the crumbs of online user behaviour 5 (2014) JIPITEC 194, para 1.

A. Introduction

1 The commercialisation of the internet has been rapid. Ubiquitous technological development and internet availability have propelled profits and the value of information. Online Behavioural Advertising (OBA) through the tracking of users has allowed for the development of user-targeted campaigns. The debates surrounding the legitimacy of this behaviour have been contentious. Traditional legal principles have struggled to come to terms with the rapid proliferation of internet technologies. The rigidity of the legal framework contrasts strongly with the fluid and ever-changing IT sector. In essence, tracking and the resulting profiling have become a key part of the business model of many Web 2.0 services, but the legality of this behaviour is still unclear.[1]

2 The aim of this analysis is to examine the use of cookies in the tracking of users for the purposes of targeted advertising. Certain restrictions regarding the scope of this article should be acknowledged from the outset. First, it will be restricted to an examination of the use of cookies in OBA in order to track and profile users. Accordingly, an examination of the emerging use of technologies and techniques such as Browser Fingerprinting, Deep Packet Inspection and History Sniffing does not come within the scope of this article. Further, the article will not explore the legal issues around the use of analytics systems which correlate various data sources (including the cookie data) and, hence, the Big Data elements of this topic. Although, in reality, user profiles in OBA contain data from various sources in addition to cookies, this does not mitigate

the fact that the tracking and processing of cookie data constitutes profiling in itself. The text will also not outline the additional considerations necessary for a holistic interpretation of the use of tracking technologies on mobile devices. Finally, during the assessment of the consent issue, the article will focus on the general issues and concerns rather than the particular debates specific to children (or others who potentially lack capacity to consent). These are issues which merit further analysis in themselves, and to examine them here would not do justice to the complex legal issues present. Nevertheless, at times references to these matters and the further obligations will be made.

3 Having narrowed the scope, it is now worth outlining the focus of the research. The Article 29 Working Party has noted that most advertising technologies use some type of client side processing of users' browsers or terminal equipment to track their activity.[2] This processing refers to the accessing and use of information stored on users' computers. In behavioural advertising, companies use software to track user behaviour and to build personal profiles. They do not refer to users by name but, instead, use a single alphanumerical code that is placed on the users' computers. These codes are utilised to help select the advertisements people see in addition to the variety of products that are offered to them.[3] These are known as 'cookies,' and they can provide a detailed profile based on user behaviour, which can be easily exploited for marketing purposes.

4 Cookies placed on users' machines by the publisher (website operator) are known as first-party cookies and these, 'are commonly used to store information, e.g., user preferences, such as a login name.'[4] These 'functional cookies' are generally exempt from the legal obligations under the Data Protection framework unless they are also used for tracking or profiling purposes.[5] However, there are also what are known as third-party cookies. These cookies originate from sources that may be unconnected with the first-party cookie website (e.g. an ad network) and are often used as a tracking mechanism for advertising purposes.[6] In the world of AdExchanges, such as Google's AdX, this issue is complicated further given the complex array of players.[7] More importantly, reference to the term 'cookie' in this text comprises of all variations, including the more controversial 'flash' cookies (also referred to as Locally Shared Objects). Although this form of cookie has serious technical advantages over the standard HTTP cookies (and has raised issues regarding 'respawning'), they are both placed and accessed on the terminal equipment of users and are fundamentally subject to the same legal requirements.[8]

5 The article will analyse the applicable legal framework, the legal requirements imposed by this framework, the difficulties surrounding the definition of consent, and the alternatives and supplements to the current EU Data Protection edifice. Reference will be made to the current EU Data Protection framework in the form of the Data Protection Directive and the E-Privacy Directive (as amended). Specific attention will also be given to the Data Protection reform package and, more specifically, the proposed Data Protection Regulation.

B. The scope of the EU Data Protection Framework - Behavioural Advertising

6 Data Protection is a distinctively European innovation that has been received outside the EU with varying degrees of success.[9] The current framework owes its origins to developments, such as the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, the 1981 Council of Europe Convention on data protection, and the 1990 UN guidelines.[10] The adoption of such provisions is hardly surprising given the historical context in which the European supranational cooperation originated.[11] However, there are two other factors which have proven decisive. First, the ubiquitous development of technology and the supranational challenges that this involves.Second, the need to facilitate the free movement of personal data within the Community and to resolve conflicts arising from differing national regimes.[12] Although there have been clear technological advances which have precipitated legal development, the core of the EU framework has remained constant and the essence of the data protection edifice has remained straightforward.[13] This section of the analysis will introduce the key instruments and examine their scope in relation to OBA.

I. Data Protection as a Primary Source

7 Data protection is a complex issue that has traditionally been associated with the concept of privacy within the context of personal data processing. However, as observed by Borghi *et al.*:

> 'at least under EU law, privacy and data protection are distinct, yet complementary, fundamental legal rights. They derive their normative force from values that—although at times coincidental and interacting in a variety of ways—may be conceptualized independently.'[14]

8 This position has allowed data protection to automatically trump other interests and gives it a status that cannot be traded-off for economic benefits.[15] The identification of data protection as a key personal right of the citizens of the Union was confirmed through the adoption of the Lisbon Treaty. Article 39 TEU and Article 16 TFEU provide specific provisions relating to data protection. Article 16, in

particular, promotes the data protection provision to a 'provision of general application' under Title II, alongside other EU fundamental principles, and also imposes an obligation on the legislator to establish a clear and unequivocal legal framework for data protection.[16] In addition, the Lisbon Treaty also formally recognised the binding legal status of the Charter of Fundamental Rights of the European Union and provided specific provisions relating to the legal significance of the European Convention of Human Rights (ECHR). Article 8 of the Charter (the right to Data Protection) and Article 8 of the ECHR (the right to private life) are of clear importance in this regard.[17]

II. Introducing the Secondary Sources

9 There are two specific pieces of EU legislation which perform a key role in the data processing monitoring regime of the Union: first, Directive 95/46/EC (the Data Protection Directive), and second, Directive 2002/58/EC (the e-Privacy Directive including the reforms implemented by Directive 2009/136/EC). Essentially, the e-Privacy Directive provides a 'sector-specific regime'[18] which operates as the *lex specialis* vis-a-vis the *lex generalis* requirements provided for by the Data Protection Directive.[19] In addition, the proposed reform of Data Protection Directive (*via* the General Data Protection Regulation[20]) provides key points of analysis. The proposed Regulation signifies the first attempt at revising the data protection rules since the Directive went into effect. As Rooney notes, changes are needed, as the Data Protection Directive is outdated and ill-equipped to deal with modern technology.[21] Each of these sources will now be analysed.

1. The Data Protection Directive

10 The Data Protection Directive requires MSs to adopt legislation regulating the processing and movement of personal data.[22] As noted by van der Sloot *et al.*, it is clear from Article 2(d) that '[t]he applicability of the Directive is triggered when "personal data" are "processed" under the authority of the "controller" of the personal data.'[23] Under the terms of this Directive, data subjects are guaranteed certain rights *vis-a-vis* their personal data, while data controllers are subject to strict rules and regulations in relation to their data processing activities.[24] This section will analyse three particular questions that will help determine the applicability of the Directive. First, does the data used in OBA fall into the classification of personal data? Second, does the subsequent use of this data for the purposes of OBA result in 'processing' under the terms of the Directive? And finally, in the context of OBA, who is the data controller?

a.) Does the data used in OBA fall into the classification of personal data?

11 According to Article 2(a):

> '"personal data" shall mean 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'.

12 In order to assess whether a particular person is identifiable, all methods likely and reasonable should be taken into consideration.[25]

13 The Directive further distinguishes between sensitive and non-sensitive data, with the former incurring a stricter regime. These 'special categories of data' require explicit consent from the data subject in order to be processed. This distinction between common and 'special categories' (sensitive) personal data is retained in the proposed Regulation and this raises clear concerns. The choice of distinguishing the categories of data and the further listing of the categories of sensitive personal data is restrictive, as it does not allow the flexibility needed to cope with technological development. In the age of big data, analysis-intensive processing methods have blurred the lines between these data categories.[26] The designation of cookies into a particular classification of data type is of clear importance. In order to understand the impact of the Directive on behavioural advertising, one must first consider how cookies should be classified.[27] Businesses involved in behavioural targeting often maintain that privacy legislation does not apply, as specific persons cannot be traced. This is based on the assumption that users remain anonymous, as they are only identifiable through the issued tracking cookie. However, in legal terms this notion is not completely accurate.[28]

14 The Article 29 Working Party opinion on behavioural advertising observes that targeted marketing clearly falls within the scope of the Directive for two particular reasons. First, the use of cookies normally involves the processing of unique identifiers and the collection of the IP addresses, which allows the tracking of particular machines (even when dynamic IP addresses are used). Second, the information that is collected relates to the users' characteristics, and this is used to influence their behaviour. This view is further established if one considers the capacity for profiles to be linked with directly identifiable information given by the data subjects (for example registration details). The Article 29 Working Party observes that 'mergers, data losses and the increasing availability on the Internet of personal data, in combination with IP addresses,' are other scenarios that can lead to identification.[29]

15 There is still strong debate as to whether IP addresses should be classified as personal data.[30] At a fundamental level, this is reflected in Court

decisions. In *EMI & Ors v Eircom Ltd [2010]*,[31] Charleton J in the Irish High Court concluded that IP addresses do not amount to personal data under the terms of the Data Protection Directive. In contrast, one year after Charleton J's judgement, the CJEU in *Scarlet v Sabam* found that IP addresses are classified as personal data, as they allow users to be directly identified.[32] The Article 29 Working Party have clearly stated on a number of occasions that IP addresses constitute personal data under the terms of the Directive, as they can be traced to a natural person with the cooperation of the internet provider.[33] With increasingly powerful processing mechanisms, the identity of users can frequently be ascertained through the analysing of large quantities of data linked to IP addresses and other seemingly anonymous data.[34] A particularly obvious example where such information may be retrieved is found in relation to so-called vanity searches.[35] However, it must be acknowledged that there are exceptions to this and not all IP addresses can be effectively linked to a user (for example, computers that are used by multiple users). The Court of Justice may have been handed the opportunity to finally clarify the law in this regard with the recent referral of question by the German Court on the legal classification of IP addresses as personal data.[36] This case should be watch carefully, as it should provide detailed guidance on this issue.

16 The Article 29 Working Party is also of the opinion that cookies, in themselves, (even when IP addresses are not siphoned) still constitute personal data. In its assessment of the concept of personal data, the Working Party found that names are not always a necessary means of identifying individuals, as there are alternative methods of distinguishing an individual from other members of a group.[37] As such, 'unlike in the case of IP addresses, the Working Party does not consider the ability to access a name as a criterion for qualifying a cookie as personal data.'[38] Instead, the mere accessing of the user's machine suffices. Under the terms of the draft Regulation the definition of personal data has been altered to include 'online identifiers' in the list of examples that may be used to identify an individual.[39] It appears that in the proposed legislative update cookies will be specifically included as personal data under the terms of the Regulation. Even in the much more liberal landscape provided for in the US, the FTC found in a consultation document on the self-regulation of behavioural advertising a tendency to classify IP addresses and cookies that are used for behavioural targeting the same as 'regular' directly identifying personal data.[40] Hence, the applicability of the Data Protection Directive should be assumed as relevant when applied to OBA. Moreover, the use of cookies for tracking purposes results in the creation of a personal data user profile.

b.) Does the subsequent use of this data for the purposes of OBA result in 'processing' under the terms of the Directive?

17 Article 2(b) states that:

> 'For the purposes of this Directive... "processing of personal data" ("processing") shall mean any operation or set of operations which is performed upon personal data... '

18 This provides an extremely broad definition of processing, which includes almost everything that can be done with personal data. It is, therefore, unlikely that the manipulation of data for the purposes of behavioural advertising would not come under the provisions of the Data Protection Directive.

c.) In the context of OBA who is the data controller?

19 Article 2(d) defines the concept of data controller. It states that:

> '"controller" shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data...'

20 This provides a clear and precise separation in responsibility. As observed by De Hert and Papakonstantinou, the traditional approach to data processing is for the most part maintained in the draft regulation.[41] This consists of data controllers processing personal information of data subjects either through their own means or by contracting a third-party data processor. This should be considered a failure of the proposals, as the continued insistence on the outdated distinction between data controllers and data processors does not reflect some of the complex actors involved in modern data processing. Instead of modifying the data controller and data processor definitions in the draft Regulation, the Commission 'chose to strengthen controlling instances by placing certain additional obligations upon data processors, as well, and acknowledge the existence of "joint controllers".'[42]

21 The addition of these further obligations strengthens the protection of the data subjects. Despite this improvement, the decision to maintain the traditional approach to data processing, where the roles are easily distinguishable and the data processors hold only passive functionality, does not reflect the technological realities. In the web 2.0 era, such a distinction must be viewed as being outdated. With this in mind, 'perhaps the preferable way forward would be for the Commission to boldly abolish the notion of "data processors" from its Regulation, altogether, and vest the data controller title, rights, and obligations upon anyone processing personal information, regardless of its means, conditions, or purposes.'[43]

22 To make matters more complicated, distinguishing between the various actors involved in OBA is not as simple as it may seem at first glance. It appears relatively obvious that Ad Networks, who collect and process the information and place and design the cookies used to retrieve the information, are classified as data controllers. However, the role of the publisher is much more complicated. Due to the way in which websites are engineered,[44] it is the data subject's browser that automatically transmits the IP addresses to the ad network provider in order to facilitate the sending/reading of the cookies and to present the tailored advertising. It is important to note that, although the data transfer is caused by the browser, it is the publisher's implementation of the website that triggers the transfer, and the data subject has no input. Thus, the Article 29 Working Party finds that publishers have certain responsibilities under the Data Protection Directive. However:

> 'This responsibility does not cover all the processing activities necessary to serve behavioural advertising, for example, the processing carried out by the ad network provider consisting of building profiles which are then used to serve tailored advertising.'[45]

23 Instead, their responsibility is restricted to the preliminary data processing activities and the initial transfer of the IP addresses. The Working Party came to this conclusion as 'the publishers facilitate such transfer and co-determine the purposes for which it is carried out, i.e. to serve visitors with tailored advertising.'[46] In addition to the division of responsibility between the publisher and the ad network, one must also consider the influence of the advertiser. Following an ad click, the users' actions may be tracked for conversion statistics and potential retargeting. Although this may not be strictly linked to the initial ad serving, this information can also be shared (in fact, this is often a requirement under the Terms of service) with the ad networks, and used to improve on future targeted campaigns. This certainly raises the notion of 'co-controllers'.

2. The E-Privacy Directive and 'Cookies'

24 According to Recital 10 of the E-Privacy Directive, the Data Protection Directive applies 'to all matters concerning protection of fundamental rights and freedoms which are not specifically covered by the provisions of this Directive, including the obligations on the controller and the rights of individuals.' In an analysis of the interplay between both of these Directives in a behavioural advertising context, the Article 29 Working Party observed that the Data Protection Directive has full applicability, with the exception of the provisions that are specifically addressed in the E-Privacy Directive. This mainly corresponds to the legal grounds for data processing found in Article 7 of the Data Protection Directive. The remaining requirements under the Data Protection Directive (including the principles regarding data quality, the data subject's rights, confidentiality and security of the processing and international data transfers) have full applicability.[47] The E-Privacy Directive provides the specific rules relating to the processing of personal data and privacy protection, in relation to the electronic communications sector.[48] Of particular importance is Article 5(3), which applies when a provider is accessing or storing information on a user's computer remotely.

25 As amended, this provision now states that:

> 'Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user has given his or her consent, having been provided with clear and comprehensive information in accordance with Directive 95/46/EC, inter alia about the purposes of the processing.'

26 The Article 29 Working Party has observed that this article has full applicability to tracking cookies as they can be classified as 'information' stored on the terminal equipment of the user which are accessed by the ad networks. Accordingly, the placing and any subsequent use of such cookies (or similar technologies irrespective of type) will require compliance with Article 5(3).[49]

3. Privacy Framework overlap and the Proposed Amendments

27 In contrast to the Data Protection Directive, Article 5(3) of the E-Privacy Directive does not relate specifically to 'personal data' but, instead, refers more generally to 'information'. In order to invoke the applicability of the Directive, it is not a prerequisite that the information is classified as personal under the terms of the Data Protection Directive.[50] This is expressed in Recital 24 which provides that the 'terminal equipment of users... and any information stored on such equipment are part of the private sphere of these users requiring protection under the European Convention for the Protection of Human Rights and Fundamental Freedoms'. Hence, information that is considered to be in the 'private sphere of the users' triggers the application of Article 5(3) and not if the data is classified as personal. The applicability of the Data Protection Directive is not affected by the E-Privacy Directive. In essence, one is required to make a clear distinction between the placing of the cookie and the actual use of the data recorded by this mechanism.[51] However, from the discussion *supra* it is clear that in all probability the cookies do fall into the category of personal data. Thus, in relation to behavioural advertising, both Directives appear to have relevance.

28 Article 20 of the proposed Regulation introduces a provision which deals directly with user profiling. The addition of a provision on profiling would be a significant step, as it would remove the ambiguity

surrounding the applicability of the data protection edifice. This also recognises the development of technology that is not reliant on the accessing of the terminal equipment of the user. This addition is also aided through the proposed strengthening of the data minimisation principles under Article 5. Indeed, '[t]he strengthening of this principle is necessary in order to address the current trends of data harvesting and data mining used for profiling consumers and which involve large amounts of personal data being collected.'[52]

29 Having examined the scope of the EU Data Protection Framework, it is now necessary to analyse the legal requirements it imposes upon behavioural advertising. These categories will be assessed in detail in the proceeding part of the analysis.

C. The legal requirements imposed by the EU Data Protection Framework

30 The applicability of both Directives to OBA, essentially, opens up three important categories of legal requirements. First, those relating to information dissemination to the users; second, those relating to consent; and finally, the further obligations laid down in the Data Protection Directive.[53] These requirements involve a high degree of overlap between the E-Privacy provisions and the *lex generis* requirements imposed by the Data Protection Directive. It is important to note that the Data Protection Directive has both general applicability to issues not covered by the E-Privacy Directive and specific impact when referred to by the terms of the E-Privacy provisions. The various requirements and their specific application will now be assessed in detail.

I. Interpreting Article 5(3) - legal obligations for Online Behavioural Advertising

31 In the opinion of the Article 29 Working Party, it is clear from a literal interpretation of Article 5(3) that prior consent is required before the information can be placed or processed. For the consent to be informed, prior information regarding the purposes of the cookie must have been given to the user.[54] It is clear that these requirements are cumulative in nature.[55] The key point of contention in relation to behavioural advertising is what constitutes unambiguous consent. However, perhaps it is prudent to, first, briefly analyse what amounts to adequate dissemination, in order to satisfy the 'informed' element of the consent requirement.

1. Information Dissemination

a.) Type of Information Required

32 Article 5(3) of the E-Privacy Directive declares that users must be provided with information 'in accordance with Directive 95/46/EC, inter alia about the purposes of the processing'. As such, one is required to refer to Article 10 of the Data Protection Directive. In relation to OBA, the users should be clearly informed about the purposes of the cookies and, hence, that they will allow the tracking of the users' visits to other websites, the advertisements they have been shown and which ones they have clicked.[56] Significantly, under the terms of the proposed changes in the draft Regulation, Article 14 provides a list of information that must be provided to the data subjects. In addition to the information required in the current Directive, the proposed Regulation specifies the period for which the data will be stored, the right to object to the processing, and the right to lodge a complaint with the supervisory body and the contact details of that body.[57] Interestingly, the new provision specifically dealing with profiling (Article 20) is not mentioned in Article 14. The BEUC (European Consumer Agency Organisation) in its assessment of the article observed that 'this provision should echo the inclusion of a specific article dealing with profiling (Article 20) by requiring information about tracking and profiling purposes, and its consequences on individuals to be added under Article 14.1 b.'[58] However, Article 20 does provide that information dissemination is required. More specifically, in addition to the requirements laid down in Article 14, this should include 'information as to the existence of processing' for the purposes of profiling and also the 'envisaged effects of such processing on the data subjects.' These changes reflect the overall move towards the principle of transparency as provided for in Article 5 of the proposed amendments.

b.) How should the information be presented?

33 It is important that the information is presented in a user-friendly manner so as not to negate its influence. This reflects the concern that the information should be easily accessible and understandable and 'should not be "hidden" in a link at the bottom of a page referring to a vague and unreadable privacy policy.'[59] Accordingly, there should be a simple explanation of the uses of the information gathered by the cookie analysis. Recital 25 of the E-Privacy Directive stipulates that notices should be displayed in a 'clear and comprehensive' manner. The Article 29 Working Party suggests that 'Statements such as "advertisers and other third parties may also

use their own cookies or action tags" are clearly not sufficient.'[60] Recital 66 goes on to state that the method for refusing cookies should be 'as user-friendly as possible'. The Directive does not provide specifics as to how this may be achieved and this is reflected in the varying implementations of cookie notices. In keeping with the general move towards more transparent data processing, Article 11 of the draft regulation contains a specific provision in relation to the communication of information. This movement towards transparency and the provision of clear communication is also aided through recital 32 of the proposal, which states that privacy policies are required to be as clear and transparent as possible and should not contain 'hidden or disadvantageous clauses'.[61] The proposed developments *vis-a-vis* the information requirements are clearly designed to strengthen the position of the data subject. This is further fortified in the draft amendments to the concept of consent.

2. Unambiguous Consent

34 Consent is a complex issue that raises clear difficulties in relation to the EU data protection framework.[62] The preliminary obligatory requirement for consent effectively renders the other legitimate interests for data processing, as provided for under Article 7 of the Data Protection Directive, inapplicable. Accordingly, consent is a prerequisite for the legitimate placing of cookies and processing of cookie data. Nevertheless, it is important to note that with the potential development of tracking methods not linked to users' terminal equipment, the other justifications for legitimate data processing may have future applicability. However, as mentioned *supra,* the draft Regulation seems to predict such a progression by providing for a specific tracking provision. Given the current dependency on the accessing of the terminal equipment of the users in order to effectively track online behaviour, the requirements provided for under Article 5(3) of the e-Privacy Directive moderate the relevancy of the Data Protection Directive. As such, cookie-based behavioural advertising is restricted by the interpretation and implementation of the concept of consent under the Data Protection Directive despite the availability of other grounds for legitimate data processing in circumstances not involving cookies or other forms of client side processing. The interpretation of this concept is the key debate in the analysis of Online Behavioural Advertising and the use of cookies. Given its importance, the difficulties surrounding the interpretation of consent will be analysed in Section D of this paper in detail.

II. Further Requirements and the Data Protection Directive

35 As previously discussed, there is a clear distinction between the personal and sensitive categories of data under the current data protection framework which is maintained in the draft regulation. Under the current provisions, the processing of these special categories of data requires explicit consent, which contrasts with the requirements for ordinary personal data. Given the applicability of Article 5(3) of the E-Privacy Directive, it appears from the discussion *supra* that opt-in consent will be required for the placing/accessing of cookies irrespective of whether the processed information is non-personal, personal or sensitive. Therefore, it seems that the additional requirements envisaged by the proposed Regulation will have already been satisfied by the consent requirement under Article 5(3). However, given the applicability of the Data Protection Directive, there are additional obligations which must be considered. The requirements that are particularly relevant to behavioural advertising will now be analysed.

1. Data Quality

36 There are several fair information principles which need to be complied with in order to satisfy the obligations under the Data Protection Directive. The key requirement of the Directive is the vague obligation that personal data must be processed 'fairly and lawfully'. Article 6 of the 1995 Directive outlines various conditions that must be satisfied by the data controller in relation to data quality. It is clear from the Article that processing can only take place for legitimate purposes. In its opinion on Search Engines, the Article 29 Working Party has stated that 'some purposes, such as "improvement of the service" or "the offering of personalised advertising" are too broadly defined to offer an appropriate framework to judge the legitimacy of the purpose.'[63] The Working Party observed that this was particularly true when the controller also mentions additional purposes for the data.[64]

37 In relation to behavioural advertising, it must be understood that the Working Party's reference to 'personalised advertising' reflects more the data controllers' explanation of the purposes to the data subjects rather than the specificity of the activity in itself. This is also indicative of the purpose limitation principle which in Article 6(1)(b) 'prohibits the processing of personal data which is not compatible with the purposes that legitimised the initial collection.'[65] This prevents the re-use of information for purposes other than those originally specified to the data subject. In order for the repurposing of the collected personal data to take place, one is

required to satisfy one of the legitimate grounds for processing under Article 7.

38 Article 6 further stipulates that data should be accurate and updated if necessary. All reasonable steps must be taken to ensure that inaccurate and/or incomplete data are erased or modified while remaining conscious of the purposes for which they are being processed. This presents a clear problem in relation to OBA in that, although analytics systems can ignore particular false positives, certain inaccuracies are unavoidable. Furthermore, Article 6(1)(e) outlines the retention principle, which requires the deletion of data where it is no longer necessary for the purposes it was gathered. This is an indication of the data minimisation principle which, although not expressly provided for, is implied by certain requirements in the Directive.[66] The principle provides that only the minimum amount of data required to adequately perform the processing should be gathered. This principle has been recognised by the Court of Justice which has found that the Directive 'must necessarily be interpreted in the light of fundamental rights, which, according to settled case-law, form an integral part of the general principles of law whose observance the Court ensures.'[67] This reflects the overall balancing of data protection with other fundamental rights, both under the terms of the Charter and the ECHR, and, hence, the importance of the principle of proportionality in this regard.

39 There have been a number of key developments in this regard in the draft regulation. These developments are understood to be necessary to address the issues associated with the current trends in data mining where large data sets are being analysed in the profiling of data subjects.[68] The draft Regulation in Article 6(f) prohibits processing in the interest of controllers where the fundamental rights of data subjects require data protection. Furthermore, as part of the draft proposals, Article 5 has clarified the principles relating to data processing by expressly providing for the principles of transparency, data minimisation and controller liability, which are currently only been implicitly referred to (see discussion *supra*).[69] Although these principles have been around for 25 years, it is only now that they have been confirmed in the draft legislative text.[70]

2. Data Subjects' Rights

40 Data subjects have the rights of access, rectification, erasure and to object as enunciated under Article 12 and 14 of the Data Protection Directive; and, these rights should be respected by the data controller. In relation to OBA, this affords the data subject the right to access the information gathered by the ad network (i.e. their profile), to demand the modification or deletion of this profile, and to object to any further profiling. Certain Ad Networks provide these services and allow the data subject to modify and erase interest categories.[71] Under the terms of the draft Regulation, the concepts of rectification and erasure are elevated in importance. These concepts are placed in a new section (Section 3), which provides for the right to rectification in Article 16 (elements of Article 12(b) in the current Directive), right to be forgotten and the right to erasure in Article 17 (elements of Article 12(b) in current Directive) and the right to data portability in Article 18. As noted by Savin, the latter of these 'which is a new right, consists of the right to obtain a copy of the data from the controller for the further use by the data subject.'[72]

3. Additional Obligations

41 It should be further noted that the obligations related to confidentiality and security of the processing are also relevant. Article 17 states that 'Member States shall provide that the controller must implement appropriate technical and organisational measures to protect personal data....' As observed by the Working Party, to comply with this provision ad network providers are required 'to implement state of the art technical and organisational measures to ensure the security and confidentiality of the information.'[73] Under Article 30(3) of the proposed Regulation, the security of personal data appears to have been elevated along with the concepts of privacy by default and design. As noted by Hildebrandt and Tielemans:

> 'By enacting these types of duties as legal obligations the EU legislator inaugurates examples of what has been coined as legal protection by design (LPbD), confronting us with a new articulation of legal norms: next to unwritten and written law, we now have something like digital law.'[74]

42 Article 18 is also applicable and requires data controllers to notify the data protection authorities of their data processing activities (unless they are exempt). Article 28 of the draft proposals replaces the cumbersome notification requirement with the obligation to maintain documentation of any processing activity. Under Article 28(2) the relevant pieces of documentation that controllers need to record are noted. The minimum requirements stipulate that the contact details for the controller and the data protection officers, the types of personal data being processed, the recipients (or categories of recipients) of the personal data, the purposes of the data processing, possible transfers to third countries and the relevant retention periods need to be maintained. As noted by the BEUC report this will 'make the checking by Data Protection Authorities easier and help improve monitoring of compliance and enforcement.'[75]

43 Finally, in relation to international data transfers, Articles 25 and 26 are also relevant. Article 25 provides that the Commission may ban data transfer to countries that fail to provide 'an adequate level of protection' of data privacy rights. Article 26 lists a number of derogations and provides that a transfer to a country that 'does not ensure an adequate level of protection' may occur if the controller enters a contractual arrangement that guarantees adequate safeguards for the protection of the fundamental rights and freedoms of the data subject.[76] In the context of OBA, international data transfers have particular importance given the transferability of the gathered information. Without robust protections, profiling practices prohibited by EU law could still be performed on EU users if their information was transferred to a third country for data processing. The draft regulation recognises the growing importance of international data transfers and reflects this new reality by abandoning the presumption that personal data cannot be transferred without an adequate level of protection. Instead, the Commission has opted to outline a number of requirements which must be satisfied before any such a transfer can occur.[77] These modifications are provided in Articles 40-45 and include examples of the criteria that the commission would use in their assessment of the adequacy of the level of protection provided by the third country. This is a very topical area, especially given the recent challenge to the legitimacy of such transfers to the US.[78]

D. Difficulties defining consent

44 Following our discussion of the three categories of legal requirements, it is clear that prior informed consent provides the crux of the debate regarding the effective regulation and advancement of responses to the use of cookies as tracking technologies in behavioural advertising. The additional requirements imposed by the Data Protection Directive are predicated on this preliminary consideration. However, the failure to find consensus on a common definition of consent renders the existing framework divisive and ambiguous.

I. Consent in its current form

45 Article 8 of the Charter specifically recognises consent as the key condition for the protection of personal data. Behavioural advertising has based itself on the ability to place cookies on users' terminal equipment. If users were unhappy with this, they were required to opt-out (provided they knew how).[79] Under the amended Article 5(3), it is clear that informed prior consent is required before any such technology is used or even installed.[80] Azim-Khan and Millard have observed that '[t]he requirement for explicit prior consent seems to have spelt the end of the "opt-out" regime....'[81] The change implemented by Directive 2009/136 provides a clear departure by legislating for an 'opt-in' requirement by default[82]and was a 'bold step'.[83] However, there is still strong criticism of this position from certain sectors.[84] Article 2(f) provides that '"consent" by a user or subscriber corresponds to the data subject's consent in Directive 95/46/EC.' Hence, the interpretation of consent provided for under the Data Protection Directive is applicable. Article 2(h) of the Data Protection Directive states that '"the data subject's consent" shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.'

46 Furthermore, Article 7(a) of the Directive states that 'Member States shall provide that personal data may be processed only if... the data subject has unambiguously given their consent'. This appears to be an extremely strict interpretation. Recital 66 of the amended E-Privacy Directive appears, however, to allow some room for the interpretations of the national legislators and advertisers in the interpretation of what constitutes consent.[85] The recital states that '[w]here it is technically possible and effective, in accordance with the relevant provisions of Directive 95/46/EC, the user's consent to processing may be expressed by using the appropriate settings of a browser or other application.' This appears to permit the use of browser settings to indicate consent to cookies.[86] As virtually all browsers have privacy settings that allow users to control cookie usage, the major talking point is whether data subjects' consent may be inferred from pre-existing browser privacy settings.[87] Despite its focus on the issue of consent and cookies, the amended E-Privacy Directive failed to effectively clarify the interpretation of implicit consent with respect to browser settings.[88]

47 The Article 29 Working Party, in its opinion on behavioural advertising, observed that consent *via* default browser settings is unlikely to meet the requirements under the data protection framework. This is for three particular reasons. First, the 'respawning' of flash cookies circumvents the deletion of cookies and allows the bypassing of the data subject's choice in their browser settings.[89] Second, consent via browser settings implies user acceptance to future processing, conceivably without any knowledge of the purposes or uses of the cookie. Third:

> 'based on the definition and requirements for valid consent *ex* Article 2 (h) of Directive 95/46/EC, generally speaking data subjects cannot be deemed to have consented simply because they acquired/used a browser or other application which by default enables the collection and processing of their information.'[90]

48 This is due to the fact that data subjects, in general, are unaware of tracking and, additionally, are not always aware of how to adjust the browser privacy settings. The lack of user understanding is difficult to refute and it is, perhaps, a fallacy to think data subject inaction provides an unambiguous indication of their wishes.[91] In a study conducted in the US by McDonald and Cranor, the authors noted that '[o]ne participant said behavioral advertising sounded like something her "paranoid" friend would dream up, but not something that would ever occur in real life.'[92] In a similar study, Smit, Van Noort and Voorveld concluded that their findings relating to general users' lack of understanding of tracking technology raised an important question: namely, 'what does informed consent mean within a not-well-informed audience?'[93] Accordingly, for those involved in OBA, in theory it appears to be difficult to avoid the opt-in requirement.[94] This has not always been reflected in practice due to the ambiguity provided for by implied consent.

II. Explicit Consent and the Proposed amendments

49 Member State implementation of the changes necessitated by the cookie Directive was initially inconsistent[95] and this division reflects the dichotomy in opinions in relation to this debate.[96] The ENISA Report on online behavioural tracking observes that while '[s]ome states have suggested existing browser settings would remain adequate, through the legal fiction that they convey "implicit consent"', the majority view favours requiring explicit, affirmative consent for each website.'[97] The ambiguity surrounding the interpretation of consent is a definite stumbling block to effective and consistent monitoring of OBA within the Union. In their recent article, de Lima and Legge have noted two particular criticisms of EU law in this regard. First, in relation to the ambiguous interpretation of the laws. Second, the failure to provide an effective balance between commercial and individual needs. The proposed Regulation has confirmed the EU's move towards an opt-in regime which 'is intended to strengthen consumer data protection rights by facilitating individual control over personal information.'[98] The draft adds a provision requiring all consent to be explicit. Previously, explicit consent was only required for the processing of sensitive data.[99]

50 The commentary supplementing the Regulation clarified that this modification was 'added to avoid confusing parallelism with "unambiguous" consent and in order to have one single and consistent definition of consent, ensuring the awareness of the data subject that, and to what, he or she gives consent.'[100] The modification of the consent requirement provided for in Article 7 of the draft is supplemented by Recital 25 which provides, '[c]onsent should be given explicitly by any appropriate method enabling a freely given specific and informed indication of the data subject's wishes.... Silence or inactivity should therefore not constitute consent.' The effect of these provisions is to effectively eliminate the enforceability of implied consent through default settings by requiring an express indication of consent by the user. According to Article 7(4) and Recital 34 consent is invalid where 'there is a clear imbalance between the data subject and the controller.'[101] Article 7(3) provides that the data subject has 'the right to withdraw his or her consent at any time.' The burden of proof rests with the data controller in all situations.[102]

51 Finally, it should be noted that the advancement of consent cannot be viewed in isolation but, instead, is indicative of the overall move towards counterbalancing 'the benefits of technological advancements and risks for individual data protection by complementing the legal framework with the principle of 'privacy by default and by design'.[103] Article 23 of the proposed Regulation provides that:

> '[h]aving regard to the state of the art and the cost of implementation, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.'

52 This provision aims at encouraging the development of user-friendly methods of incorporating privacy in the overall primary design and code in order to move towards the notion of user empowerment. This could impose a heavy burden upon existing business models that would need a complete overhaul to comply with the proposed provisions. Nevertheless, the development of this concept reflects the EU's insistence upon explicit consent and the struggle to find an effective and simple means for its implementation.

53 The move towards explicit consent in the proposed Regulation would remove some of the ambiguities surrounding the interpretation of this concept. Nevertheless, it is unclear whether this development is to be welcomed. An analysis of the potential problems associated with explicit consent is necessary.

III. Defining Consent and the associated difficulties

54 The proposed Regulation's emphasis on explicit consent indicates the assumption that the opt-in

version provides a stronger protection for users. At first glance it may seem that such a robust interpretation is justified. However as noted by Tene:

> 'individuals explicitly consent to agreements all the time without such consent being informed, voluntary, or meaningful. Individuals sign boilerplate contracts (e.g., with banks or insurance companies), execute clickwrap agreements and end-user license agreements (EULAs), and download apps granting whatever permissions are asked of them.'[104]

55 This is an interesting argument that possibly reflects the societal realities. US Chief Justice John Roberts has famously indicated that he does not read boilerplate provisions.[105] It is perhaps fair to conclude that a large proportion of users fail to take into account the terms of standard form contracts online. Many commentators have argued that the legalese used in these agreements renders them incomprehensible and thus irrelevant to the users.[106] Accordingly, the true value of providing the user with the information may be questionable. Nevertheless, it is worth mentioning in this regard the proposed regulation's emphasis on user-friendly information dissemination.

1. Economic justifications for information 'free-flow'

56 Richard Posner, writing *extra judiciously* and in a US context, has offered some economic justifications to allow the free flow of information. Posner has observed that these privacy harms are arguably unsubstantial *vis-a-vis* the economic and societal benefits which tracking offers.[107] Moreover, to render consent difficult to procure may prevent entities from engaging in those activities given the associated costs. As per Solove, 'the result might be to restrict uses of data in a formalistic manner that fails to distinguish beneficial from harmful uses.'[108] However, one cannot forget that users are not only consumers but are also citizens of the Union, and that they should be afforded the protections provided in the EU primary and secondary legal sources. It must be acknowledged that there is a fundamental difference in the way data protection and privacy are viewed in the US and the EU.

57 Although Posner and the proponents of the economic argument make a strong case, it is uncertain whether dividing the benefit of data access so clearly in favour of commercial gains truly benefits and reflects societal interests. Nevertheless, as noted by Tene *et al.*:

> 'Excessive reliance on opt-ins inevitably will disrupt user interfaces and encumber individuals with repetitive prompts, which they will be eager to click through to reach their destination. This will be exacerbated by the requirement in Article 7(2) of the GDPR that consent to data processing must be unbundled from other agreements.'[109]

58 The result would be a poor user experience that nullifies any positive effects of opt-in consent. The more common cookie notices become, the more mundane, easily dismissed and ineffective the obligation to consent is rendered.

59 Accordingly, this issue appears to be somewhat of a double-edged sword that will result in dissatisfaction in some form, irrespective of the decision taken. It is apparent that explicit opt-in consent places the burden on the commercial entities. Nevertheless, it is uncertain whether these changes will, in fact, have any meaningful impact for the users. The task of adequately balancing interests is undoubtedly difficult. In assessing this issue, one has to realise that the commercial and data protection interests are clearly polarised. As outlined above, this manifests itself most notably in the debate surrounding the varied interpretation of consent. This ambiguity is reflected in many of the solutions presented and remains a clear stumbling block which has proven extremely difficult to navigate.

2. Choosing defaults

60 The key difficulty in this regard is the choosing of a default position. In her article, Willis analyses this issue and refers to what she classifies as 'sticky defaults'.[110] Willis' perspective centres on the importance of default positions in manipulating user behaviour. A default position in the context of OBA refers to the standard and modifiable consent settings (i.e. opt-in or opt-out) offered to a user. Three clear assumptions from behavioural economic literature form the basis of her analysis:

> '[f]irst, that any default chosen will be "sticky," meaning that more consumers stay with the default than would explicitly choose to do so if forced to make a choice. Second, that those consumers with a preference for the opt-out position —and only those consumers—will opt out. Third, that where firms oppose the default position, they will be forced to explain it in the course of trying to convince consumers to opt out, resulting in well-informed decisions by consumers.'[111]

61 These assumptions have clearly motivated industry responses to opt-in consent. Although there are a series of commentaries relevant to how and why default positions are sticky, this does not fall within the scope of this text.[112] Instead, it is sufficient to say that the decisions relating to default settings have clear behaviour manipulating effects. Accordingly, it is no surprise that the move towards an opt-in version of consent has resulted in vastly differing interpretations. The purpose of the rest of this article is to examine the proposed solutions. The analysis contends that the future regulation of OBA lies in a legislative system that is supplemented by clever code. This is a manifestation of the concept of Privacy by Design, as proposed in the draft Regulation. It is thought that this approach could help circumvent

the difficulties imposed by the debate surrounding the default position of consent.

E. Alternatives and supplements to the EU framework

62 An alternative means of ensuring actual user agreement with the placing of tracking software (and by extension, the processing of personal data) is required. Accordingly, this section will examine the means of supplementing the current EU forms of regulating in order to effectively guarantee the protection of users. The analysis will outline and assess the alternatives offered by industry and academics and will present a potential solution to the problem.

I. Self-Regulation - A means of filling in the Regulatory gap?

63 Although it is argued that the solution lies with the concept of Privacy by Design, it is necessary to first examine self-regulation as industry associations have suggested that it could provide a platform upon which compliance with the legal requirements could be reached.[113] There have been some seemingly positive developments regarding self-regulatory mechanisms. These have focused on the standardisation of approaches not explicitly (or ambiguously) regulated by law. It should be acknowledged that these methods for self-regulation have, for the most part, harmonised the approaches in the US and the EU. The Network Advertising Initiative (NAI), the Digital Advertising Alliance (DAA), the European Advertising Standards Alliance (EASA) and the Interactive Advertising Bureau Europe (IAB Europe) all impose the same core requirements,[114] namely:

1. To provide information regarding their practices.

2. Allow users to opt out for behavioural advertising (note that this only relates to advertising and does not affect other uses).

64 In a speech delivered by Neelie Kroes in 2011 positive reference was made to the adoption of the Best Practice Recommendation and Framework by the EASA and IAB Europe advertising associations.[115]

65 Despite outward appearances, the legitimacy and legality of the adopted best practices remains unclear (especially regarding the opt-out default). In its assessment of the framework, the Article 29 Working Party concluded that the proposals failed to adhere to EU law and that they could be damaging to the industry if they believed them to be compliant.[116] Aside from the clear opt-out by default concerns, the WP outlined three additional difficulties. First, despite the fact that the opt-out cookie prevents further personalised advertising, it does not prevent the future accessing and storing of information on the user's terminal. Second, the user remains unaware of whether the cookie is retained on their computer and indeed the purposes of this retention. Third, the decision to install the opt-in cookie does not offer the possibility to manage previously installed cookies, while at the same time it establishes the mistaken assumption that it disables tracking.[117] Accordingly, the potential value of the recommendations is certainly questionable. The failure to adequately meet the obligations under the legislation reflects the weaknesses associated with self-regulation.

66 Hirsh, in his assessment of the self-regulatory approach, has outlined three criticisms.[118] First, in the balance between the public and commercial interests, firms will maintain loyal to their own profits as a priority. Indeed, the Electronic Privacy Information Center (EPIC) has observed that the self-regulatory efforts of the telecommunications industry during the 1990s enrolled approximately 5 million consumers in comparison to the over 200 million now registered on the FTC Do-Not-Call list. It is probable that this trend would be likely to continue in a behavioural advertising context and such a prediction appears to hold true to form.[119] Second, these programmes generally lack the capacity to force compliance with the guidelines against their members. In a US context, the FTC has incentivised participation by threatening potential legislative intervention.[120] This signifies the clear impotency of self-regulation to ensure compliance and progress. Third, voluntary membership will result in companies choosing to take advantage of the goodwill generated without any particular restriction being imposed by the guidelines themselves. This reflects the notion that large corporations use self-regulatory innovations as mere public relations stunts and this is perhaps indicative of the make-up of these organisations. As noted by the ENISA report, '[a]t present most of the largest online advertising and analytics companies participate, and most of the smaller ones do not. Social networks and content providers are almost entirely absent.'[121]

67 This scepticism of the industry's willingness to place consumer interests first has been evidenced in practice.[122] It is clear that this approach is not a preferable option, as it lacks the clout to force compliance and adequately protect users. However, that is not to say that it has no role in the future regulation of OBA. There have been some positive initiatives associated with user education and awareness.[123] Nevertheless, commercial interests will always outweigh user safety in the eyes of advertising

agents. Therefore, self-regulatory initiatives should be limited to soft policy best practices.

II. Privacy Enhancing Technologies

68 Given the widely accepted failure of self-regulation[124] technical solutions have been proffered and developed by industry enthusiasts. These technologies which are based on the core principles for data protection are referred to as Privacy Enhancing Technologies (PETs) and have gained increasing popularity in the last number of years.[125] PETs owe their origins to Chaum's seminal 1981 paper on 'Mix-Networks'.[126] However, awareness and adoption rates appear to have remained low.[127] This is perhaps linked to a lack of user awareness and also, potentially, the failure to provide user friendly interfaces. As observed by Mitrou and Karyda, PETs are often application or system specific and depend 'on the underlying legal and regulatory framework, on users' privacy awareness and their privacy concerns, as well as on the cost and benefits associated with their use.'[128]

69 Despite the fact that the implementation of and concepts behind these technologies are relatively simple, 'the complexity of the term makes it difficult for many stakeholders, individuals, as well as data controllers to apprehend their usefulness and, therefore, employ them.'[129] However, there has been large scale development of PETs in the form of plug-ins that use Tracking Protection Lists to monitor and block the placing of cookies on the terminal equipment of the users. The difficulty with these TPLs is that they are dependent on the effective maintenance of the list in order to avoid slipping into obsolescence and exposing the users to the risk of the newest tracking technologies.

1. 'Do Not Track' – and the proliferation of PETs

70 The development of the 'Do Not Track' policy and technology is a recent example of the proliferation of PETs. This proposal aims at enabling 'users to opt out of tracking by (all) websites they do not visit, including analytics services, advertising networks, and social platforms.'[130] It must be understood that this is not a blocking technology but, instead, is merely a means of alerting publishers and ad networks of a user's wish not to be tracked. Essentially, the mechanism inserts a 'DNT flag' into the header of the user's browser which is communicated during routine exchanges with website servers. If the flag is enabled, the user is stating that they do not consent to tracking. This does not, in itself, either block the placing of cookies or prevent the accessing of cookies on the terminal equipment of the user. Hence, the mechanism is entirely dependent on its acceptance and adoption as a policy by the advertisers. Although all of the large browsers offer Do-Not-Track, Microsoft sparked some debate with the launch of its Internet Browser version 10 by implementing the Do-Not-Track as a default feature.

2. 'Sticky defaults' and the DNT debate

71 The problems inherent in the EU framework surrounding consent and the notion of 'sticky defaults' are also prevalent in the Do Not Track debate. As noted by Fairfield:

> 'The problem is inherent in the implementation of the DNT flag. Do-Not-Track is, logically speaking, a binary flag. The value of Do-Not-Track is equal to zero or one. The switch is either "on" or "off". Yet there is a third state in the protocol, "unset," and the unset state must be provided by every software agent designer. Given that DNT:1 means that tracking is forbidden, and DNT:0 means that tracking is permitted, the unset term serves only as a gap-filler, a placeholder, a state from which every consumer must take action at non-zero cost, in order to reach his or her true preference.'[131]

72 The interpretation of this 'unset' state is extremely controversial, especially given that the idea appears to have had broad support amongst privacy enthusiasts. To counteract the DNT momentum, advertisers have attempted to reduce its relevance by diluting its standards and threatening to withdraw support. As noted by Fairfield in a US context, the attempts to side-step the purpose of the Do-Not-Track policy have focussed on the Digital Advertising Alliance's argument that the policy still permits the tracking of users as long as they are not targeted with advertisements. This contradicts the FTC opinion, which equates Do-Not-Track with Do-Not-Collect.[132] The same arguments have also been prevalent in Europe and this has led to the effective elimination of this concept as a conceivable means of supplementing user protection interests in the EU.[133]

3. Privacy by design and the future of PETs

73 Nevertheless, the lessons learned in the DNT context could be effectively used and developed to inspire fresh ideas under the heading of PETs.[134] This is especially true in applying the principles behind the DNT policy in a privacy-by-design context. Kirsch in his assessment of this issue proposes the adoption of a DNT policy that would encompass a legally mandatory browser start-up wizard that would explain the two available options (i.e. to allow tracking or not). This would require users to make a decision before they begin browsing. Individual advertisers could then contact the users in order to procure an exception excluding them from this rule. This approach would clearly satisfy the requirements expressed under the data protection framework and the proposed Regulation. Under the proposal, users would give informed prior consent that would

clearly fall into the explicit opt-in consent category due to the absence of a pre-selected default position.

74 The proposal may dilute the significance of the consent requirement by requiring users to repeatedly reconfirm their decision. In the context of internet browsing, this form of dynamic consent may be more of a nuisance than an aid. This approach also fails to take into account multi-user devices which may only allow the first user to effectively decide for or against tracking. Of course, an effective solution to this would be to require a browser log-in to enable access. This would allow ad networks and other similar service providers to distinguish between users and, hence, user consent preferences. However, to establish a log-in requirement would be cumbersome, impractical and a violation of the very idea behind the internet. In addition, such restrictions of access could potentially be deemed a violation of human rights given the increasing recognition of the right to broadband globally and, paradoxically, could also create privacy concerns in itself, as it would directly result in the creation of a profile.[135] Alternatively, one could require the start-up wizard to appear on the opening of each browsing session. This would allow the users to make informed decisions, but it would not deal with the potential development of a tracking profile that may have been created during previous browsing sessions. Moreover, this repeated requirement to make a decision would dilute the effectiveness and genuine legitimacy of user consent and would also be, potentially, deemed a restriction on the right of access.

75 It is clear from the above that it is extremely difficult to find an adequate balance between user and commercial interests. However, the systems described rely on existing notions of technology. Alternatively, one could consider tackling this issue at its root by changing technology's interaction with privacy in the design phase. With this in mind, Ian Brown has outlined an approach to protecting user data through guarding it on the user's device rather than allowing ad networks to store this information on their servers.[136] The proposal envisages the use of advertising scripts that would then request access to the device in order to render targeted advertisements. These scripts would not record or send any data. In simple terms, the advertiser would send a number of advertisements to the device and based on the personal data contained in certain specified files (i.e. a locally held profile), an appropriate advertisement would be rendered. This model was first considered by Brown *et al.* in the context of mobile phones, however, it appears to have general applicability across all devices.[137] The proposal depends on the adequate processing power of the devices and technological capacity. To effectively implement the proposals, no negative impact on the user experience can be permitted. This model is influenced strongly by the notion of user empowerment and appears to be an improved version of the privacy by design proposals described above in detail. This goal of user empowerment and, thus, data subject control over personal data has also been explored from an economic perspective and has come to be known as the Proprietary Rights Model.

III. The Proprietary Rights Model

76 The Proprietary Rights Model proposes the direct sale of information by users. It is based on the premise that user information should be considered as a tradable commodity to be purchased by companies. In simple terms, this model suggests that companies should pay users (data creators) for the access and use of their information.[138] This system conceptualises personal data in a way similar to intellectual property rights. In a behavioural advertising context, users have, potentially, limited control over their data and knowledge of the controller's identity under the current system. As such, the concept of users controlling and selling their data as a commodity is appealing. However, although there are clear benefits to this model, it appears to lack the practicality to truly develop as an alternative in this unrefined form. There are several key reasons for this negative outlook. First, there is strong debate as to whether or not the traditional forms of property laws are capable of providing the necessary protection for personal information.[139] This is due to the fact that '[n]ormatively, no proprietary rights exist on personal information. It pertains to an individual, but it does not belong to him or her in a proprietary sense'.[140]

77 It is difficult to equate personal data with intellectual property rights as, in contrast to IP, personal data only gains value when placed in the hands of advertisers.[141] Lessig, in advocating the merits of this economic approach and his instrumentalist theory of propertisation, has observed that if personal data was viewed in economic terms, the industry would be forced to develop specific PETs that would be capable of adequately protecting the users' personal data.[142] However, it remains unclear whether or not the commodification of personal data would truly inspire this protection. Companies rely on this information for advertising which, in turn, allows them to offer their website's services. If advertisers were forced to buy the information from the users, large portions of the publishers' revenue would be eliminated.[143] This could result in widespread charging for website access. In addition, this model would result in ubiquitous standard form contracts as the large internet service providers would be unable to individually negotiate contracts with each user. This would seemingly defeat this model's purpose of empowering people by forcing them to comply with contracts designed for the masses.

Finally, as noted by Cohen, the model appears to be contrary to the EU concept of 'personhood'.[144] This stipulates that privacy is a fundamental part of the person which is 'non-commodifiable' and part of the European human rights edifice.[145]

78 In addition to the criticisms already mentioned, there are also some very practical concerns regarding the actual relevance of this model given big data processing. Essentially, with today's technology the proprietary rights model may not be feasible as users would not be able to restrict access to the massive amounts of data (including meta-data) they place online. Companies are capable of exploiting this data leakage and would, therefore, be able to track users' behaviour without having to rely on the data held by the users themselves. There is, therefore, a need for an open access personal data tracking platform that allows users to effectively manage their online identity. Without such a mechanism, this will remain a very abstract model that fails to realistically cater for the recent computing developments. Brown's model does provide an interesting expansion of this idea, despite the fact that he does not quite extend his definition of property to include personal data. To incorporate privacy into the very design of the product could legitimately provide a strong basis for the future protection of users. This move towards device-specific protections could result in the development of an adequate response. Nevertheless, it should be noted that any move in this direction could be strongly opposed by manufacturers, ad networks and other advertising industry service providers.

IV. Code is Law

79 It is clear that the effective balancing of the respective interests is difficult. In order to make significant progress in relation to the protection of users, privacy will need to be incorporated into the design of devices. To focus too strongly on the implementation of legal requirements is inappropriate given the inflexibility of this form of regulation. It is important to remember Lessig's classifications and, thus, the balancing of the modalities of regulation.[146] This refers to the notion that 'Code is law' and, hence, the effective balancing of the law, norms, architecture (code) and market. It is the mix of these modalities that is significant and any response needs to effectively consider the merits of each. Lessig proffers that code, in itself, has a regulatory dimension in that it can effectively direct the actions of the users. Indeed, he notes that code and law both play an important role in the information society. Significantly, code is preferable as it is not as easily ignored as legal rules. Use is restricted by the architecture of the system, whereas compliance with laws can be a matter of choice. In applying this concept to OBA, ad networks could be restricted in their actions through the effective implementation of a code which effectively balances the modalities of regulation. The incorporation of privacy-enhancing defaults into the design of future technologies is perhaps the only means of ensuring the effective safeguarding of user privacy.

80 The key point from the above analysis is that the interpretation of consent will continue to be a sticky issue under the EU Data Protection framework unless decisive measures are taken. The development of the PETs have shown that, without the consideration of privacy from the outset, uncertainties regarding protection will remain. Accordingly, the concept of privacy by design holds the key to the development of future protections capable of adequately protecting personal data.

F. Conclusion

81 In a world of ones and zeroes, the traditional legal concepts of privacy and data protection struggle daily with advanced technological development. The current legal framework is ill-equipped to deal with modern computing. Privacy protection is of clear importance to modern society and a strong privacy framework is paramount. However, that is not to say that commercial interests should be disregarded. The economic benefits of an open internet that allows for behavioural advertising are clear and one should not simply arrest development. Technologists should be given the scope to commercialise their ingenuities. Nevertheless, just because an action is technologically possible does not mean that it should be legal or that it benefits society. From the analysis, it is clear that the use of cookies in the context of behavioural advertising invokes the applicability of the EU Data Protection Framework. Although there appears to be some uncertainty as to whether this practice amounts to personal data processing, it is clear from the analysis that this is the most probable interpretation. Nevertheless, the *lex specialis* rules in the E-Privacy Directive ensure some degree of protection for the users. The requirements elicited by these Directives are easy to decipher. However, the interpretation (and lack of a concrete definition) of the concept of consent has proven to be a serious impediment to progress. The proposed adoption of an explicit opt-in consent requirement is controversial. One has to question whether this will result in the dilution of the notion of consent and its benefits.

82 As outlined *supra*, the notion of 'sticky defaults' and the associated problems are the consequences of the focus on consent. The online advertising industry has taken advantage of this uncertainty. Nevertheless, it is also questionable whether a simple switch in

default position would effectively protect users. As noted by Mitchell:

> 'While this approach certainly solves the dilemma of reasonable data privacy expectations, it does not address what I believe is the fundamental problem associated with modern internet use: in order to use the internet for any purpose, individuals must sacrifice their right to data privacy in some measure. Such conditional use always puts the user at a substantial disadvantage. The bargaining leverage websites enjoy in this regard borders on coercion, especially when considering the modern need of internet use and the substantial sacrifice associated with private data access.'[147]

83 It is, therefore, apparent that in order to effectively guarantee the protection of users' personal data, a change in approach is required. The development of future tracking technologies is something that regulators need to monitor closely. Browser Fingerprinting, Deep Packet Inspection and History Sniffing are all conceivable means of tracking users. Given the levels of development, it is likely that technologists will find other methods of tracking users. In the era of big data, anonymisation on the internet may be a thing of the past.[148] It should also be noted that this is aided by the tracking of users across multiple devices. The acknowledgement of this development is seen in the proposed Regulation's specific provision on user tracking.

84 Privacy by design provides a potential solution that combines elements of code and law to solve this issue. To require software engineers to incorporate protections at the outset would enable the protection of users. From the lessons learned during the DNT debate, it is clear that system-specific PETs can only have a limited impact as the user is require to be aware and competent to ensure their installation. Moreover, self-regulatory approaches lack the teeth to truly have an impact. The Commission should require industry change and the incorporation of protections into the design of the devices. Although an economic or proprietary rights definition of Data Protection would yield some interesting benefits, it does not appear to be the most balanced approach for the EU. Instead, the future of protection lies with laws regulating manufacturing standards and the concept of privacy by design. As noted by Hildebrandt and Tielemans, '[t]his would incentivize technological innovation with regard to built-in data protection, because once such technology is state-of-the-art, it becomes the legal standard.'[149]

85 Nevertheless, it must be acknowledged that any such change would be difficult. The EU is the forerunner in Data Protection development globally. As a consequence, there are clear disparities with countries outside the EU. This is reflected in the recent decision by the Irish High Court to refer questions regarding the legality of the Safe Harbour provision to the CJEU.[150] Hence, any further development would be in sharp contrast with countries outside of the EU and could further isolate the EU's standards from those of other countries. However, this should not prevent action where it is merited and it is clear that reform is required. The fate of the proposed regulation and the potential future amendment of the E-Privacy Directive must be watched closely.

86 Therefore, the legal realities surrounding OBA remain uncertain. Without clarification, the monitoring of the protection of personal data will be unclear and ineffective. In conclusion, the European Commission has wrongly focused on the issue of consent and should require more active protection in the design phase of the devices as provided for under the proposed Regulation.

* Researcher at ICRI/CIR KU Leuven. This article is based on the thesis I presented as part of my LLM in IP and E-law at University College Cork. I would like to thank my supervisor Prof. Maeve McDonagh for her comments throughout the thesis writing process and YS, N and PJ for their comments on drafts of this article.

1 Patrick Van Eecke and Maarten Truyens, 'EU study on the New rules for a new age? Legal analysis of a Single Market for the Information Society' <http://goo.gl/jDlm48> accessed on 04/08/14

2 Article 29 Data Protection Working Party, Opinion 2/2010 on online behavioural advertising, Adopted on 22 June 2010

3 Paul Schwartz and Daniel Solove, 'The PII Problem', Draft Paper for Privacy Law Scholars Conference 2011, Berkeley, CA. http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=2638&context=facpubs accessed on 04/08/14

4 http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/sec%5Fcook.mspx?mfr=true

5 See the exception provided for under Recital 66 of the E-Privacy Directive

6 http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/sec%5Fcook.mspx?mfr=true.

7 For more see: https://support.google.com/adxbuyer/answer/1325008?hl=en.

8 For a discussion on the flash cookies and their advantages over standard cookies refer to the first part of the following analysis: Omer Tene and Jules Polonetsky, 'To Track or "Do Not Track": Advancing Transparency and Individual Control in Online Behavioral Advertising' (2012) 13 MINN. J. L. SCI. & TECH. 281.

9 Maurizio Borghi, Federico Ferretti, and Stavroula Karapapa, 'Online data processing consent under EU law: a theoretical framework and empirical evidence from the UK' (2013 Vol. 21 No. 2) International Journal of Law and Information Technology 109–153.

10 Omer Tene, 'Privacy: The new generations' (October 5 2010) International Data Privacy Law Advance 1-8.

11 D. Kelleher, Privacy and Data Protection Law in Ireland (Tottel Publishing 2006) 66. For more see: David Bainbridge, EC Data Protection Directive (Butterworths 1996) 14.

12 Borghi (n. 9) 109–153.

13 Paul De Hert and Vagelis Papakonstantinou, 'The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals' (2012 28) Computer law & Security review, 130-142.

14 Borghi (n. 9) 109–153.

15 ibid

16 ibid

17 See: Andrej Savin, EU Internet Law, (Elgar European Law Cheltenham UK 2013) 190-218.

18 Borghi (n. 9) 109–153.

19 Orla Lynskey, 'Track[ing] changes: an examination of EU Regulation of online behavioural advertising through a data protection lens' (2011 36(6)) E.L. Rev. 874-886

20 See: European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 25.01.2012, COM(2012) 11 final.

21 Colin Rooney, 'Reform of Data Protection Laws' (March/April 2012 ISSUE 83) Public Affairs Ireland http://www.arthurcox.com/wp-content/uploads/2014/01/PAI-Journal-Issue-83-MarchApril-2012.pdf accessed on 04/08/14

22 Jeroen Koëter, 'Behavioural targeting and data protection' available at: http://www.cambridgeforums.com/ww.admin/materials/privacy/5Behavioral%20targeting_paper_draft%20publication_030510.pdf accessed on 04/08/14

23 Bart van der Sloot and Frederik Zuiderveen Borgesius, 'Google and Personal Data Protection' in Aurelio Lopez-Tarruella (ed.) Google and the Law: Empirical Approaches to Legal Aspects of Knowledge-Economy Business Models (Springer Information Technology and Law Series Vol. 22 2012) 75-111.

24 Koëter (n.36)

25 Van der Sloot (n.37) 75-111

26 De Hert (n. 13) 130-142.

27 Koëter (n.36)

28 ibid

29 A29WP OBA (n.2)

30 See Peter Fleischer's (Global Privacy Counselor for Google) blogpost at http://peterfleischer.blogspot.ie/2008/02/can-website-identify-user-based-on-ip.html.

31 EMI & Ors v Eircom Ltd [2010] IEHC 108.

32 Scarlet v Sabam Case C-70/10, November 24, 2011

33 A29WP SE (n.36)

34 ibid

35 Lilian Edwards and Jordan Hatcher, 'Consumer Privacy Law 2: Online Direct Marketing' in Lillian Edwards and Charlotte Waelde (eds.), Law and the Internet 3rd Ed. (Hart Publishing 2009) 511-543

36 BGH, 28. 10. 2014, >> Az. VI ZR 135/13) see: juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=pm&Datum=2014&Sort=3&nr=69184&pos=0&anz=152

37 Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, Adopted on 20th June, available at: ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf

38 ibid.

39 Frederik Zuiderveen Borgesius, 'Behavioral Targeting, a European Legal Perspective', (2013 vol. 11 no. 1) IEEE Security & Privacy 82-85

40 http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf, p. 20 et seq.

41 De Hert (n. 13) 130-142.

42 ibid

43 De Hert (n. 13) 130-142.

44 A29WP OBA (n.2)

45 A29WP OBA (n.2)

46 ibid.

47 ibid.

48 N. van Eijk, N. Helberger, L. Kool, A. van der Plas and B. van der Sloot, 'Online tracking: questioning the power of informed consent' (2012 Vol. 14 No. 5) info 57-73.

49 A29WP OBA (n.2)

50 ibid.

51 Koëter (n.36).

52 Kostas Rossoglou and Nuria Rodríguez, (Ref.: X/2012/039 - 27/07/2012) Data Protection Proposal for a Regulation BEUC Position Paper http://epic.org/privacy/BEUC-Position-Paper.pdf accessed on 04/08/14.

53 N. van Eijk, N. Helberger, L. Kool, A. van der Plas and B. van der Sloot, 'Online tracking: questioning the power of informed consent' (2012 Vol. 14 No. 5) info 57-73.

54 A29WP OBA (n.2).

55 Eleni Kosta, 'Peeking into the cookie jar: the European approach towards the regulation of cookies' (2013 Vol. 21 No. 4) International Journal of Law and Information Technology 380–406.

56 A29WP OBA (n.2)

57 Arthur Cox, 'Technology Group Briefing New Data Protection Regulation – How will it affect your business?' http://www.arthurcox.com/wp-content/uploads/2014/01/Arthur-Cox-New-Data-Protection-Regulation-February-2012.pdf

58 BEUC (n.68)

59 N. van Eijk, N. Helberger, L. Kool, A. van der Plas and B. van der Sloot, 'Online tracking: questioning the power of informed consent' (2012 Vol. 14 No. 5) info 57-73.

60 A29WP OBA (n.2)

61 Christopher Kuner, Cedric Burton and Anna Pateraki, 'The Proposed EU Data Protection Regulation Two Years Later' (2014 13 PVLR 8) Privacy & Security Law Report http://www.wsgr.com/eudataregulation/pdf/kuner-010614.pdf accessed on 04/08/14

62 Borghi (n. 9) 109–153.

63 A29WP SE (n.32).

64 ibid.

65 A29WP OBA (n.2).

66 Van der Sloot (n.37) 75-111.

67 Case C-274/99 P Connolly v Commission, see also more recently in Case C-131/12, Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González.

68 BEUC (n.68).

69 Andrej Savin, *EU Internet Law*, Elgar European Law (Cheltenham, UK, 2013), pp.190-218.

70 Mitrou (n.20) 1-23.

71 See: https://support.google.com/ads/answer/2662850.

72 Andrej Savin, *EU Internet Law*, (Elgar European Law Cheltenham UK 2013) 190-218.

73 A29WP OBA (n.2).

74 Mireille Hildebrandt and Laura Tielemans, 'Data protection by design and technology neutral law' (2013 29) Computer law and Security Review 509-521.

75 BEUC (n.68).

76 Avner Levin and Mary Jo Nicholson, 'Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground', (2005 2:2) UOLTJ 357-395.

77 BEUC (n.68).

78 Schrems -v- Data Protection Commissioner (No.2) [2014] IEHC 351.

79 Andrew McStay, 'I consent: An analysis of the Cookie Directive and its implications for UK behavioral advertising' (2012 15(4)) New Media & Society 596–611.

80 European Parliament Consumer Behaviour in a Digital Environment (2011) at http://www.europarl.europa.eu/document/activities/cont/201108/20110825ATT25258/20110825ATT25258EN.pdf 117 – 122.

81 Rafi Azim-Khan and Jonathan Millard, 'EU Data Protection Opinion on Behavioural Ads & Cookies – Clarifying or Confusing?' (July 27 2010 pillsbury.com) Privacy, Data Security & Information Use 1-4.

82 Orla Lynskey, 'Track[ing] changes: an examination of EU Regulation of online behavioural advertising through a data protection lens' (2011 36(6)) E.L. Rev. 874-886

83 ibid

84 Joanna Penn, 'Behavioral Advertising: The Cryptic Hunter and Gatherer of the Internet', Federal Communications Law Journal: (2012) Vol. 64: Iss. 3, Article 6. Available at: http://www.repository.law.indiana.edu/fclj/vol64/iss3/6

85 Rafi Azim-Khan and Jonathan Millard, 'EU Data Protection Opinion on Behavioural Ads & Cookies – Clarifying or Confusing?' (July 27 2010 pillsbury.com) Privacy, Data Security & Information Use 1-4.

86 Omer Tene and Jules Polonetsky, 'To Track or "Do Not Track": Advancing Transparency and Individual Control in Online Behavioral Advertising' (2012) 13 MINN. J. L. SCI. & TECH. 281.

87 Rafi Azim-Khan and Jonathan Millard, 'EU Data Protection Opinion on Behavioural Ads & Cookies – Clarifying or Confusing?' (July 27 2010 pillsbury.com) Privacy, Data Security & Information Use 1-4.

88 Matthew S. Kirsch, 'Do-Not-Track: Revising the EU's Data Protection Framework to Require Meaningful Consent for Behavioral Advertising' (2011 XVIII) RICH. J.L. TECH. 2 http://jolt.richmond.edu/v18i1/article2.pdf.

89 European Parliament Consumer Behaviour in a Digital Environment (2011) at http://www.europarl.europa.eu/document/activities/cont/201108/20110825ATT25258/20110825ATT25258EN.pdf 117 – 122.

90 A29WP OBA (n.2).

91 ibid.

92 Aleecia M. McDonald Lorrie Faith Cranor, 'Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising', August 16, 2010.

93 Edith G. Smit, Guda Van Noort, Hilde A.M. Voorveld, 'Understanding online behavioural advertising: User knowledge, privacy concerns and online coping behaviour in Europe', Computers in Human Behavior 32 (2014) 15–22

94 Orla Lynskey, 'Track[ing] changes: an examination of EU Regulation of online behavioural advertising through a data protection lens' (2011 36(6)) E.L. Rev. 874-886.

95 See UK ICO opinion ICO, Guidance to the Privacy and Electronic Communications (EC Directive) Regulations 2003, Pt 2: Security, Confidentiality, Traffic and Location Data, Itemised Billing, CLI and Directories, paras 2.4, 6. http://www.ico.gov.uk/upload/documents/library/privacy_and_electronic/detailed_specialist_guides/pecr_guidance_part2_1206.pdf Following the Working Party Opinion the ICO has modified their opinion see: http://www.ico.gov.uk/for_organisations/privacy_and_electronic_communications/cookie_rules_prepare.aspx.

96 Frederik Zuiderveen Borgesius, 'Behavioral Targeting, a European Legal Perspective', (2013 vol. 11 no. 1) IEEE Security & Privacy 82-85.

97 ENISA, Privacy considerations of online behavioural tracking https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-considerations-of-online-behavioural-tracking accessed on 04/08/14.

98 Marc Rotenberg and David Jacobs, 'Updating the law of Information Privacy: The New Framework of the European Union' (2013 Vol. 36 No. 2) Harvard Journal of Law & Public Policy 605-652.

99 Slaughter and May, 'The new EU Data Protection Regulation - revolution or evolution?' Briefing April 2012 https://www.slaughterandmay.com/media/1844766/the-new-eu-data-protection-regulation-revolution-or-evolution.pdf accessed on 04/08/14.

100 Explanatory Memorandum available at http://ec.europa.eu/justice/data-protection/ document/review2012/com_2012_11_en.pdf accessed on 04/08/14

101 Slaughter and May, 'The new EU Data Protection Regulation - revolution or evolution?' Briefing April 2012 https://www.slaughterandmay.com/media/1844766/the-new-eu-data-protection-regulation-revolution-or-evolution.pdf accessed on 04/08/14: This will be particularly prevalent in respect of children

102 De Hert (n. 13) 130-142.

103 Borghi (n. 9) 109–153.

104 Omer Tene and Christopher Wolf, 'Draft EU General Data Protection Regulation: Costs and Paradoxes of Explicit Consent' (Summer 2013 Vol. 4 Issue 3) Information Security & Privacy News19-28.

105 http://www.abajournal.com/news/article/chief_justice_roberts_admits_he_doesnt_read_the_computer_fine_print/

106 Clark D. Asay, 'Consumer Information Privacy and the Problem(s) of Third-Party Disclosures' (2012-2013 11) Nw. J. Tech. & Intell. Prop. [xxxi]-358.

107 Richard A. Posner, Privacy, Surveillance, and Law (2008 75) U. CHI. L. REV. 249-251.

108 Daniel Solove, Privacy Self-Management and the Consent Paradox (2013 126) Harvard Law Review 1880 .

109 Omer Tene and Christopher Wolf, 'Draft EU General Data Protection Regulation: Costs and Paradoxes of Explicit Consent' (Summer 2013 Vol. 4 Issue 3) Information Security & Privacy News 19-28.

110 Lauren E. Willis, 'Why Not Privacy by Default?' (Forthcoming 2014) 29 Berkeley Tech. L.J. http://nrs.harvard.edu/urn-3:HUL.InstRepos:11266829 accessed on 04/08/14.

111 ibid.

112 See for example: Cass R. Sunstein, 'Impersonal Default Rules vs. Active Choices vs. Personalized Default Rules: A Triptych' (May 19 2013 9 Harvard Law Sch. Working Paper Series) http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2171343 accessed on 04/08/14 .

113 See for discussion: Daniel Castro, 'Benefits and Limitations of Industry Self-Regulation for Online Behavioral Advertising' (December 2011) ITIF www.itif.org/files/2011-self-regulation-online-behavioral-advertising.pdf (accessed on 04/08/14).

114 NAI 2008, DAA2009, IABE2011, DAA2011.

115 Neelie Kroes, 'Online privacy – reinforcing trust and confidence' (22 June 2011 SPEECH/11/461) Online Tracking Protection & Browsers Workshop Brussels.

116 Article 29 Working Party, Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising WP 188 (08.12.2011).

117 ibid.

118 Dennis D. Hirsch, 'The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?' (2007 34) Seattle U. L. Rev. 458 .

119 Matthew S. Kirsch, 'Do-Not-Track: Revising the EU's Data Protection Framework to Require Meaningful Consent for Behavioral Advertising' (2011 XVIII) RICH. J.L. TECH. 2 http://jolt.richmond.edu/v18i1/article2.pdf.

120 Steven C. Bennett, 'Regulating Online Behavioral Advertising' (2011) 44 J. Marshall L. Rev. 899.

121 ENISA (n.98) .

122 Ian Brown and Christopher T. Marsden, *Regulating Code: Good Governance and Better Regulation in the Information Age* (MIT Press 2013) 56.

123 Article 29 Working Party, Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising WP 188 (08.12.2011)

124 Chris Jay Hoofnagle, 'Privacy Self Regulation: A Decade of Disappointment' (2005) Elec. Privacy Info. Ctr. http://epic.org/reports/decadedisappoint.html accessed on 04/08/14, Scott Foster, 'Online Profiling Is on the Rise: How Long Until the United States and the European Union Lose Patience with Self-Regulation?' (2000 41) Santa Clara L. Rev. 255, 258, 277.

125 Mitrou (n.20) 1-23.

126 D. L. Chaum, 'Untraceable electronic mail, return addresses, and digital pseudonyms' (1981 24 (2)) Communications of the ACM 84.

127 Mitrou (n.20) 1-23.

128 ibid.

129 ibid.

130 ENISA (n.98).

131 Joshua A.T. Fairfield, 'Do-Not-Track as Default' (2013 11) Nw.J. Tech. & Intell. Prop. 575 http://scholarlycommons.law.northwestern.edu/njtip/voll1/iss7/2

132 ibid.

133 Computers Privacy and Data Protection, Reforming Data Protection: The Global Perspective, 7th International Conference 22-24th of January 2014 Brussels Belgium, Relevant video at https://www.youtube.com/watch?v=mrjFmGWisDg.

134 Ibid: See in particular Walter van Holst's presentation and Q&A session.

135 E. Bonadio, 'File sharing, copyright and freedom of speech' (2011 3(10)) European Intellectual Property Review 619-631

136 Computers Privacy and Data Protection, Reforming Data Protection: The Global Perspective, 7th International Conference 22-24th of January 2014 Brussels Belgium, Relevant video at https://www.youtube.com/watch?v=mrjFmGWisDg.

137 H. Haddadi, P. Hui and I. Brown, 'MobiAd: Private and Scalable Mobile Advertising' (2010 ACM International Workshop on Mobility in the Evolving Internet Architecture, Chicago).

138 Desiree De Lima and Adam Legge, 'The European Union's approach to online behavioural advertising: Protecting individuals or restricting business?' (2014 30) Computer Law & Security Review 67-74.

139 Paul M. Schwartz, 'Property, Privacy, and Personal Data' (2004 Vol. 117 No. 7) Harvard Law Review 2055 SSRN: http://ssrn.com/abstract=721642 accessed on 04/08/14 and Nadezda Purtova, 'Property in Personal Data: a European Perspective on the Instrumentalist Theory of Propertisation' (Autumn/Winter 2010 - Volume 2 - Issue 3) European Journal of Legal Studies accessed on 04/08/14 http://www.ejls.eu/6/84UK.pdf

140 Borghi (n. 9) 109–153.

141 Desiree De Lima and Adam Legge, 'The European Union's approach to online behavioural advertising: Protecting individuals or restricting business?' (2014 30) Computer Law & Security Review 67-74.

142 Lawrence Lessig, *Code and Other Laws of Cyberspace* (Basic Books New York 1999).

143 Desiree De Lima and Adam Legge, 'The European Union's approach to online behavioural advertising: Protecting individuals or restricting business?' (2014 30) Computer Law & Security Review 67-74.

144 J E Cohen, 'Examined lives: Informational privacy and the subject as object' (2000 52) Stanford Law Review 1436.

145 M J Radin, 'Incomplete commodification in the computerized world' (2002) The Hague: Kluwer Law International 17-18.

146 Lawrence Lessig, *Code and Other Laws of Cyberspace* (Basic Books New York 1999).

147 Ian D. Mitchell, 'Third-Party Tracking Cookies and Data Privacy' (April 25 2012). Available at SSRN: http://ssrn.com/abstract=2058326 or http://dx.doi.org/10.2139/ssrn.2058326

148 Paul Ohm, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization' (2010 57) UCLA Law Review 1701-1777.

149 Mireille Hildebrandt and Laura Tielemans, 'Data protection by design and technology neutral law' (2013 29) Computer law and Security Review 509-521.

150 Schrems -v- Data Protection Commissioner (No.2) [2014] IEHC 351.