



**Maastricht University**

**Maastricht  
Centre for  
European  
Law**



Maastricht Centre for European  
Law

# Master Working Paper

2017/2

**Christopher Mondschein**

**The Regulation of Targeted Behavioural Advertising in the  
European Union**

**Master Working Paper Series**

The MCEL Master Working Paper series seeks to give excellent Master students the opportunity to make their work accessible to a wide audience.

In order to give visibility to highly promising students interested in EU law and their research in European Law may be selected for publication on this page of the website of the Maastricht Centre for European Law under the following conditions:

1. The field of European law

2. A minimum of 10 or higher

All rights reserved

No part of this paper may be reproduced in any form

Without the permission of the author(s)

The MCEL Master Working Paper series seeks to give excellent Master students the opportunity to publish their final theses and to make their work accessible to a wide audience. Those wishing to submit papers for consideration are invited to send work to:

[mcel@maastrichtuniversity.nl](mailto:mcel@maastrichtuniversity.nl)

Our submission guidelines and further information are available at:

<http://www.maastrichtuniversity.nl/web/Institutes/MCEL/Publications1/MasterWorkingPapers.htm>

© Christopher Mondschein

Published in Maastricht, July 2017

Faculty of Law  
Maastricht University  
Postbox 616  
6200 MD  
Maastricht  
The Netherlands

This paper is to be cited as MCEL Master Working Paper 2017/2

# Table of Contents

1. Introduction .....	2
2. Online Advertisement and Targeted Behavioural Advertisement .....	4
2.1. Creating Advertisement Space on Websites .....	4
2.2. Targeting Users.....	5
2.3. Targeted Behavioural Advertisement .....	6
2.4. The Logistics of Targeted Behavioural Advertisement .....	7
2.4.1. The Ad Network Provider.....	8
2.4.2. Advertisers.....	10
2.4.3. Website Publishers.....	10
2.4.4. How is the User Connected to this Complex Network of Exchanges? .....	10
2.5. Profiling and Tracking in Targeted Behavioural Advertisement .....	10
2.5.1. Profiling .....	10
2.5.2. Tracking Users – General Remarks .....	11
2.5.3. Tracking Users – User Control over the Means of Tracking .....	12
3. The European Union Legal Framework Applicable to Targeted Behavioural Advertising.....	18
3.1. General Remarks .....	18
3.2. The Shifting Territorial and Substantive Scope of European Union Data Protection Law.....	20
3.3. Triggering Article 5(3) and the Regulation of Technical Means of User Tracking.....	22
3.4. Obtaining Consent – Who and How .....	25
3.4.1. The Act Required to Give Consent.....	26
3.4.2. Freely Given Consent .....	28
3.4.3. Informing Users .....	29
3.5. Conclusion.....	33
4. A Critical Reflection on Notice and Consent as a Regulatory Tool for Targeted Behavioural Advertising ....	34
4.1. The Reasons Notice and Consent Fails.....	34
4.1.1. Why is Notice and Consent Used?.....	34
4.1.2. Individual and Systemic Problems with Notice and Consent .....	35
4.1.3. The Adverse Effects of Notice and Consent for Individuals .....	36
4.2. The Tools in the Toolbox .....	42
4.2.1. Reducing Search and Information Costs.....	42
4.2.2. Simplified Notices = Better Notices? .....	43
4.2.3. Some Iconoclastic Thoughts .....	44
4.3. Simplified Notifications and Icons Likely Do Not Address All Individual and Systemic Problems Related to Notice and Consent for Targeted Behavioural Advertising.....	49
5. Looking for Help Elsewhere – Competition Law as a Remedy for More Systemic Problems? .....	50
6. Conclusion.....	52
7. Bibliography .....	54
7.1. Legislation .....	54
7.2. Case Law .....	55
7.3. Secondary Sources.....	56

# 1. Introduction

With the coming of age of the digital economy,<sup>1</sup> new economic models have been - and are continuously being - developed in order to reap the benefits of more efficient advertisement processes on the Internet. Over the past few years, the digital advertising economy in Europe has witnessed immense growth. In 2012, the value of the European digital advertising market alone was estimated at around €24.3bn<sup>2</sup> and it is projected to grow to \$260.4bn globally by 2020.<sup>3</sup> Further, online advertising outperformed and partially displaced 'classical' advertising methods (for example, print media, billboards, television, and so on), growing by an estimated 11.5% in 2012 alone.<sup>4</sup> This aptly illustrates the economic potential of the digital advertising market.

One of the most sophisticated online advertising methods is targeted behavioural advertisement. This method tracks users' behaviour over the course of browsing different websites, which are connected in a so-called 'ad network' that is being hosted by a provider, in order to combine the data in a user profile. This profile is then used to make inferences about an individual user's interest in order to target the specific user with more relevant advertisement on the websites within the ad network.

Targeted behavioural advertisement is effective at curbing the inefficiencies posed by the 'matching problem' prevalent in the advertisement industry. The matching problem is aptly described by the well-known quote: 'Half the money I spend on advertising is wasted; the trouble is, I don't know which half'.<sup>5</sup> The underlying problem consists of the inefficiency of matching the right ads to susceptible consumers; it is based on a lack of information on the consumer's interests and leads to a waste of resources since resources are spent advertising to unsusceptible consumers. Personalization and a finer granularity in differentiation between relevant audiences as well as the possibility to discern consumers for the purpose of targeting advertisement, therefore, constitute the most significant advantages of such targeted online advertisement over traditional forms of advertisement. The result is that targeted behavioural advertisement reduces the resources spent by advertisers while it increases the 'accuracy of the match' between advertisers and consumers, benefitting advertisers with lower costs and consumers with more relevant information.

---

<sup>1</sup> The term 'digital economy' was coined by Don Tapscott in 1995, see D. Tapscott, *The digital economy: promise and peril in the age of networked intelligence* (McGraw-Hill, 1997).

<sup>2</sup> IAB Europe website, <http://www.iabeurope.eu/digital-advertising/key-facts-statistics>.

<sup>3</sup> PWC, 'Internet Advertising', *PWC Global* (2016), <http://www.pwc.com/gx/en/industries/entertainment-media/outlook/segment-insights/internet-advertising.html>.

<sup>4</sup> IAB Europe website, <http://www.iabeurope.eu/digital-advertising/key-facts-statistics>.

<sup>5</sup> See e.g., J. Bullmore, 'Why it's time to Say Goodbye to IKHTMISAIW\* - (\*I know that half the money I spend on advertising is wasted ...)', *WPP Annual Report & Accounts* (2013), <http://www.wpp.com/annualreports/2013/what-we-think/why-its-time-to-say-goodbye-to-ikthtminoaiw/>.

However, targeted behavioural advertisement poses risks to users since it requires a large amount of personal data from users.<sup>6</sup> Users are confronted with targeted behavioural advertisement through the notification and consent mechanism that is incorporated in the EU data protection framework.<sup>7</sup> Here, the e-Privacy Directive<sup>8</sup> introduces the prior informed consent requirement in Article 5(3) that states that users must be provided all necessary information pursuant to the Data Protection Directive (DPD)<sup>9</sup> (and soon the General Data Protection Regulation (GDPR))<sup>10</sup> before they are tracked for targeted behavioural advertising. Developments on the improvement of this regulatory tool are already underway in order to facilitate the provision of information so that users are able to understand the complex processes regarding their personal data.

It is in this context that this paper questions the use of the regulatory tool of notice and consent for targeted behavioural advertising. Do users understand the information they are presented on targeted behavioural advertising, thereby fulfilling the requirement of being 'informed' before consenting? It is argued that users encounter both *individual* and *systemic* impediments in the wake of targeted behavioural advertisement, which renders the giving of informed consent to be tracked and profiled ineffective. It therefore must be questioned whether there are ways to improve the flow of information and to overcome these impediments (e.g. by simplification of notifications or the use of icons). Are the tools in the EU data protection framework adequate to achieve these goals or are there other sources of law that might help tackle these issues?

---

<sup>6</sup> See e.g., O. Lynskey, *The Foundations of EU Data Protection Law* (OUP, 2015), p. 196-227, listing a number of tangible and intangible harms; ENISA, Privacy considerations of online behavioural tracking, 19.10.2012, p. 13-14.

<sup>7</sup> In the context of this paper, the term 'data protection' is used to denote the EU notion attached to it. The term 'privacy' is used in the US context to incorporate notions that in the EU can be split up into 'data protection' and 'privacy'. See e.g. J. Kokott and C. Sobotta, 'The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR', 4 *IDPL* (2013); and O. Lynskey, *The Foundations of EU Data Protection Law*, Ch. 4 and p. 265 et seq.

<sup>8</sup> Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (e-Privacy Directive), [2002] OJ L 201/37, as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (Text with EEA relevance) (The Citizen's Rights Directive), [2009] OJ L 337/11. Unless not noted otherwise, the term 'e-Privacy Directive' will be used to refer to the amended framework. The term 'Citizens Rights' Directive' refers explicitly to Directive 2009/136/EC.

<sup>9</sup> Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive), [1995] OJ L 281/31.

<sup>10</sup> Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), [2016] OJ L 119/1.

The paper is structured as follows: Section 2 introduces the concept of targeted behavioural advertising, the key entities involved therein and the tools used to track users along with an assessment of the users' control over these tools. In this regard, it is asked whether users can actively opt out of being tracked or whether tracking is mandatory when using a given online service. Section 3 dissects the EU data protection framework regulating targeted behavioural advertising which is currently being reformed. The centre-piece of this analysis is the functioning of the informed consent requirement as well as the introduction of simplified notices and icons. Section 4 critically assesses the efficacy of notice and consent for targeted behavioural advertising. It first paints a picture of the individual and systemic problems users face, followed by an analysis of the tools introduced by the GDPR to improve informed consent. It draws on insights from empirical research, behavioural economics and semiotics to gauge the effectiveness of the proposed improvements to the notification system. Section 5 reflects on the usefulness of EU competition law to further data protection goals in the event that the data protection framework fails to provide an improvement. Section 6 concludes this article.

## 2. Online Advertisement and Targeted Behavioural Advertisement

### 2.1. Creating Advertisement Space on Websites

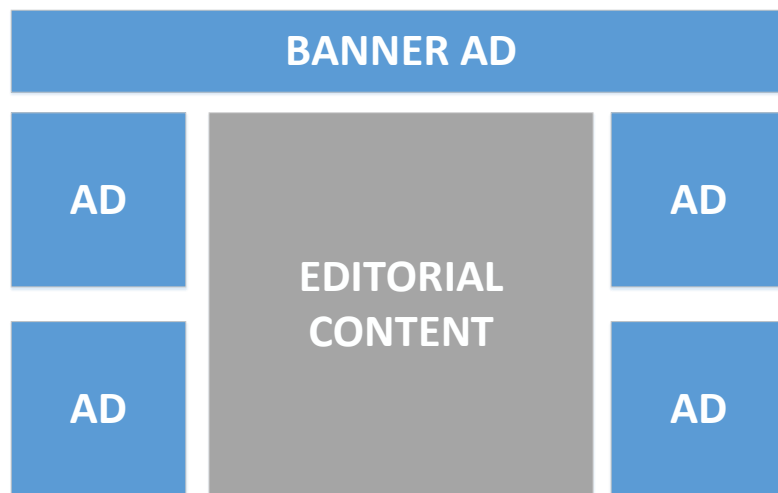
To create revenue, web developers specifically arrange for advertising space in the architecture of a website; this advertisement space is then rented out. *Figure 1* is one of many examples of a website's layout: next to editorial content (grey), advertisement space (blue) is added around the editorial content.<sup>11</sup> Traditionally, advertisement space (ad space) in these segments on a website was sold directly to advertisers, with the publisher in full control of the ad space. However, as Mayer and Mitchell state '[t]he web has evolved to facilitate development and delivery of webpages composed of content from multiple websites', citing that technologies such as HTML, Java and CSS enable web developers to delegate control of parts of a website to other entities. This made it possible for website publishers to cede control over advertisement space to specialized entities that created platforms to match advertisers and website publishers more efficiently. Advertisements filling the advertisement space (marked blue in *Figure 1*) can therefore come directly from the website publisher or from third parties designated by the website publisher. The user browsing the website will not be able to identify the origin of the advertisement by plain sight. This can become problematic in the context of targeted behavioural advertisement, as it is indistinguishable for users whether a given website has ceded control to another entity for tracking and

---

<sup>11</sup> Other forms of online advertisement are e.g., pop-ups (windows that open and cover part of the screen on top of a website's layout).

profiling users by virtue of an online ad's appearance. More importantly though, the power to track users on a website in the context of online advertisement is also partially ceded to third parties. These third parties create networks and as they grow, the amount of (personal) data collected about users also grows, as users are now tracked over all the websites that belong to such a network.

Figure 1 - Example: Layout of a Website



© Christopher Mondschein 2015

Source: C. Mondschein

## 2.2. Targeting Users

Targeting describes the act of tailoring advertisements to a specific group of users or to an individual user.<sup>12</sup> Since not all advertisements are suitable for all individuals, individuals are grouped based on their interests (this is called market segmentation)<sup>13</sup> and advertisements are then tailored to these interests and delivered to the segmented groups. The more granularity that is introduced into the distinction between consumer groups – all the way to individualization – the more likely it is that consumers will be susceptible to an advertisement and subsequently purchase a product or service. However, it is also possible for advertisers to target ads too precisely and in a way that they evoke a feeling of ‘creepiness’ in users. Yet, advertisers are not disincentivized from collecting and using large amounts of data for advertising; they simply hone and refine the way in which the advertising is presented or flag certain insights as not fit to serve for advertising.<sup>14</sup>

<sup>12</sup> See R.T. Kreutzer, *Praxisorientiertes Online-Marketing – Konzepte, Instrumente, Checklisten* (2<sup>nd</sup> edition, Springer-Gabler, 2014), p. 12-13 and 175 et seq.

<sup>13</sup> See L. Freidman, ‘Market Segmentation’, CUNY, <http://academic.brooklyn.cuny.edu/economic/friedman/mmmarketsegmentation.htm>.

<sup>14</sup> B. Schneier, *Data and Goliath – The Hidden Battles to Collect Your Data and Control Your World* (W.W. Norton & Company, 2015), p. 55-56.

Targeting users is nothing novel in the advertisement industry since advertisers have long sought to be more efficient in matching advertisements to susceptible consumers. An example would be that TV advertisements are targeted to an audience that is presumed to fit the demographic of the viewers currently watching a particular programme.

However, compared to traditional media, the presumption with online media is that a single individual is browsing the Internet on an 'end user device' (e.g. personal computer, smartphone, and so on). This means that in terms of communication, the advertiser interacts with a single person as opposed to a larger, innominate group of people, which facilitates the act of targeting since it will be easier to generate assumptions about the individual's interests.<sup>15</sup>

Different forms of targeting exist and the utilization of these forms depends on the advertising context.<sup>16</sup> Information used for targeted advertisement can be based on (i) socio-demographic traits (for example, collected via user profiles on Facebook, Amazon, and so on in which users actively report this information); (ii) the user's location, which can be measured via the IP address and Geo-Tags;<sup>17</sup> (iii) the user's hardware/software configuration (most prominently, whether the end user device is a mobile device such as a smartphone or a stationary PC);<sup>18</sup> (iv) the context of the website the user is visiting and finally (v) through tracking a user's behaviour over time while surfing different websites and creating a user profile from which the user's interests can be adduced – known as so-called behavioural tracking.<sup>19</sup> The latter form of tracking is dependent on technical means, which are explained in further detail below. Here, it is important to gauge whether the user can actually elicit control over the means of tracking utilized.<sup>20</sup>

### 2.3. Targeted Behavioural Advertisement

Based on the forms of targeting described above, different models of targeted advertisement exist: for instance, the Article 29 Working Party<sup>21</sup> refers to *contextual advertising, segmented*

---

<sup>15</sup> Ibid., Ch. 4.

<sup>16</sup> R.T. Kreuzer, *Praxisorientiertes Online-Marketing – Konzepte, Instrumente, Checklisten*, p. 175.

<sup>17</sup> Ibid.

<sup>18</sup> Ibid., p. 176.

<sup>19</sup> Ibid., p. 175-181.

<sup>20</sup> See subsection 2.E.3. below.

<sup>21</sup> The Article 29 Working Party is an independent advisory body to the European Commission, based on Article 29 of the DPD. It comprises members of the European Commission, the European Data Protection Supervisor and of the national Data Protection Agencies (DPAs) and issues (non-binding) Opinions, recommendations, working documents, letters, and so on, regarding the interpretation of the provisions of the Data Protection Directive. Even although the Opinions of the Article 29 Working Party are non-binding on the Commission and are considered 'soft law', due to the expertise and persuasiveness of the Opinions, they should be considered as de facto benchmarks for the interpretation of the provisions of the Data Protection Directive. For the role of 'soft law' in the EU in general, see R. Schütze, 'Constitutionalism and the European Union', in C. Barnard and S. Peers (eds.), *European Union Law* (OUP, 2014), p. 99-103, especially 102-103. For the role of 'soft law' and the



*advertising* and *targeted behavioural advertising* in its Opinion on targeted behavioural advertisement.<sup>22</sup> The different methods all rely on user information to determine which ads should be displayed to a given user in order to ensure maximum effectiveness. However, targeted behavioural advertisement is different insofar as it utilizes tracking and profiling to paint a more detailed picture of the user's interests.<sup>23</sup> It must be mentioned that the tracking methods are in no way mutually exclusive and can be combined in the overall advertisement and marketing strategy.<sup>24</sup>

In sum, targeted behavioural advertisement entails the collection of a user's behavioural data (while browsing the web)<sup>25</sup> over a given period and over multiple websites connected to an ad network in order to create a user profile holding information on a particular user's preferences. From this user profile, the advertiser can infer the user's interests. Ads based on the user's presumed interests are then displayed to the user over different websites that belong to an ad network.

## 2.4. The Logistics of Targeted Behavioural Advertisement

Targeted behavioural advertisement is based on a complex system involving multiple actors engaging in a number of exchanges, most of which are automated and which occur in mere milliseconds. Three key players next to the user exist: (i) the advertiser, (ii) the website publisher (iii) and the ad network provider.<sup>26</sup> The business practice of targeted behavioural advertising can be viewed as a number of exchanges between the various parties with the ad network provider as the intermediary platform. *Figure 2* gives an abstract overview of how the different entities are connected.

---

Article 29 Working Party, see P. Church, 'Should you care what the Article 29 Working Party says?', 60 *Linklaters Technology Media and Telecommunications* (2011).

<sup>22</sup> Opinion 2/2010 of the Article 29 Working Party on online behavioural advertising, 22.6.2010, WP 171, p. 5.

<sup>23</sup> See e.g., C. Casteluccia, 'Behavioural Tracking on the Internet: A Technical Perspective', in S. Gutwirth et al. (eds.), *European Data Protection: In Good Health?* (Springer, 2012), p. 21 et seq.

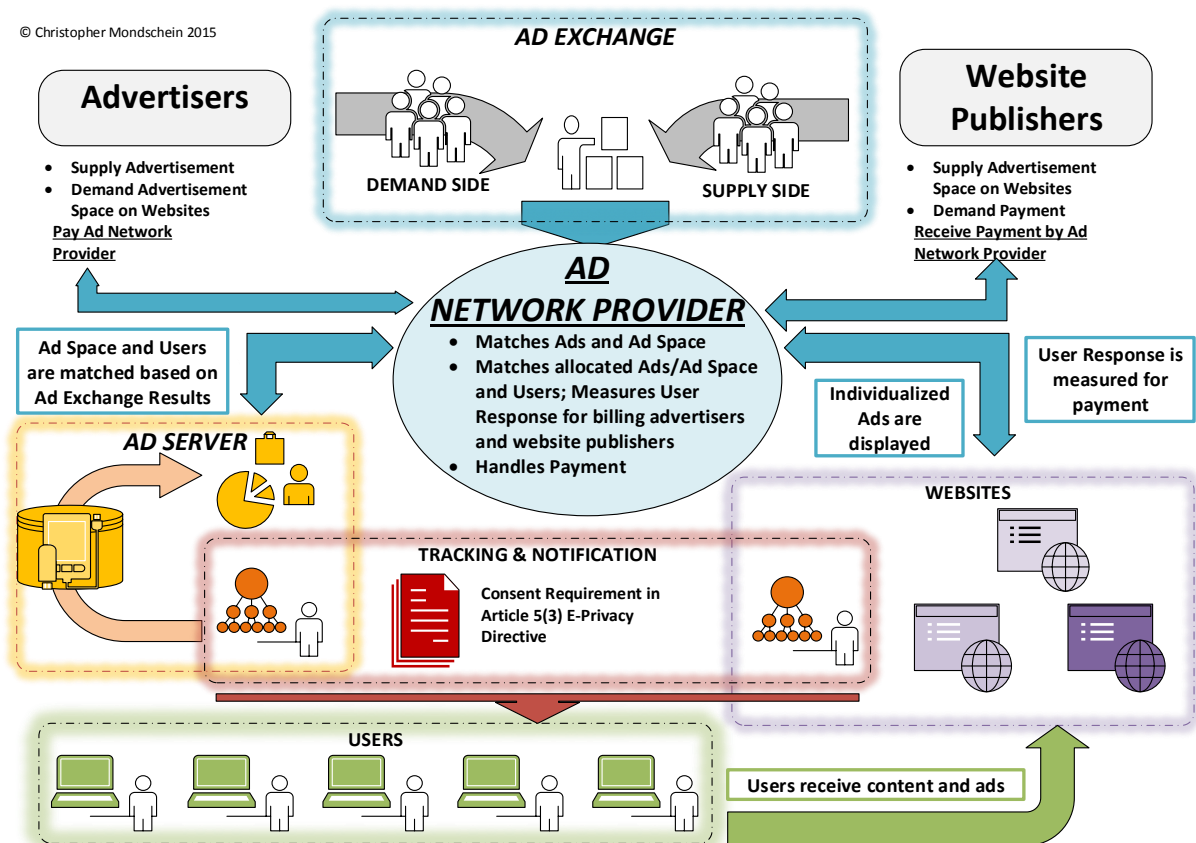
<sup>24</sup> See the next subsection for an overview of tracking techniques.

<sup>25</sup> N.B., for the purposes of this paper, focus is put on web tracking. Other tracking methods described by Casteluccia are not further discussed due to the limitation of this paper to the online environment and the inherent difference to web tracking. These other forms are location tracking in the context of RFID and smart phone/GPS data applications and social network tracking. See, C. Casteluccia, in S. Gutwirth et al. (eds.), *European Data Protection: In Good Health?*, p. 25-31.

<sup>26</sup> ENISA, Privacy considerations of online behavioural tracking, 2010, p. 4; E. Ustaran (ed.), *European Privacy – Law and Practice for Data Protection Professionals* (IAPP, 2012), p. 262; Opinion 2/2010 of the Article 29 Working Party on online behavioural advertising, 22.6.2010, WP 171, p. 4-5.

Figure 2 - The Logistics of TBA

© Christopher Mondschein 2015



Source: C. Mondschein

### 2.4.1. The Ad Network Provider

The ad network provider is the platform that connects advertisers, website publishers and users. Around the turn of the millennium, ‘the growth in advertiser demand and ad slot supply (“inventory”) made it impractical for advertisers and publishers to deal directly’.<sup>27</sup> As intermediaries, ad network providers were able to bring down the costs for matching an advertisement to an ad space and boost the reach for advertisers and website publishers.<sup>28</sup> Further, as advertisement is considered a ‘multi-sided market’ with the ad network provider as the intermediary, an ad network must reach a stable size on all ends of the platform to be profitable and to benefit from the effects of economies of scale and specialization.<sup>29</sup>

<sup>27</sup> J.R. Mayer and J.C. Mitchell, ‘Third-Party Web Tracking: Policy and Technology’, *2012 IEEE Symposium on Security and Privacy (SP)* (2012), <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&number=6234427>, p. 420.

<sup>28</sup> Ibid.

<sup>29</sup> Generally, on this, J.-C. Rochet and J. Tirole, ‘Two-Sided Markets: An Overview’, *MIT* (2004), [http://web.mit.edu/14.271/www/rochet\\_tirole.pdf](http://web.mit.edu/14.271/www/rochet_tirole.pdf); J.-C. Rochet and J. Tirole, ‘Two-Sided Markets: A Progress Report’, *Toulouse School of Economics* (2005), [http://www.tse-fr.eu/sites/default/files/medias/doc/by/rochet/rochet\\_tirole.pdf](http://www.tse-fr.eu/sites/default/files/medias/doc/by/rochet/rochet_tirole.pdf); G.G. Parker and M.W. van Alstyne, ‘Two-Sided Network Effects: A Theory of Information Product Design’, *51 Management Science* (2005); S.P. Anderson and J.J. Gabszewicz, ‘The media and advertising: a tale of two-sided markets’, in V. Ginsburgh and D. Throsby (eds.), *Handbook of the Economics of Arts and Culture – Vol. 1* (Elsevier, 2006); A. Lamadrid de Pablo, ‘The double duality of two-sided markets’, *5 Comp. Law* (2015). The size of an ad network provider’s network

Ad network providers are tasked with matching the advertisement provided by advertisers with the ad space provided by the website publisher. This can happen via direct matching based on the ad network's inventory of advertisement and ad space (blue arrows in *Figure 2*) or via the use of ad exchanges (grey arrows in *Figure 2*).

Ad exchanges became prominent in the mid-2000s as a means of allocating, by way of real-time auctioning, free ad space to advertisement that was not matched directly by the ad network provider.<sup>30</sup> In this regard, it is observed that 'there is a growing practice between advertising networks to collaborate with each other through a bidding system'.<sup>31</sup>

Next, these combinations (of advertisement and ad space) are matched with user profiles. For this purpose, users are tracked and ad servers analyse the user behaviour to discern patterns (analytics). These patterns are then collected over time in a user profile, which forms the basis for the categorization of a user into a market segment. Users in each market segment are then matched to the combination of advertisement and ad space, which is then displayed to them over all the websites that are connected to the ad network. Therefore, users are effectively 'followed' by 'relevant' ads when browsing websites in the ad network.

The ad server will also measure user response to the ads for billing.<sup>32</sup> The cash flow is as follows: advertisers pay ad network providers a certain amount  $P_a$  for matching and displaying

---

is key to its success. Thus, ad network providers have to reach a certain scale on all sides of the platform to ensure profitability: there must be sufficient demand for advertisement; there must be a sufficient supply of advertisement space and ad network providers must be able to draw on a large number of users to profile and to view the ads. The persistent collection of user data is closely linked to the provider's ability to create vast amounts of highly detailed user profiles through tracking and to maintain a large target audience to display advertisement. These elements are all interdependent and various pricing strategies for the individual nodes connected to the network exists (e.g. one side of the network may be used as a loss-leader), offering possibilities to make use of network effects. Therefore, the scale of the ad network influences both the demand side and the supply side and vice versa. Ad networks therefore have an incentive to grow which may lead to oligopolistic or monopolistic market structures. The scale of an ad network has a direct impact on the cost structure: e.g. the more profiles and high-quality information an ad network possesses and the more ad space it has, the higher the prices the ad network can charge from advertisers. However, managing these quantities also increases the costs of maintaining the ad network. Further research into the market and on the scaling of the price structures for ad network providers is necessary.

<sup>30</sup> J.R. Mayer and J.C. Mitchell, *2012 IEEE Symposium on Security and Privacy (SP)* (2012), <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6234427>, p. 420. For the technical process, see M. Stange, 'Real-Time Advertising', 5 *Wirtschaftsinformatik* (2014), p. 336. Remarkably, the process happens in real-time and the whole transaction takes only a few milliseconds due to automation. Supply-side entities and demand-side entities play a big role as additional intermediaries and specialists.

<sup>31</sup> Opinion 2/2010 of the Article 29 Working Party on online behavioural advertising, 22.6.2010, WP 171, p. 5.

<sup>32</sup> Measurement parameters for user response are: (i) Page Impressions (based how many visitors did a web page have); (ii) Ad-Impressions (how many users saw the advertisement), (iii) Ad-Clicks (how many users clicked on the ad), (iv) Click-Through-Rate (the percentage of Ad-Clicks per visitor), (v) Bounce-rate (how quickly the user exits a web page), (vi) Site-Stickiness (how long a user stay on a web page), (vii) Sign-up (amount of sign-ups for newsletters, etc.), (viii) Sales (amount of sales related to the advertisement displayed), (ix) Turnover-per-Sale (how much turnover was created per sale related to the advertisement displayed) and (x) Conversion-Rate (percentage of visitors who have completed a previously specified action). The price can then be measured in (i) Cost-per-Mille/CPM (amount per 1000 Impressions), (ii) Cost-per-Click (amount for

the advertisement. Website publishers receive a certain amount  $P_p$  from the ad network provider for renting out their ad space. The ad network keeps a certain portion of  $P_a$  called  $P_n$ .  $P_n$  is influenced by the costs of running the ad network and a profit margin for the ad network provider. For the ad network to be profitable  $P_a > P_p$  and  $P_a = P_p + P_n$ .

### 2.4.2. Advertisers

Advertisers create advertisement campaigns for products and services. Advertisement campaigns can vary between different forms of media (for example, online, offline, or a mix of both) and types of advertisement (for example, targeted advertisement, non-targeted advertisement, or a mix thereof).

### 2.4.3. Website Publishers

Publishers own websites on which advertisement space is created and rented out for the purposes of financing website content and making operations profitable.

### 2.4.4. How is the User Connected to this Complex Network of Exchanges?

Users receive 'free' content and services on a website.<sup>33</sup> For this, they are tracked and profiled over time if they have given 'informed, prior consent' and are targeted with an individualized advertisement when browsing websites that belong to an ad network.

## 2.5. Profiling and Tracking in Targeted Behavioural Advertisement

### 2.5.1. Profiling

Profiling consists of the process of 'transforming data into knowledge' by 'collecting [user] data (recording, storing and tracking) and searching for identifying patterns (with the help of data mining algorithms)'.<sup>34</sup> These patterns form the basis for the selection of the advertisement that is displayed to users. There exists a myriad of traits which can be measured and which can be used to infer user preferences from a user profile, such as age, gender, location and so on.

---

individual click), (iii) Cost-per-View (as cost per click, however for videos), (iv) Cost-per-Lead (amount based on origin of an advertisement lead to a product/service page or web shop), (v) Cost-per-Order (amount payable for advertisement that lead to a successful purchase/transaction), (vi) Cost-per-Action (amount payable for advertisement that lead to a successful action), (vii) Cost-per-Time period (e.g. amount payable for the user staying on a web page for a specified time), (viii) Costs for targeting and (ix) Cost for Frequency Capping (the costs for ensuring that a single user who has visited a web page multiple time does not count for more than one Impression). See R.T. Kreutzer, *Praxisorientiertes Online-Marketing – Konzepte, Instrumente, Checklisten*, p. 183-186.

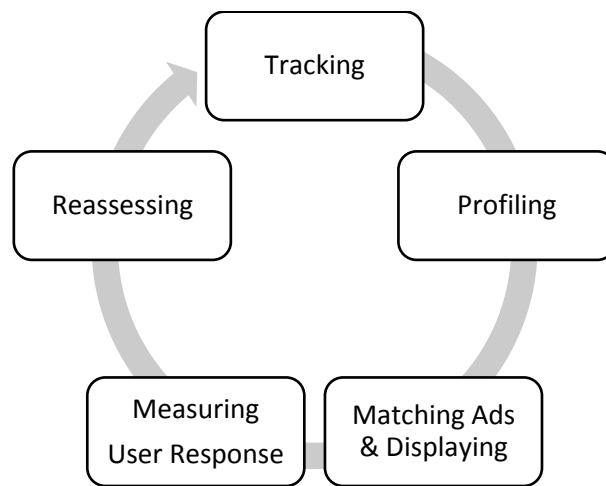
<sup>33</sup> EDPS, Preliminary Opinion on Privacy and Competitiveness in the Age of Big Data – The Interplay between Data Protection, Competition Law and Consumer Protection in the Digital Economy, March 2014.

<sup>34</sup> C. Casteluccia, in S. Gutwirth et al. (eds.), *European Data Protection: In Good Health*, p. 21.

Profiling enables a detailed picture of the user to emerge, since the individual user’s search terms, browsing habits, ‘clickstreams’,<sup>35</sup> IP address and other data are collected in an unobtrusive fashion.<sup>36</sup> The data collected by means of tracking is likely to enable ad network providers to identify the user’s personal traits with a high degree of certainty.

Hence, the more user data that is available and the longer a user can be profiled, the richer the inferences are which can be derived from a user profile. The user profiles in the context of targeted behavioural advertisements therefore lend for a more nuanced approach and higher granularity when it comes to selecting ads to be displayed to a user, and are hence of higher value. The process also tends to improve over time due to larger amounts of data and the feedback loop created in the process (see *Figure 3*).

*Figure 3 - The ‘Feedback Loop’ of Targeted Behavioural Advertisement*



Source: C. Mondschein

### 2.5.2. Tracking Users – General Remarks

User tracking is done through various technical means, which are explained further in the subsection below. As will be demonstrated, the ability for users to elicit control over being tracked is limited.

It is important to note that the tools utilized for user tracking are not solely confined to targeted behavioural advertisement as they serve several purposes on the Internet. The use of tracking outside the scope of online advertising lies in the need to identify individual users

<sup>35</sup> “Clickstream data” describes data that records the webpages a user viewed at a website, how long the user spent on each webpage, the visitor’s path through the site (including her points of entry and exit), the visitor’s IP address, and the webpage the user viewed immediately before arriving at the website’, A. Goldfarb and E. Tucker, ‘Privacy Regulation and Online Advertising’, 57 *Management Science* (2011), p. 9.

<sup>36</sup> *Ibid.*, p. 9.

for billing, fraud prevention and anti-money laundering purposes as well as for the fight against copyright infringement and in order to aid law enforcement.<sup>37</sup> These actions not only provide the legal basis for tracking users but in some cases even make it mandatory to track users.<sup>38</sup> Hence, tracking is a process that is necessary and cannot be prohibited or ‘turned off’ *per se*.

### 2.5.3. Tracking Users – User Control over the Means of Tracking

This subsection sketches out the most prominent tracking techniques applied in the context of targeted behavioural advertisement and assesses the degree of control users have on being tracked. It concludes by illustrating that users cannot escape being tracked since some of the techniques applied are mutually reinforcing. Further, user tracking may be mandated or useful in contexts outside of the scope of online advertisement. This still begs the question of how user tracking should be handled in the context of targeted behavioural advertisement and underscores the necessity to tackle this issue.

#### 2.5.3.1. HTTP Cookies

HTTP cookies are small text files (4kb) which are saved on the individual user’s terminal equipment<sup>39</sup> and enable websites to see if (and when) a user accesses a website which has set the cookie.<sup>40</sup> Generally, cookies are used to personalize a user’s surfing experience by enabling the website to recognize an individual user (e.g. making it unnecessary for the user to re-enter a password) and aid in preventing websites from incurring costs for storing a large amount of user information by delegating the storage of information to the user’s browser.<sup>41</sup> The expiration date for a cookie can vary tremendously – from a few days to hundreds of years; this is controlled by the entity setting the cookie.<sup>42</sup>

A distinction can be made between so-called *1<sup>st</sup> party cookies* and *3<sup>rd</sup> party cookies*.<sup>43</sup> *1<sup>st</sup> party cookies* are employed by publishers and only work on a specific website to which the cookie belongs.<sup>44</sup> *3<sup>rd</sup> party cookies* work across different websites and are usually employed by ad network providers in order to better track user behaviour and to build a more detailed picture

---

<sup>37</sup> O. Tene and J. Polonetsky, ‘To Track or “Do Not Track”’: Advancing Transparency and Individual Control in Online Behavioural Advertising’, 13 *Minnesota Journal of Law, Science & Technology* (2012), p. 305.

<sup>38</sup> *Ibid.*

<sup>39</sup> Also referred to as ‘end-user devices’, these terms denote the device with which the user accesses the Internet and from which user data is collected. Examples are personal computers, smartphones and other devices that are connected to the Internet and let the user browse websites. See Opinion 2/2010 of the Article 29 Working Party on online behavioural advertising, 22.6.2010, WP 171.

<sup>40</sup> See e.g., D.M. Kristol, ‘HTTP Cookies: Standards, Privacy, and Politics’, *Lucent Technologies* (2001).

<sup>41</sup> *Ibid.*, p. 4 et seq. ENISA, Privacy considerations of online behavioural tracking, 2010, p. 6.

<sup>42</sup> D.M. Kristol, ‘HTTP Cookies: Standards, Privacy, and Politics’, *Lucent Technologies* (2001), p. 4.

<sup>43</sup> For examples of the different categories, see Opinion 04/2012 of the Article 29 Working Party on Cookie Consent Exemption, 7.6.2012, WP 194. B. Schneier, *Data and Goliath – The Hidden Battles to Collect Your Data and Control Your World*, p. 47-48.

<sup>44</sup> *Ibid.*

of the user.<sup>45</sup> While 3<sup>rd</sup> party cookies are recognized by all websites in an ad network, 1<sup>st</sup> party cookies are constrained to the website which actually places the cookie. Thus, tracking by means of 3<sup>rd</sup> party cookies enables the ad network provider to see which pages a user frequents and the sequence in which these websites are visited. Most web browsers offer the possibility for users to control the cookie setting as a reaction to criticism concerning user privacy.

Therefore, the effective blocking of cookies in most web browsers is possible by using the private browsing modes that various web browsers offer (which automatically delete cookies after a browsing session) or by using browser plug-ins and extensions which will block cookies.<sup>46</sup> Hence, users potentially have a high degree of control over HTTP cookies.

#### 2.5.3.2. Flash Cookies/Supercookies/Evercookies

These are an exploit of Adobe FlashPlayer allowing the storage of ‘supercookies’, which are up to 100 kb large, on the end-user device.<sup>47</sup> Flash cookies are necessary for displaying certain media in the browser. These ‘supercookies’ were used to ‘resurrect’ other, already deleted cookies in the browser.<sup>48</sup>

Unlike HTTP cookies, Flash cookies were up until recently not affected by users’ browser settings and as a corollary by users’ choices concerning the limitation of third party tracking.<sup>49</sup> Further, Flash cookies are able to ‘respawn’, meaning that a Flash cookie that was previously deleted can restore itself, thus overriding the user’s express will not to be tracked.<sup>50</sup> After much media attention and some litigation in the US, Adobe Systems has reacted by ensuring that the deletion of Flash cookies is now part of the cookie control feature.<sup>51</sup>

Viewing this, a pattern emerges in the (ab)use of technology in the context of commercial tracking: (i) a technology is developed to identify users for security reasons or other legitimate purposes; (ii) the technology is then used to track individuals for commercial purposes such as targeted advertising; (iii) this practice is detected and made public by experts and/or stakeholders; (iv) there is an *ex post* reaction to the perceived abuse of the technology (by the regulator and/or the proprietor of the technology). This pattern of using already existing technology (here, Flash cookies necessary for viewing media in the browser) and extending their use to tracking for commercial purposes (for example, to gain more information by tracking users to more effectively serve targeted ads) until detection and, finally, the prohibition of the practice, is not limited merely to Flash cookies. Research has uncovered

---

<sup>45</sup> Ibid.

<sup>46</sup> See ENISA, Privacy considerations of online behavioural tracking, 2010, p. 15.

<sup>47</sup> O. Tene and J. Polonetsky, 13 *Minnesota Journal of Law, Science & Technology* (2012), p. 292-294.

<sup>48</sup> See ENISA, Privacy considerations of online behavioural tracking, 2010, p. 7.

<sup>49</sup> Ibid.; O. Tene and J. Polonetsky, 13 *Minnesota Journal of Law, Science & Technology* (2012), p. 292-294.

<sup>50</sup> O. Tene and J. Polonetsky, 13 *Minnesota Journal of Law, Science & Technology* (2012), p. 292-294.

<sup>51</sup> Ibid.

other examples following this pattern, for example in connection to Microsoft Silverlight, HTML5 databases, ETags and many more; the evolution of a more complex architecture of the Internet provides many opportunities for the occurrence of this pattern.<sup>52</sup>

### 2.5.3.3. History sniffing

History sniffing is one of the many exploits used with JavaScript.<sup>53</sup> It works by using the history function in the browser. Browsers save the pages a user has visited in order to highlight URLs of websites already opened in purple, instead of blue, text colour.<sup>54</sup> With a JavaScript programme, a list of websites is checked against the browser's saved history to see whether there are matches. This mode of tracking works by finding matches in the user's browsing history with the list used by the exploit. If matches are found, it can be ascertained that the user has visited the matching websites.<sup>55</sup>

The detection of this method of tracking is difficult and users may not notice that browser history sniffing is taking place.<sup>56</sup> Unlike HTTP cookies, browser history sniffing is not affected by the browser settings or browser plug-ins and extensions, consequently, impeding the user's ability to control this tracking process.

### 2.5.3.4. Browser Fingerprinting

Browser fingerprinting is a means of tracking that identifies the user's browser settings, plug-ins, extensions, the computer's operating system and many other factors to distinguish a web browser configuration on a user's terminal equipment from other web browsers on the Internet.<sup>57</sup> These elements are necessarily sent out to websites in order to properly display and engage a website in a web browser.<sup>58</sup> In essence, a chain of variables is created by taking into account the various traits of a browser sent to a website. From the composition of the different traits it is possible to identify an individual user's browser and distinguish it from a large number of other users' browsers. Browser fingerprinting thus works similar to fingerprinting in a forensic setting: while forensic fingerprinting makes use of the human finger's unique patterns and ridges on the finger's skin, browser fingerprinting uses the web browser's identification number along with its browser settings (language, software and

---

<sup>52</sup> Ibid., p. 294.

<sup>53</sup> See on the weakness of JavaScript, ENISA, Privacy considerations of online behavioural tracking, 2010, p. 7.

<sup>54</sup> D. Jang et al., 'An Empirical Study of Privacy-Violating Information Flows in JavaScript Web Applications', *Proceedings of CCS* (2010), p. 270. See also B. Krebs, 'What you should know about History Sniffing', *KrebsonSecurity* (2010), <http://krebsonsecurity.com/2010/12/what-you-should-know-about-history-sniffing/>.

<sup>55</sup> Ibid.

<sup>56</sup> Ibid.

<sup>57</sup> See e.g., P. Eckersley, 'How Unique Is Your Browser?', *Electronic Frontier Foundation* (2014), <https://panopticklick.eff.org/browser-uniqueness.pdf>; Opinion 9/2014 of the Article 29 Working Party on the application of Directive 2002/58/EC to device fingerprinting, 25.11.2014, WP 224; ENISA, Privacy considerations of online behavioural tracking, 2010, p. 7.

<sup>58</sup> Opinion 9/2014 Article 29 Working Party on the application of Directive 2002/58/EC on device fingerprinting, 25.11.2014, WP 224, p. 5.



hardware, region, browser extensions and so on) to identify users.<sup>59</sup> The number of factors used for identification as well as the browser identification number establish a unique combination that is reminiscent of a human fingerprint. Therefore, it is possible to identify an individual user's browser among a large number of other browsers based on these features.

This tracking tool works passively and does not access the user's terminal device; simply by analysing the unique set-up of a user's browser, it is able to identify a user's browser with a high degree of accuracy. Therefore, users cannot detect when they are being tracked via browser fingerprinting. This is problematic since users cannot control being tracked as there is no simple opt-out or mechanism akin to a 'cookie-blocker'.

What is more, the privacy-minded user who customizes his web browser by making use of privacy-enhancing tools, such as browser plug-ins and extensions - for example, to stop being tracked via cookies -, actually facilitates his identification by installing these programmes on his web browser. The installation of such programmes adds more variables to the chain, which in turn makes the browser more unique and therefore easier to identify. This means that in order to exert control and to prevent tracking through cookies, customizing your web browser is necessary. Whereas in order to mitigate and control tracking by browser fingerprinting, leaving the browser in the default setting is the best option in order to be as unidentifiable as possible, thus creating a conundrum for the user in terms of controlling tracking and rendering protection from tracking by both tools mutually exclusive.

The Article 29 Working Party has reacted to the shift from the use of cookies to track users to the supplemental use of browser fingerprinting by issuing an Opinion stating that browser fingerprinting falls under the scope of Article 5(3) of the e-Privacy Directive.<sup>60</sup> This means that third parties must obtain prior informed consent from users under the same standards as required for cookies. However, due to the obfuscated nature of browser fingerprinting and the fact that counter-measures do not exist and, even more, countermeasures against cookies increase the effectiveness of browser fingerprinting, this tracking tool poses a risk to users.

#### 2.5.3.5. Web Bugs/Beacons/Tracking Pixels

These are very small objects (usually only 1 x 1 Pixel in size) embedded in a website's code which are invisible to the user.<sup>61</sup> Unlike HTTP cookies, Web Bugs are not stored on the user's terminal equipment.<sup>62</sup> They are used to track a user's movement between different websites and to monitor how long a user remains on a website and how far the user scrolls down on a

---

<sup>59</sup> The following web tool illustrates the information browser fingerprinting collects, <http://fingerprinting.comyr.com>. In order to check how identifiable your browser is amongst other, see Panoptick, <https://panoptick.eff.org/index.php?action=log&js=yes>.

<sup>60</sup> Article 29 Working Party Opinion 9/2014 on the application of Directive 2002/58/EC on device fingerprinting, 25.11.2014, WP 224, p. 2-3; and Section 3.E. below.

<sup>61</sup> A. Goldfarb and E. Tucker, 57 *Management Science* (2011), p. 7.

<sup>62</sup> *Ibid.*

web page.<sup>63</sup> Goldfarb and Tucker point out that ‘Web Bugs are widely used on commercial websites’, citing that in 2000, 96% of the US Top 50 websites utilized Web Bugs for commercial tracking.<sup>64</sup>

Due to their unobtrusive nature and passive tracking abilities, users have little control over Web Bugs.

#### 2.5.3.6. Deep Packet Inspection

Deep Packet Inspection (DPI) is a technique that can be utilized by Internet Service Providers (ISP) by scanning the contents of so-called data packets, which are data bundles transmitted from and to users and which pass through the ISP.<sup>65</sup> All user traffic travels through the ISP since the ISP connects the user to the Internet (and is remunerated by the user for this service). Therefore, the ISP is the de facto link between the user and the rest of the Internet. The nature of the data analysed in DPI is sensitive and it has been likened to the act of ‘postal employees opening envelopes and reading the letters inside’.<sup>66</sup>

Initiatives for the collaboration between ISPs and advertisers in using DPI have sparked public outrage, especially in the UK where between 2006 and 2011 the company Phorm partnered up with British ISPs BT, TalkTalk and Virgin Media to conduct targeted advertising based on DPI.<sup>67</sup> Ultimately, the public outcry and the intervention by the Commission and the UK authorities led to the restriction of DPI for targeted advertising in a strict opt-in model (which has not proven successful).<sup>68</sup> This is a further indicator of the validity of the pattern described above (as was the case for Flash Cookies).

Therefore, users obtained a high degree of control only *after* a strong opt-in stance was taken as a result of public outcry.

#### 2.5.3.7. Do-Not-Track & Technical Means Employed to Stop Tracking

---

<sup>63</sup> Ibid.

<sup>64</sup> Ibid.

<sup>65</sup> O. Tene and J. Polonetsky, 13 *Minnesota Journal of Law, Science & Technology* (2012), p. 298.

<sup>66</sup> Ibid.

<sup>67</sup> For a detailed summary and legal analysis, see L. Edwards and J. Hatcher, ‘Consumer Privacy Law 2: Data Collection, Profiling and Targeting’, in L. Edwards and C. Waelde (eds.), *Law and the Internet* (2009, Hart Publishing), p. 531-537. See also, O. Tene and J. Polonetsky, 13 *Minnesota Journal of Law, Science & Technology* (2012), p. 299; C. Williams, ‘BT and Phorm: how an online privacy scandal unfolded’, *The Telegraph*, 08.04.2011, <http://www.telegraph.co.uk/technology/news/8438461/BT-and-Phorm-how-an-online-privacy-scandal-unfolded.html>. For a more technical perspective, see R. Clayton, ‘The Phorm “Webwise” System’, *Computer Laboratory, University of Cambridge* (2008), <http://www.cl.cam.ac.uk/~rnc1/080518-phorm.pdf>.

<sup>68</sup> E. Kosta, *Consent in European Data Protection Law* (Nijhoff, 2014), p. 290-291.

An abundance of privacy enhancing counter-measures against tracking are at the user's disposal.<sup>69</sup> Ad-blocking browser plug-ins and extensions such as Adblock Plus<sup>70</sup> prevent the display of ads in the web browser, whereas Ghostery and similar plug-ins prevent the setting of HTTP cookies.<sup>71</sup> Similarly, Do-Not-Track was a proposed standard to avoid user tracking, which, however, was not widely accepted and work on it is still ongoing.<sup>72</sup>

Website publishers and ad network providers oppose these tools. Recalling the economic mechanism behind tracking and targeted behavioural advertisement, they argue that the use of these tools by individual users is only sustainable as long as a sufficient number of users refrain from their use.<sup>73</sup> This is based on the premise that content is provided in exchange for user information which in turn is used to advertise goods to users. Hence, if privacy-enhancing tools were to proliferate, it is arguable that at a certain point the whole exchange model could potentially become unsustainable.<sup>74</sup>

Further, the efficacy of these tools is contested as their use is only effective against some forms of tracking technology (HTTP cookies and, as of recently, Flash cookies) while their use can facilitate tracking through other means (browser fingerprinting) or has no effect on other tools (history sniffing, Web Bugs). In many cases, the user cannot fully control whether and when (s)he wants to be tracked.<sup>75</sup>

Concerning the economic implications for content delivery, as for now, the use of blocking technologies has not yet reached a point where it severely affects the finances of ad networks. This can be attributed to the general lack of knowledge about the underlying mechanisms of targeted behavioural advertising and their implication for user privacy as well as the lack of

---

<sup>69</sup> See ENISA, Privacy considerations of online behavioural tracking, 2010, p. 15.

<sup>70</sup> However, the business model relies on 'white listing': Adblock Plus receives payment from advertisers and ad network providers in order to circumvent blocking, see e.g., L. O'Reilly, 'Google, Microsoft, and Amazon are paying Adblock Plus huge fees to get their ads unblocked', *Business Insider UK* (2015), <http://uk.businessinsider.com/google-microsoft-amazon-taboola-pay-adblock-plus-to-stop-blocking-their-ads-2015-2?r=US>. The legality of these business models was recently put to the test in Germany, where a group of publishers including Axel Springer AG sued Eyeo GmbH, the owners of Adblock Plus. Multiple cases were brought inter alia before the Regional Courts in Cologne, Munich I and Hamburg. The latter two courts have decided in favour of Eyeo GmbH, holding the service provided by Adblock Plus to be legal (see LG Munich I, Urt. v. 27.05.2015, Az. 37 O 11673/14, 37 O 11843/14; LG Hamburg, Urt. V. 21.04.2015, Az. 416 HKO 159/14), whereas the case before the Cologne court is still pending.

<sup>71</sup> Website of Ghostery, <https://www.ghostery.com/en-GB/>.

<sup>72</sup> See J. Mayer, 'Do Not Track as a Generative Approach to Web Privacy', *W3C* (2010), <http://www.w3.org/2011/track-privacy/papers/mayer.pdf>; O. Tene and J. Polonetsky, 13 *Minnesota Journal of Law, Science & Technology* (2012), p. 320.

<sup>73</sup> E.g., IAB and C3Research, 'Ad Blocking: Who Blocks Ads, Why and How to Win Them Back', *IAB Website* (2016), [www.iab.com/wp-content/uploads/2016/07/IAB-Ad-Blocking-2016-Who-Blocks-Ads-Why-and-How-to-Win-Them-Back\\_2016.pdf](http://www.iab.com/wp-content/uploads/2016/07/IAB-Ad-Blocking-2016-Who-Blocks-Ads-Why-and-How-to-Win-Them-Back_2016.pdf).

<sup>74</sup> Ibid.

<sup>75</sup> B. Schneier, *Data and Goliath – The Hidden Battles to Collect Your Data and Control Your World*, p. 47 et seq.

knowledge of the existence of blocking tools.<sup>76</sup> However, current debates on whether browsers should implement an opt-in or opt-out mechanism for tracking by having a default do-not-track status have received a lot of attention.<sup>77</sup> The ‘opt-in vs opt-out’ debate is far-reaching and depicts the fundamental problem of balancing the economic viability of serving content online and the protection of the users’ data protection rights and the degree of control users should possess over being tracked.<sup>78</sup>

#### 2.5.3.8. Conclusion

This subsection has illustrated that users often lack control over being tracked, as tracking is in some cases legally required, but for the most part, users are not able to detect or prevent themselves from being tracked. Further, as in the case of cookies, a legal differentiation is made between cookies necessary to provide services and other forms of commercial cookies, which has a direct impact on the mode of consent necessary to be obtained from the user: no consent is needed for the necessary technical cookies whereas consent is needed for other forms of cookies (for example, for commercial tracking by third parties such as ad networks for targeting advertisement).<sup>79</sup> The situation is complicated by the fact that the requirement for consent differs in various Member States and harmonization efforts have not been fruitful.

Additionally, regulatory lag plays a large role here, which can be illustrated by the rise of browser fingerprinting as a means to circumvent the (fragmented) regulation on cookies. The pattern that emerged in the context of Flash cookies and the business operations of Phorm is indicative for the reactive nature of the regulator(s).

In sum, users face difficulties in exerting control over being tracked – it seems as if the deck is stacked against them. However, what is most striking is the fact that all this is the case with the underlying presumption that the user is a well-informed, rational decision-maker when interacting with these technologies. The next section will explore the fragmented legal framework and will look more closely at the legal requirements for website publishers and ad network providers vis-à-vis users.

## 3. The European Union Legal Framework Applicable to Targeted Behavioural Advertising

### 3.1. General Remarks

---

<sup>76</sup> PageFair and Adobe, ‘Adblocking goes mainstream’, PageFair and Adobe report 2014, <https://downloads.pagefair.com/wp-content/.../05/Adblocking-Goes-Mainstream.pdf>.

<sup>77</sup> O. Tene and J. Polonetsky, 13 *Minnesota Journal of Law, Science & Technology* (2012), p. 320.

<sup>78</sup> Ibid.

<sup>79</sup> See Section 3.C. below.

The EU data protection framework applies in two distinct, yet related ways to targeted behavioural advertisement: first, users must be presented with information provisions to inform them of the scope of tracking and targeting applications on a website; second, users' consent must be obtained before tracking and targeting can take place. These two elements pose some uncertainty as to their practical application – which is also partly attributable to the divergent implementation of EU data protection law across the Member States. Further, the GDPR, which will be applicable from spring 2018,<sup>80</sup> will alter the current EU data protection framework. This also paves the way for the revision of the e-Privacy Directive.<sup>81</sup>

EU law regulates the tracking of users based on the provisions of the Data Protection Directive, which form a baseline through its key principles and Articles 2(h) and 7(a) of the DPD on consent as well as the information rights for users in Articles 10 and 11 of the DPD.<sup>82</sup> These provisions are specified by the e-Privacy Directive, whereby Article 5(3) mandates user consent and prior information for the purpose of tracking in most cases in the online environment.

The e-Privacy Directive is *lex specialis* to the Data Protection Directive.<sup>83</sup> The e-Privacy Directive was amended in 2009 by the so-called Citizen's Rights Directive, which inter alia broadened the scope of Article 5(3) of the e-Privacy Directive and further addressed cookies in Recital 66 thereof.<sup>84</sup> The current version of Article 5(3) of the e-Privacy Directive as amended by the Citizens Rights' Directive reads:

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 concerned 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. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.

---

<sup>80</sup> Article 99 of the GDPR.

<sup>81</sup> See Website of the European Commission, <https://ec.europa.eu/digital-single-market/en/news/eprivacy-directive-commission-launches-public-consultation-kick-start-review>. At the time of writing, the public consultation phase has closed.

<sup>82</sup> Consent is one of the legal bases that legitimize data processing, see Article 7 of the DPD and, in the future, Article 6 of the GDPR.

<sup>83</sup> Opinion 2/2010 of the Article 29 Working Party on online behavioural advertising, 22.6.2010, WP 171, p. 9-10. See also, inter alia, O. Lynskey, 'Track[ing] changes: an examination of EU Regulation of online behavioural advertising through a data protection lens', 36 *European Law Review* (2011), p. 876-877; E. Kosta, *Consent in European Data Protection Law*, p. 277-278.

<sup>84</sup> See E. Kosta, *Consent in European Data Protection Law*, p. 292 et seq.

The obligation laid down in Article 5(3) of the e-Privacy Directive is twofold: first, the user must be provided ‘with clear and comprehensive information, in accordance with Directive 95/46/EC’; second, after the user has received such information, the user has to consent to the ‘storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user’. This also means that the relation between the e-Privacy Directive and the DPD (and the GDPR, once it replaces the DPD) is twofold: first, Article 5(3) of the e-Privacy Directive makes direct reference to the DPD regarding the information that must be provided to users; second, the DPD applies to all cases that fall within the scope of the EU data protection framework but which are not explicitly covered by the e-Privacy Directive.<sup>85</sup> The last sentence of Article 5(3) of the e-Privacy Directive contains an exception based on strict necessity, waiving the requirement to obtain consent from users, albeit users still must be informed prior to the placement of cookies or similar tracking technologies in their terminal equipment.

### 3.2. The Shifting Territorial and Substantive Scope of European Union Data Protection Law

Article 1(2) of the e-Privacy Directive together with Article 4(1)(a) and (c) of the DPD determine the territorial scope of the EU data protection framework in the context of targeted behavioural advertising. The scope of the e-Privacy Directive is contingent upon the provisions of the DPD, however, this is a contentious issue due to the lack of harmonization and the complex link between the two legal instruments.<sup>86</sup>

Article 1(2) and Recital 10 of the Preamble to the e-Privacy Directive refer to the DPD regarding the territorial scope.<sup>87</sup> EU data protection law applies to controllers who process personal data in the territory of the EU (Article 4(1)(a) of the DPD) or if the controller is established outside the EU but makes use of equipment located in the EU and such equipment is not solely used for the purposes of transit through the EU (Article 4(1)(c) of the DPD).<sup>88</sup>

---

<sup>85</sup> See for instance, L. Moerel, ‘The Long Arm of EU Data Protection Law: Does the Data Protection Directive Apply to Processing of Personal Data of EU citizens by Websites Worldwide?’, 2 *IDPL* (2010). Compare F.J. Zuiderveen-Borgesius, ‘Personal data processing for behavioural targeting: which legal basis?’, 5 *IDPL* (2015), p. 170 et seq.

<sup>86</sup> See for instance, P. Lee, ‘The e-Privacy Directive - when and how does it apply exactly?’, *FieldFisher Privacy, Security and Information Law* (2011), <http://privacylawblog.fieldfisher.com/2011/the-e-privacy-directive-when-and-how-does-it-apply-exactly/>. The issue is also currently at stake in the debate surrounding the revision of the e-Privacy Directive, see e.g., European Commission, ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation, Final Report (European Commission, 2015), p. 8-9, 69; ETNO, Study on the ePrivacy Directive (DLA Piper, 2016), p. 29.

<sup>87</sup> Compare Article 3(1) of the e-Privacy Directive. See P. Lee, ‘The e-Privacy Directive - when and how does it apply exactly?’, *FieldFisher Privacy, Security and Information Law* (2011), <http://privacylawblog.fieldfisher.com/2011/the-e-privacy-directive-when-and-how-does-it-apply-exactly/>.

<sup>88</sup> See on the scope of Article 4 of the DPD, L.A. Bygrave, *Data Privacy Law – An International Perspective* (2014, Oxford University Press), p. 199-203, for a critical appraisal of the territorial scope of the DPD. See for a definition of the concept of ‘controller’ and ‘processor’ in EU data protection law, Opinion 1/2010 of the Article 29 Working Party on the concepts of “controller” and “processor”, 16.2.2010, WP 169. See for a

As for the substantive scope, in the context of Article 5(3) of the e-Privacy Directive, it is stated in Recital 24 of the Preamble to the e-Privacy Directive that the scope is not limited to personal data but ‘to *any information* that is stored on the terminal equipment of a user and not only to information that qualifies as personal data’.<sup>89</sup> The provision therefore serves as a catchall that is not limited to ‘publicly available electronic communications services’ that are mentioned in Article 3(1) of the e-Privacy Directive since this provision is circumvented by the combined reading of Article 1(2) and Recital 10 of the Preamble to the e-Privacy Directive.<sup>90</sup>

The criteria applied have the effect of exposing a very large number of websites to the EU data protection framework, a sentiment shared by the Article 29 Working Party in the context of targeted behavioural advertising.<sup>91</sup> However, the vagueness of the concept and the lack of definitions of key terms in Article 4(1)(c) of the DPD still leaves a great deal of uncertainty on this matter.

The connecting factor of ‘establishment’ in the DPD was put to a test in the Court of Justice of the European Union’s (CJEU) judgment in *Google Spain*,<sup>92</sup> whereby the CJEU was criticized for expanding the scope of the DPD outside the letter of the law.<sup>93</sup> The ensuing debate did little to bring a clear line in the discussion surrounding the territorial scope of the EU data protection framework.

With the GDPR, the territorial scope applicable to targeted behavioural advertising will mitigate possible lacunae: Article 3(2)(ii) of the GDPR has shifted away from the concept of

---

discussion of the application of Article 4(1)(a) and (c) of the DPD and a critical examination of its grey areas, L. Moerel, 2 *IDPL* (2010).

<sup>89</sup> E. Kosta, *Consent in European Data Protection Law*, p. 297. Emphasis kept from the original. Opinion 2/2010 of the Article 29 Working Party on online behavioural advertising, 22.6.2010, WP 171, p. 9.

<sup>90</sup> Opinion 2/2010 of the Article 29 Working Party on online behavioural advertising, 22.6.2010, WP 171, p. 9, with reference to Opinion 1/2008 of the Article 29 Working Party on data protection issues related to search engines, 4.4.2008, WP 148, p. 12-13.

<sup>91</sup> Opinion 2/2010 of the Article 29 Working Party on online behavioural advertising, 22.6.2010, WP 171, p. 10-11, referencing Article 29 Working Party Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites, WP 56, 5035/01/EN/Final, 30 May 2002, especially p. 5-11.

<sup>92</sup> Case C-131/12 *Google v. Agencia Espanola de Proteccion de Datos (AEPO) and Mario Costeja Gonzalez*, EU:C:2014:317.

<sup>93</sup> Compare the Opinion of Advocate General Jääskinen in Case C-131/12 *Google v. Agencia Espanola de Proteccion de Datos (AEPO) and Mario Costeja Gonzalez*, EU:C:2013:424, para. 60-68. On the extraterritorial effect and the divergence between the wording of the DPD and the scope of interpretation by the CJEU see e.g., C. Wolf, ‘Impact of the CJEU’s Right To Be Forgotten – Decisions on Search Engines and Other Service Providers in Europe’, 21 *Maastricht Journal of European and Comparative Law* (2014), p. 548-550; compare H. Hijmans, ‘Right to Have Links Removed: Evidence of Effective Data Protection’, 21 *Maastricht Journal of European and Comparative Law* (2014), arguing that the effective protection of EU fundamental rights (i.e. the protection of individuals’ personal data) requires EU data protection law to apply in these cases. This can be viewed as a clash between two the streams that the EU data protection framework has to bridge: namely (i) the effective protection of fundamental rights and (ii) creating clear rules for economic integration on the free movement of personal data. See on this, O. Lynskey, *The Foundations of EU Data Protection Law*, Ch. 3.

‘establishment’ towards triggering the applicability of the EU data protection framework when entities ‘monitor EU residents’ behaviour’. This means that ad network providers and website publishers who previously did not count as having an establishment in the EU (however far the wording of the DPD was stretched), now certainly fall within the scope of EU data protection law when they monitor EU residents’ behaviour.

In effect, this means that the legal framework has now shifted from a data controller-centric approach to a data subject-centric approach. This shift has provoked criticism due to the potential jurisdictional overreach of EU law based on its extraterritorial effect.<sup>94</sup> The impact of this shift on the revision of the e-Privacy Directive will be interesting to observe – from a fundamental rights standpoint, this approach can be lauded as serving to ensure a higher level of protection; however, it is still to be seen how the international community and industry will react to these changes. For users located in the EU, this means that all websites they access which monitor their behaviour, for example, in the context of behavioural advertisement, must comply with the EU data protection framework.

### 3.3. Triggering Article 5(3) and the Regulation of Technical Means of User Tracking

Entities which access users’ terminal equipment in order to obtain data stored in the equipment or to store information on it, must obtain prior consent from users. The act of accessing a users’ terminal equipment for the purpose of tracking occurs through various technical means that were outlined above in Section 2.3.E. According to the Article 29 Working Party, cookies fall within the scope of Article 5(3) of the e-Privacy Directive and thus require prior notification and user consent.<sup>95</sup> The requirement for a transfer of information in Article 5(3) of the e-Privacy Directive<sup>96</sup> is triggered by the fact that by visiting a website, a cookie is placed in a user’s browser – an act of storing information on the user’s terminal equipment and accessing that information at a later stage. It must be stressed that following Recital 24 of the Preamble to the e-Privacy Directive, the scope of the information required to trigger Article 5(3) of the e-Privacy Directive is potentially much wider than what is defined as personal data in the DPD; it applies to ‘any information stored on [the user’s] equipment [and which is] of the private sphere of the user’.<sup>97</sup> However, in most Member States,

---

<sup>94</sup> See, among many, the special issue of *International Data Privacy Law* containing contributions by D.J.B. Svantesson, ‘Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation’, 5 *IDPL* (2015); C. Kuner, ‘Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law’, 5 *IDPL* (2015); M. Taylor, ‘The EU’s human rights obligations in relation to its data protection laws with extraterritorial effect’, 5 *IDPL* (2015) and M. Brkan, ‘Data protection and European private international law: observing a bull in a China shop’, 5 *IDPL* (2015).

<sup>95</sup> Opinion 2/2010 of the Article 29 Working Party on online behavioural advertising, 22.6.2010, WP 171, p. 13.

<sup>96</sup> I.e.: ‘the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user’.

<sup>97</sup> See Opinion 2/2010 of the Article 29 Working Party on online behavioural advertising, 22.6.2010, WP 171, p. 9; D. Clifford, ‘EU Data Protection Law and Targeted Advertising – Consent and the Cookie Monster – Tracking



identifiers such as cookies or ID-numbers are considered personal data, meaning that the distinction found in the two instruments is arguably small.<sup>98</sup> With the GDPR, the scope of the notion of ‘personal data’ has been broadened to explicitly encompass these forms of data.<sup>99</sup>

Yet, not all cookies require prior informed consent. The Article 29 Working Party differentiates between 1<sup>st</sup> and 3<sup>rd</sup> party cookies that are used for commercial purposes, such as user tracking for online advertisement, and 1<sup>st</sup> party cookies that are strictly necessary for the functioning of a website or to improve a service as stated in the last sentence of Article 5(3) of the e-Privacy Directive.<sup>100</sup> This exception only applies either for cookies following the ‘sole purpose of carrying out the transmission of communication (...)’ or those which are ‘strictly necessary in order to provide an information society service explicitly requested by the subscriber or user to provide the service’.<sup>101</sup>

Furthermore, the exception is only applicable to the consent requirement; controllers must still inform users of these cookies. 3<sup>rd</sup> party advertising cookies do not fall under either exception and therefore fully trigger the prior informed consent requirement.<sup>102</sup>

In cases where cookies follow multiple purposes, one of which falls outside the category of strict technical necessity, the prior informed consent requirement in Article 5(3) of the e-Privacy Directive still applies. Therefore, it is not possible to pass off dual purpose cookies to users under the exception included in the last sentence of Article 5(3) of the e-Privacy Directive.

A similar verdict was reached for browser fingerprinting, as the findings of the Article 29 Working Party ‘[do] not exclusively apply to cookies but [are] also applicable to “similar technologies”’.<sup>103</sup> Originally, Article 5(3) of the e-Privacy Directive did not envision other, more passive, means of tracking such as browser fingerprinting, which work by analysing the various data transmitted by a user’s browser – data that are transmitted without the website accessing or storing information in the user’s browser. In this regard, the scope of the provision has been broadened with the enactment of the Citizen’s Rights Directive in 2009.<sup>104</sup>

---

the crumbs of online user behaviour’, 5 *Journal of Intellectual Property, Information Technology and E-Commerce Law* (2014), margin note 27.

<sup>98</sup> E.g. in Germany, both under the implementation act of the e-Privacy Directive - the Federal Data Protection Act (*Bundesdatenschutzgesetz*; BDSG) - and in the upcoming GDPR. See N. Härting, *Datenschutzgrundverordnung – Das neue Datenschutzrecht in der betriebliche Praxis* (Otto Schmidt Verlag, 2016), margin note 275 et seq.

<sup>99</sup> Article 4(1) and Recital 30 of the Preamble to the GDPR.

<sup>100</sup> Recital 66 of the Preamble to the e-Privacy Directive. See also Opinion 4/2012 of the Article 29 Working Party on Cookie Consent Exception, 7.6.2012, WP 194.

<sup>101</sup> Article 5(3) of the e-Privacy Directive, last sentence.

<sup>102</sup> Opinion 4/2012 of the Article 29 Working Party on Cookie Consent Exception, 7.6.2012, WP 194, p. 9-10.

<sup>103</sup> Opinion 9/2014 of the Article 29 Working Party on the application of Directive 2002/58/EC to device fingerprinting, 25.11.2014, WP 224, p. 3.

<sup>104</sup> See E. Kosta, *Consent in European Data Protection Law*, p. 294-295.

The Article 29 Working Party explicitly acknowledges that browser fingerprinting is being sought out as a means to circumvent Article 5(3) of the e-Privacy Directive, being overall more difficult to detect.<sup>105</sup> Unlike cookies, it is harder to argue from a technical perspective that browser fingerprinting triggers the obligations in Article 5(3) of the e-Privacy Directive since browser fingerprinting works passively by reading the data that is sent by the browser for mostly technical reasons.<sup>106</sup> Therefore, the activity of storing information on the user's terminal equipment does not occur, unlike with cookies, where a small file is placed in the user's browser.

It becomes more complicated when considering the alternative requirement triggered by the 'gaining of access to information already stored' in the user's terminal equipment. Does the act of retrieving the data broadcasted by the user's web browser trigger Article 5(3) of the e-Privacy Directive?<sup>107</sup> The Article 29 Working Party opines that the utilization of the various identifying elements that are transmitted by the user and which are used to single out, link or infer a user indeed trigger the obligations set out in Article 5(3) of the e-Privacy Directive.<sup>108</sup> It concludes that the combination of those elements can produce a 'sufficiently unique' fingerprint to identify an individual and thus fall within the category of personal data.<sup>109</sup> Additionally, elements such as IP addresses that are used in this process are also deemed personal data.<sup>110</sup> This was recently affirmed by Advocate General Sánchez-Bordona in *Breyer*.<sup>111</sup> However, final clarification on this subject is still missing as the final judgment has not yet been issued by the CJEU.

Additionally, mirroring the distinction between 1<sup>st</sup> and 3<sup>rd</sup> party cookies, the *telos* of employing the retrieved data in the context of browser fingerprinting is not strictly technical – and therefore cannot be excused as per the last sentence of Article 5(3) of the e-Privacy Directive – if it is employed as a technical means to circumvent the obligations contained in Article 5(3) of the e-Privacy Directive. An overly formalistic reading of the wording of the article would impede and undermine the effectiveness of the fundamental right to data protection. Hence, drawing on the spirit of the law and focusing on the fundamental rights dimension of the EU data protection framework - as was the case in *Google Spain* - leads to the conclusion that browser fingerprinting triggers the application of Article 5(3) of the e-Privacy Directive.

---

<sup>105</sup> Opinion 9/2014 of the Article 29 Working Party on the application of Directive 2002/58/EC to device fingerprinting, 25.11.2014, WP 224, p. 4.

<sup>106</sup> See on the technical description, Opinion 9/2014 of the Article 29 Working Party on the application of Directive 2002/58/EC to device fingerprinting, 25.11.2014, WP 224, p. 4-6.

<sup>107</sup> N.B., from a technical standpoint, the browser must send this data in order to properly display a website.

<sup>108</sup> Opinion 9/2014 of the Article 29 Working Party on the application of Directive 2002/58/EC to device fingerprinting, 25.11.2014, WP 224.

<sup>109</sup> *Ibid.*, p. 6.

<sup>110</sup> *Ibid.*

<sup>111</sup> Opinion of Advocate General Sánchez-Bordona in Case C-582/14 *Patrick Breyer v. Federal Republic of Germany*, EU:C:2016:339. The judgment has not been rendered at the time of writing.

In a similar matter, the Commission recently answered in the affirmative, a request sent by an online activist on whether websites retrieving and analysing transmitted browser data to detect ad blocking applications<sup>112</sup> triggers Article 5(3) of the e-Privacy Directive, further underlining that the EU data protection framework applies to the use of types of browser and device data which are not strictly used for technical means but which fall within the user's 'private sphere'.<sup>113</sup> This is the case even although the data is broadcasted from the browser (for technical purposes) and the processing takes place in the controller's devices and not in the user's terminal equipment.<sup>114</sup>

The e-Privacy Directive also refers to other tracking technologies in Recital 23 of the Preamble to the 2002 version of the e-Privacy Directive, explicitly mentioning 'spyware, web bugs, hidden identifiers and other similar devices', indicating that their use is permissible 'only for legitimate purposes, with the knowledge of the users concerned'. Recital 24 of the Preamble to the 2002 version of the e-Privacy Directive then links these tracking tools to the requirements that apply to cookies. Hence, the requirements illustrated above also apply to these tools.<sup>115</sup> In effect, the EU data protection framework encompasses the prevalent tracking technologies.

### 3.4. Obtaining Consent – Who and How

The allocation of the duty to provide users with information, in order to obtain informed consent, in the context of targeted behavioural advertising is complex. On the one hand, the Article 29 Working Party opines that the obligation to obtain consent before accessing users' terminal equipment falls on the ad network provider since ad network providers rent space from websites and receive a portion of control over the websites in their ad network (i.e. the ability to place cookies or other technical means of tracking and displaying ads). Further, they have complete control over the processing of personal data in their ad network (i.e. creating user profiles, targeting ads).<sup>116</sup>

On the other hand, the classification of a website publisher vis-à-vis EU data protection law is not clear cut: although website publishers 'rent out' and therefore cede power over certain parts of their website to ad network providers, they are the ones ultimately in control of the website, and they therefore control how the personal data of users will be handled. This situation is particularly complex when considering the various forms of user tracking that can

---

<sup>112</sup> More specifically, it refers to an ad-blocking browser extension such as those mentioned above in Section 2.E.2.g.

<sup>113</sup> See Opinion 2/2010 of the Article 29 Working Party on online behavioural advertising, 22.6.2010, WP 171, p. 9.

<sup>114</sup> Letter of Mr Hanff to the President of the European Commission Jean-Claude Juncker of 25 February 2016. On file with the author.

<sup>115</sup> See on this also, E. Kosta, *Consent in European Data Protection Law*, p. 293-294.

<sup>116</sup> Opinion 2/2010 of the Article 29 Working Party on online behavioural advertising, 22.6.2010, WP 171, p. 10.

be applied in the context of targeted behavioural advertising;<sup>117</sup> the more involved the website publisher is in transferring personal data of users that the ad network provider is unable to obtain directly through being granted partial control of the website, the more likely the website provider can be classified as a joint controller together with the ad network provider.<sup>118</sup>

This leaves the question how consent can effectively be obtained from the user. Article 5(3) of the e-Privacy Directive prescribes that consent must be obtained (i) prior to accessing the user's equipment, (ii) must be informed and (iii) consent must be freely given. The following sub-sections elaborate on the necessary requirements.

### 3.4.1. The Act Required to Give Consent

According to the Article 29 Working Party, the act of rendering consent is not clearly defined but must be active and must follow the presentation of clear information to the user; consent cannot be implied or presumed and has to entail a clear affirmative action following an act of communication between the controller(s) and the user.<sup>119</sup> Following this rationale, it is not possible to adduce or presume the user's consent from their browser settings.<sup>120</sup> This means that users have to actively opt in, in order for website publishers and ad network providers to access the user's terminal device (for example by clicking a non-preselected box).

The reason mentioned in the Opinion by the Article 29 Working Party is that consent implies an affirmative action; having a browser setting that accepts all cookies or other tracking means by default does not fulfil this requirement, as consent has to be obtained in every single instance of processing in case the obligation is triggered.<sup>121</sup> Conversely, compliance with Article 5(3) of the e-Privacy Directive is valid in circumstances where the browser setting rejects all tracking by default (for example, Do-Not-Track).

Much of the current problems with the e-Privacy Directive in this regard can be attributed to the lack of harmonization. The amendment of the e-Privacy Directive by the 2009 Citizen's Rights Directive complicated the matter and failed to eliminate the divergence in implementation, amongst the Member States, of the opt-in requirement in Article 5(3) of the e-Privacy Directive.

#### 3.4.1.1 The 2002 e-Privacy Directive – Opt-Out

---

<sup>117</sup> See Section 2.E.2. above.

<sup>118</sup> Opinion 2/2010 of the Article 29 Working Party on online behavioural advertising, 22.6.2010, WP 171, p. 11. See also, D. Clifford, 5 *Journal of Intellectual Property, Information Technology and E-Commerce Law* (2014), margin note 20-23.

<sup>119</sup> Opinion 15/2011 of the Article 29 Working Party on the definition of consent, 13.7.2011, WP187, p. 9-10.

<sup>120</sup> Opinion 2/2010 of the Article 29 Working Party on online behavioural advertising, 22.6.2010, WP 171, p. 13.

<sup>121</sup> *Ibid.*, p. 14.

The 2002 version of the e-Privacy Directive stated that users shall be ‘offered a right to refuse’ and shall be ‘provided with clear and comprehensive information in accordance with Directive 95/46/EC’ about the processing. This wording can be construed to merely require an opt-out from users (right to *refuse* processing), while it also does not warrant for the condition of *prior* information of users.<sup>122</sup> During the negotiations of the 2002 Directive, the condition of prior informed consent was proposed by the European Parliament but was met with resistance by business groups and was ultimately watered down to the right to refuse by the Council.<sup>123</sup> For the implementation of the 2002 e-Privacy Directive, Member States could therefore rely on the right to refuse, leading to multiple Member States adopting opt-out regimes.<sup>124</sup>

### 3.4.1.2. The 2009 Citizens Rights’ Directive – Opt-In, but with Problems

After tense negotiations, the 2009 Citizens Rights’ Directive finally introduced the prior consent requirement for Article 5(3) of the e-Privacy Directive.<sup>125</sup> The first reading by the European Parliament included wording that enables the use of browser settings for the determination of user consent, however this was ultimately omitted.<sup>126</sup> The idea of consent informed by browser settings however persisted in the form of Recital 66 of the Preamble to the amended e-Privacy Directive.<sup>127</sup> This, in turn led to a fragmented system among Member States where some Member States accept technical settings such as browser settings as valid forms of consent whereas other Member States rejected this form of consent and require an active role of the user.<sup>128</sup>

The complicated negotiations have resulted in legal uncertainty as to what exactly constitutes consent and has in turn spawned backlash by a number of Member States, who insisted on a right refuse (opt-out), arguing that Recital 66 can be viewed as reinforcing the pre-Citizens Rights’ Directive legal regime.<sup>129</sup> This stands in contrast with the view of the Article 29 Working Party on this matter.<sup>130</sup> In sum, the act of consenting in the context of Article 5(3) of

---

<sup>122</sup> E. Kosta, *Consent in European Data Protection Law*, p. 297-298.

<sup>123</sup> *Ibid.*, p. 299.

<sup>124</sup> European Commission, *ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation, Final Report* (European Commission, 2015), p. 57-58.

<sup>125</sup> See E. Kosta, *Consent in European Data Protection Law*, p. 300-303, for an overview of the positions of the EU institutions and the ensuing debate. The Commission and the Council in the end gave in to the demand of the European Parliament to introduce the prior informed consent requirement.

<sup>126</sup> *Ibid.*, p. 301. ‘(...) storing information or gaining access to information already stored, in the terminal equipment of a subscriber or user, either directly or indirectly by means of any kind of storage medium, is prohibited unless the subscriber or user concerned has given his/her prior informed consent, *taking into account that browser settings constitute prior consent*, and is provided with clear and comprehensive information in accordance with Directive 95/46/EC (...)’. Emphasis added.

<sup>127</sup> Recital 66 of the Preamble to the Citizen’s Rights Directive.

<sup>128</sup> European Commission, *ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation, Final Report* (European Commission, 2015), p. 63-66.

<sup>129</sup> See E. Kosta, *Consent in European Data Protection Law*, p. 303-305.

<sup>130</sup> See Opinion 2/2010 of the Article 29 Working Party on online behavioural advertising, 22.6.2010, WP 171; Opinion 15/2011 of the Article 29 Working Party on the definition of consent, 13.7.2011, WP187.

the e-Privacy Directive is still not clearly defined, however, it is clear that under the modernized framework, consent includes a form of communication and an active element by the user.<sup>131</sup>

### 3.4.1.3. The GDPR as a Possible Alternative?

The GDPR will introduce its own system of coping with the tracking of users' behaviour and it might well be that the new e-Privacy regime will not include specific provisions on the matter anymore as these might become redundant if the EU legislator decides there is no added value to have a regime next to the GDPR.<sup>132</sup> The reason for this is that the e-Privacy Directive has arguably missed its mark: the lack of harmonization and the ineffectiveness of the notices required after the amendment did not enact the change so desired by the legislator.<sup>133</sup> It must also be recalled that the 2002 e-Privacy Directive and the amendment by the 2009 Citizens Rights' Directive were aimed at rectifying the regulatory gaps that originated through the rise of online technologies for which the DPD, which was passed in 1995 and had to be transposed by Member States by 1998, was simply outdated.

For targeted behavioural advertising, Article 6 of the GDPR serves to replace Article 5(3) of the e-Privacy Directive in order to regulate the tracking of users. As outlined above, Article 4(1) together with Recital 30 of the Preamble to the GDPR cover a wide range of tracking tools under the notion of 'personal data'. Article 6(1)(a) of the GDPR would serve as a legal basis utilizing consent for all tracking tools that are not strictly necessary, whereas tracking tools such as technical cookies which are necessary to provide a requested service could fall under Article 6(1)(b) of the GDPR. Lastly, Article 6(1)(f) of the GDPR would encompass tracking tools that serve a security purpose.

This approach fits well with the differentiation made by the Article 29 Working Party.<sup>134</sup> Yet, with the revision of the e-Privacy Directive looming on the horizon, it is not certain whether the GDPR will be a replacement or whether the new e-Privacy Directive will serve to add more granularity to the EU data protection framework applicable to targeted behavioural advertising.

### 3.4.2. Freely Given Consent

---

<sup>131</sup> C. Markou, 'Behavioural Advertising and the "New Cookie Law" as a Victim of Business Resistance and a Lack of Official Determination', in S. Gutwirth, R. Leenes and P. de Hert (eds.), *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection* (Springer, 2016), p. 222-225.

<sup>132</sup> See ETNO, Study on the ePrivacy Directive (DLA Piper, 2016), p. 29-30.

<sup>133</sup> *Ibid.*, p. 29.

<sup>134</sup> See Opinion 04/2012 of the Article 29 Working Party on Cookie Consent Exemption, 7.6.2012, WP 194.

The act of making use of a website or online service contingent on the acceptance of cookies has led to the emergence of so-called 'cookie walls'.<sup>135</sup> This occurs when a website blocks access in cases where users do not accept all cookies, including 3<sup>rd</sup> party advertising cookies. Publishers may argue that websites require the revenue created from tracking and advertising to offset costs for providing content and for generating revenue; therefore, accepting cookies is viewed as necessary in the eyes of publishers in exchange for the services they offer.

Yet, in the context of Article 5(3) of the e-Privacy Directive, this resulted in claims that the requirement of *freely given* consent is not met, the underlying argument being that users are coerced into accepting cookies and do not do so by their free volition. Leenes and Kosta speak of a regulatory failure in this regard, citing the example of the Dutch transposition of the law: through creative compliance on behalf of the website publishers and the lack of appropriate enforcement tools for the regulator, website publishers were 'able to create an unusual alliance with the targets (victims) or profiling against their protectors (the regulator)'.<sup>136</sup>

Article 7(4)<sup>137</sup> read together with Recital 42, sentence 5<sup>138</sup> and Recital 43, sentence 2<sup>139</sup> of the Preamble to the GDPR might be able to remedy the situation. In the context of targeted behavioural advertising, user consent under the GDPR is invalid if access to a website is made dependent on consenting to the processing of personal data that is not strictly necessary (i.e. tracking for advertising purposes). In cases where the user is confronted with situations where there is 'no genuine choice', such as cookie walls, it must therefore be presumed that consent is not valid.<sup>140</sup>

### 3.4.3. Informing Users

Website publishers and ad network providers are required to provide users with the necessary information pursuant to Article 5(3) of the e-Privacy Directive and the information provisions in the DPD (and once it enters into force, the GDPR) before placing tracking tools

---

<sup>135</sup> See e.g., EPDS, Opinion 5/2016 Preliminary EDPS Opinion on the review of the ePrivacy Directive (2002/58/EC), 22.7.2016, p. 14; R. Leenes and E. Kosta, 'Taming the Cookie Monster in Dutch Law – A Tale of Regulatory Failure', 31 *Computer Law & Security Review* (2015); N. Helberger, 'Freedom of Expression and the Dutch Cookie-Wall', *SSRN* (2013), [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2351204](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2351204).

<sup>136</sup> R. Leenes and E. Kosta, 31 *Computer Law & Security Review* (2015), p. 331. See more recently, E. Kosta, 'The Netherlands – The Dutch Regulation of Cookies', 2 *EDPL* (2016).

<sup>137</sup> Article 7(4) of the GDPR: 'When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract'.

<sup>138</sup> Recital 42, sentence 5 of the Preamble to the GDPR: 'Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment'.

<sup>139</sup> Recital 43, sentence 2 of the Preamble to the GDPR: 'Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance'.

<sup>140</sup> See N. Härting, *Datenschutzgrundverordnung – Das neue Datenschutzrecht in der betriebliche Praxis*, margin note 385 et seq.

on the end-user's terminal equipment. In this context, it is important to question (i) what information must be displayed to the user and (ii) how this information should be displayed to the user.

### 3.4.3.1 What Information Must the User Receive?

Article 5(3) of the e-Privacy Directive makes reference to the DPD regarding the information users must receive. Article 10 of the DPD is the provision that is key for targeted behavioural advertising. It states that:

Member States shall provide that the controller or his representative must provide a data subject from whom data relating to himself are collected with at least the following information, except where he already has it:

- a) the identity of the controller and of his representative, if any;
- b) the purposes of the processing for which the data are intended;
- c) any further information such as
  - the recipients or categories of recipients of the data,
  - whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply,
  - the existence of the right of access to and the right to rectify the data concerning himin so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.

Next to this information, website publishers are required to inform users when they use cookies or wish to track users by others means.<sup>141</sup>

Replacing the DPD, the scope of the information that users must receive is broadened under Article 13 of the GDPR. The provision adds the following items that must be included in the notice: information on the data protection officer (where applicable); the legal basis for the processing (for example, consent, legitimate interest, and so on); if data is collected for security reasons, the legitimate interest pursued for the processing; whether the controller intends to transfer data to third countries and if so, by what legal means; the period of storage of the data; in cases where consent is used as the legal basis, information on the right to withdraw and its legal consequences; if automated decision-making is utilized, meaningful information on the mechanisms and the logic involved in the decision-making process.

---

<sup>141</sup> Opinion 16/2011 of the Article 29 Working Party on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising, 8.12.2011, WP 188.



The two most striking features that may improve user control over targeted behavioural advertising are the indication of the legal basis and whether the data controller uses automated decision-making. Since the legal basis for targeted behavioural advertising will rest on the consent requirement, users will be informed about the possibility to deny their consent and the consequences thereof. Coupled with the prohibition of cookie walls, this has the effect of strengthening the users' position vis-à-vis website publishers and ad network providers. Since the matching that takes place between users and ads is an automated process, it is also a requirement that users are made aware of this.

The GDPR thus adds a number of relevant items to the notice that aim at empowering users.

#### 3.4.3.2. How Should the Information Be Presented?

Initially, the presentation of the information described above was done by including a segment on data protection in the general notice of the website.<sup>142</sup> In terms of visibility, this meant that users would be tracked by virtue of accessing a website and could only opt out after searching and finding the right provision in the general notice. Hence, users had to click through to the notice, which usually could be found by following a link on the start page of a website. The user then had to navigate to the relevant provision regarding cookies and tracking.

Already in 2004, the Article 29 Working Party published an Opinion on the need for more harmonized information provisions.<sup>143</sup> After having issued an Opinion on the minimum information requirements for the Internet, the Article 29 Working Party noted that the level of harmonization achieved in the Member States was insufficient and national transposing laws varied considerably.<sup>144</sup> Four major points were mentioned in this context: (i) '[t]he need to facilitate compliance across the EU'; (ii) '[t]he need to improve citizen's awareness of data protection rights'; (iii) '[t]he need to present information with meaningful, and appropriate content to the data collection situation' and (iv) '[t]he need to improve the quality of data protection from the individuals' perspective'.<sup>145</sup>

To achieve these goals, the Article 29 Working Party proposed to (i) simplify the language used in notices; (ii) a multi-layered format of notices, where the first layer ('short notice') would provide the reader with a brief, plain-language description of 'core information'; the second layer ('condensed notice') would offer a more thorough description and the items required in the DPD, still in plain language; and the third layer would provide the full technical

---

<sup>142</sup> Opinion 2/2010 of the Article 29 Working Party on online behavioural advertising, 22.6.2010, WP 171, p. 13-16.

<sup>143</sup> Opinion 10/2004 of the Article 29 Working Party on More Harmonised Information Provisions, 25.11.2004, WP 100.

<sup>144</sup> *Ibid.*, p. 3-4, with reference to the implementation report and the technical analysis of the transposition of the DPD.

<sup>145</sup> *Ibid.*

description that was often the standard in the early notices and (iii) lastly, Member States should be enabled to legalize this approach as long as there is consistency between the different layers and the application of the layered approach to notices ensures their effectiveness.<sup>146</sup>

In 2009, the Citizens Rights' Directive mandated that *prior* informed consent is required; thus, users must be provided with the relevant information before being tracked. In an Opinion published in 2011 following the proposal of a self-regulatory code of compliance by two big online advertising industry representatives, the Article 29 Working Party criticized the code for not complying with the new directive.<sup>147</sup> The Opinion included a clarification mandating that additional notices for cookies should be in place on websites.<sup>148</sup> The Article 29 Working Party suggested that this information should be provided by pop-up screens or alternatively by static information banners on top of the website, splash screens that appear when entering a website or technical settings that block cookies until users opt in and allow the setting of cookies.<sup>149</sup>

Since the GDPR is set to replace the DPD, the presentation of information required in Article 5(3) of the e-Privacy Directive which makes direct reference to the provisions of the DPD will also be altered to follow the rules of the GDPR. A first novelty is that the plain-language requirement is now prominent in the GDPR. Article 12(1) of the GDPR mandates that

[t]he controller shall take appropriate measures to provide any information (...) relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means.

The requirement that was found in the Article 29 Working Party Opinions has now found its way into an instrument of secondary EU law.

A further novelty of the GDPR is the introduction of icons and machine-readable text. Article 12(7) of the GDPR states that the information required 'may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing'. It further states that 'where the icons are presented electronically they shall be machine-readable'.

---

<sup>146</sup> Ibid., p. 7.

<sup>147</sup> Opinion 16/2011 of the Article 29 Working Party on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising, 8.12.2011, WP 188.









<sup>148</sup> Ibid.

<sup>149</sup> Ibid., p. 9-10.

The inclusion of these icons in the GDPR can be traced back to the Draft Report of the LIBE Committee of the European Parliament from 21 November 2013 (Figure 4).<sup>150</sup> In the end, the draft icons were not included in the final version of the GDPR, however, Article 12(8) GDPR grants the Commission the right to adopt delegated acts ‘for the purpose of determining the information to be presented by the icons and the procedures for providing standardised icons’.

Figure 4 – Draft icons

*Annex 1 - Presentation of the particulars referred to in Article 13a (new)*  
 1) Having regard to the proportions referred to in point 6, particulars shall be provided as follows:

ICON	ESSENTIAL INFORMATION	FULFILLED
	No personal data are <b>collected</b> beyond the minimum necessary for each specific purpose of the processing	
	No personal data are <b>retained</b> beyond the minimum necessary for each specific purpose of the processing	
	No personal data are <b>processed</b> for purposes other than the purposes for which they were collected	
	No personal data are <b>disseminated</b> to commercial third parties	a)
	No personal data are <b>sold or rented out</b>	
	No personal data are retained in <b>unencrypted</b> form	b) 

Source: EP Draft Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), Committee on Civil Liberties, Justice and Home Affairs, A7-0402/2013, 21.11.2013, ANNEX 1

### 3.5. Conclusion

The complex legal framework that applies to targeted behavioural advertising mandates that users receive all relevant information in an understandable manner, prior to giving consent

<sup>150</sup> European Parliament, Draft Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), Committee on Civil Liberties, Justice and Home Affairs, A7-0402/2013, 21.11.2013, ANNEX 1, p. 194-195.

to being tracked (i.e. informed consent). Consent must also be freely given, which consequently prohibits cookie walls. Even in its amended form, the e-Privacy Directive has failed to create an EU-wide harmonized framework on what exactly constitutes consent and by which means it should be given.

The GDPR is set up to potentially replace the e-Privacy Directive to regulate the tracking of users; it adds clarification to the notion of consent, which is nevertheless still an ambiguous concept. In any case, the GDPR will replace the DPD and thus the information provision required by the link in Article 5(3) of the e-Privacy Directive to the DPD. Here, the GDPR offers users more information and aims at creating simpler notices. The territorial scope of application of the GDPR is clearer than that of the e-Privacy Directive. It is not clear how the substantive scope in the GDPR and the e-Privacy Directive square off – i.e. the notion of ‘personal data’ in the GDPR compared to the notion of ‘information’ in the e-Privacy Directive.

## 4. A Critical Reflection on Notice and Consent as a Regulatory Tool<sup>151</sup> for Targeted Behavioural Advertising

The EU data protection framework dealing with targeted behavioural advertising is complex and its effectiveness is questionable. As was illustrated above, the regulatory tool utilized in this area is notice and consent. At the time of writing, the final version of the GDPR has been published and the preliminary findings of the public consultation for the review of the e-Privacy Directive are available.<sup>152</sup> It is therefore necessary to reflect on the role of notice and consent in the form of the requirement of prior informed consent for targeted behavioural advertising and its usefulness as a regulatory tool in the light of adequately informing users.

### 4.1. The Reasons Notice and Consent Fails

The starting point in analysing the efficacy of notice and consent for targeted behavioural advertising must be to look at what users know about the practice, their inclination towards it and how they interact with websites that utilize targeted behavioural advertising. It becomes clear that users are faced with both systemic as well as individual issues when confronted with notice and consent for targeted behavioural advertising. These issues will be analysed in this subsection, followed by the examination of tools and techniques to address these issues.

#### 4.1.1. Why is Notice and Consent Used?

---

<sup>151</sup> The term ‘regulatory tool’ to describe notice and consent was taken from C. Sunstein, ‘Empirically Informed Regulation’, 78 *University of Chicago Law Review* (2011), p. 1417.

<sup>152</sup> Website of the European Commission, <https://ec.europa.eu/digital-single-market/en/news/eprivacy-directive-commission-launches-public-consultation-kick-start-review>.

One of the basic questions to be asked is why notice and consent is such a pervasive regulatory tool, especially in the online environment. One reason that notice and consent is used is due to its cost: it is a cheap regulatory tool as it delegates responsibility from legislators to draw up detailed rules, to individuals, who are then tasked with managing their affairs.<sup>153</sup> Other reasons might be that the cost for drawing up detailed regulation is very high and that the speed of innovation quickly makes such detailed regulation obsolete. A different reason might be that there is a lack of societal or political consensus; if there is no clear goal, it becomes difficult to formulate legal intervention to ascertain these goals. In this respect, one needs to mention that there is also an underlying political dimension in that there must be a decision on how paternalistic the regulator wishes to be in forming a legal response. If there is no such consensus, notice and consent might be viewed as the smallest common denominator. This could be a reason for opting for the option of having and keeping notice and consent as a legal basis in the EU data protection framework, as in highly technical fields such as targeted behavioural advertisement there are also distributive consequences of regulation that has been noticed by industry. The intense lobbying surrounding the drafting of the GDPR might point in this direction.<sup>154</sup>

Further, considerations of innovation could play a role since pre-emptively restricting a certain technology or process may arguably hinder innovation. In addition, legislators tend to require some time to adapt to changes – given the rapid pace of innovation in digital markets, the gap in time that the legislator must bridge to catch up seems daunting. In sum, there are many possible reasons for why the legislator opted for including notice and consent and further research is needed – currently the reasons sketched out above are mere conjectures. However, what is clear is that the effect of relying on informed consent for new technologies has adverse effects on individuals.

#### 4.1.2. Individual and Systemic Problems with Notice and Consent

The informed consent requirement in the EU data protection framework has been under intense scrutiny for some time now. Research shows that individuals have problems with informed consent, which is a form of notice and consent that is specific to the EU data protection framework (as has been highlighted above). The biggest problem seems to be that individuals have difficulty understanding these notices and the underlying complex processes

---

<sup>153</sup> O. Ben-Shahar and C.E. Schneider, *More Than You Want To Know – The Failure of Mandated Disclosure* (Princeton University Press, 2014), Ch. 9.

<sup>154</sup> See the famous quote by W. Long, 'Significant Impact of New EU Data Protection Regulation on Financial Services', *Global Banking & Financial Review* (2014), <https://www.globalbankingandfinance.com/significant-impact-of-new-eu-data-protection-regulation-on-financial-services/>: 'Due to its potential impact, the proposed Regulation has been one of the most lobbied pieces of European legislation in European Union history'. An examination of the lobbying patterns was performed by E. Özlem Atikcan and A.W. Chalmers, 'The Business of Internet Privacy: Interest Group Lobbying and the European Union's General Data Protection Regulation', *European Consortium for Political Research (ECPR)* (2016), <https://ecpr.eu/Filestore/PaperProposal/292751a0-218d-4af9-a574-ff3298e7bcca.pdf>.

that revolve around the collection and use of their personal data. The issues individuals have can be roughly separated into individual problems and systemic problems.

For the scope of this inquiry, individual problems are defined as problems pertaining to the individual user and are based on qualities inherent to the user. Examples are that users lack the necessary knowledge or awareness about processes used in targeted behavioural advertisement; they do not take action or proactively protect their personal data; they lack the necessary skills, such as a sufficient level of literacy to understand notices; or they suffer from an array of biases that obstruct their decision-making processes. These are all problems characterized by their close connection with the individual user.

Systemic problems are problems that are not *directly* linked to the interaction with individuals or the individual's inherent qualities, but that focus on issues in the organization of a wider system. Examples of this are the sheer amount of notice and consent situations that individuals face on a daily basis as well as the length of notices they are confronted with; and the lack of options in consent – i.e. most offers for online services work under a take-it-or-leave-it mentality.

The above distinction is not clear-cut and the individual still plays a role in systemic problems. Yet, this distinction might help in addressing these issues and in finding possible solutions to the underlying problems with the informed consent requirement for targeted behavioural advertisement. Further, it must be mentioned that the distinction between systemic and individual problems in this context does not denote a distinction between problems that occur often and problems that only occur to a limited number of individuals. As will be illustrated below, both problems are pervasive.

### 4.1.3. The Adverse Effects of Notice and Consent for Individuals

#### 4.1.3.1. Individual Problems

An array of surveys from the EU and the US show that most users are not aware what user tracking, profiling and targeted behavioural advertising is.<sup>155</sup> Users usually lack the knowledge about some of the most basic functions and processes of the Internet; therefore, it seems impossible for individuals to understand complex processes involving their personal data when the basic knowledge is already missing.<sup>156</sup> In this respect, the digital environment is

---

<sup>155</sup> See among many, European Commission, Data Protection in the European Union: Citizens' perceptions – Analytical Report, Flash Eurobarometer Series no. 225, 2008, p. 26 et seq.; European Commission, Attitudes on Data Protection and Electronic Identity in the European Union, Special Eurobarometer 359, 2011; European Commission, Data Protection Report, Special Eurobarometer 431, 2015, p. 58, 81 et seq.; F.J. Zuiderveen-Borgesius, *Improving privacy protection in the area of behavioural advertising* (PhD Thesis, IViR UV Amsterdam, 2014), p. 253-257 and the footnotes therein.

<sup>156</sup> A. Smith, *What Internet Users Know about Technology and the Web – The Pew Research Center's 'Web IQ' Quiz* (PEW, 2014).

prone to add to this problem. Palfrey notes on the rapid development and innovation of digital technologies that:

The final problem is that it is very difficult for the citizen to keep up with the pace of technological change. The rate of development of new digital technologies is very fast, such that even technology experts have little sense of what is even commercially available in fields tangentially related to their own. Few people would be knowledgeable enough about digital technologies to have an effective sense of what information they are sharing is publicly accessible and what is private.<sup>157</sup>

Seldom do users know that targeted behavioural advertising exists and if they do know about it, they usually only have a vague sense of what it is but do not fully understand its complexities, marking a stark information asymmetry between users and data controllers.<sup>158</sup> In one survey, users were confronted with tracking practices that are utilized in the context of targeted behavioural advertising and even doubted that these practices were legal.<sup>159</sup> In most surveys, users in the US and the EU who were confronted with the practise by a majority rejected targeted behavioural advertising, although with regional differences; only a small percentage held a positive stance towards the practice.<sup>160</sup> When reading notices, users often expressed exasperation and a sense of fatalism as they cited that no matter what the notice says, they did not have control.<sup>161</sup>

It is often also the case that individuals do not read notices.<sup>162</sup> This feature is not confined to targeted behavioural advertisement or even the online environment but it is also common in the general interaction of individuals with consumer contracts.<sup>163</sup> Additionally, Ben-Shahar and Schneider refer to a 'literacy problem' as an impediment to notification.<sup>164</sup> They argue

---

<sup>157</sup> J. Palfrey, 'The Public and the Private at the United States Border with Cyberspace', 78 *Mississippi Law Journal* (2008), <http://cyber.law.harvard.edu/publications>, p. 285.

<sup>158</sup> I. Brown, 'Privacy Attitudes, incentives and behaviours', *SSRN* (2011), <http://ssrn.com/abstract=1866299>, p. 7.

<sup>159</sup> B. Ur et al., 'Smart, Useful, Scary, Creepy: Perceptions of Online Behavioural Advertising', *Proceedings of the SOUPS 2012* (2012), [http://www.cylab.cmu.edu/research/techreports/2012/tr\\_cylab12007.html](http://www.cylab.cmu.edu/research/techreports/2012/tr_cylab12007.html).

<sup>160</sup> European Commission, Data Protection in the European Union: Citizens' perceptions – Analytical Report, Flash Eurobarometer Series no. 225, 2008, p. 26 et seq.; European Commission, Attitudes on Data Protection and Electronic Identity in the European Union, Special Eurobarometer 359, 2011; European Commission, Data Protection Report, Special Eurobarometer 431, 2015, p. 58, 81 et seq.; F.J. Zuiderveen-Borgesius, *Improving privacy protection in the area of behavioural*, p. 253-257 and all footnotes therein.

<sup>161</sup> R. Heckle and W.G. Lutters, 'Re-examining User Perceptions of Online Privacy Notices: The Value of Real-Time Observation', *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)* (2005), <http://cups.cs.cmu.edu/soups/2005/2005posters/17-heckle.pdf>.

<sup>162</sup> D. Solove, 'Privacy Self-Management and the Consent Dilemma', 126 *Harvard Law Review* (2013), p. 1884.

<sup>163</sup> I. Ayres and A. Schwartz, 'The No-Reading Problem in Consumer Contract Law', 66 *Stanford Law Review* (2015).

<sup>164</sup> O. Ben-Shahar and C.E. Schneider, *More Than You Wanted To Know – The Failure of Mandate Disclosure*, Ch. 5; C. Jensen and C. Potts, 'Privacy Policies as decision-making tools: an evaluation of online privacy notices', *Proceedings of the SIGCHI conference on Human Factors in Computing Systems* (2004).

that the average user lacks the literacy required to read and, moreover, to understand notices.

Even if users were to read all notices, users' decision-making processes would still pose a problem as individuals have inherent biases and shortcomings when asked to make complex decisions. The burgeoning literature on behavioural economics often speaks of shortcomings that users have when coping with complex decision-making processes. Concepts belonging to the categories of framing, heuristics and bounded rationality have been found in relation to users' decision-making and interaction with notice and consent in the context of data protection.<sup>165</sup> Research has identified a number of cognitive shortcomings in individuals, which Ben-Shahar and Schneider tally to at least sixty different biases in the field of behavioural economics that play a role in mandated disclosure.

The cognitive shortcomings that impede the full, rational analysis of complex situations by users are replaced by so-called 'heuristics'.<sup>166</sup> These are rules of thumb based on experience, which are then used by individuals to confront the task of making complex decisions.<sup>167</sup> The term 'bounded rationality' describes the difficulty of rendering these complex decisions.<sup>168</sup>

When making these complex decisions, individuals consider data protection implications as an immaterial factor since other concerns are perceived as more important. This behaviour is called myopia and it describes the act of pursuing instant gratification while ignoring future costs that arise from this short-sighted behaviour.<sup>169</sup>

The main problem with the findings from behavioural economics is that research in this field is currently growing but it has not yet shed enough light on the matter. Next to this, the extrapolation of the findings from behavioural economics experiments on privacy and data protection is problematic and quick generalizations should be avoided. In addition, these

---

<sup>165</sup> See e.g., A. Acquisti and J. Grossklags, 'What can Behavioural economics Teach Us About Privacy?', in S. De Capitani di Vimercati et al. (eds.), *Digital Privacy - Theory, Technologies, and Practices* (Auerbach Publications, 2007); A. Acquisti et al., 'Sleights of Privacy - Framing Disclosures, and the Limits of Transparency', *Proceedings of the Ninth Symposium on Usable Privacy and Security* (2013), <http://dl.acm.org/citation.cfm?id=2501613>; A. Acquisti, 'Nudging Privacy – The Behavioural Economics of Personal Information', *IEEE Security & Privacy Economics* (2009); A. Acquisti and J. Grossklags, 'Privacy and Rationality in Individual Decision Making', *IEEE Security and Privacy* (2005). Zuiderveen-Borgesius makes use of a number of findings from behavioural economics and applies these to targeted behavioural advertisement, see F.J. Zuiderveen-Borgesius, *Improving privacy protection in the area of behavioural advertising*, p. 286-293.

<sup>166</sup> D. Solove, 126 *Harvard Law Review* (2013), p. 1887; R.H. Thaler and C. Sunstein, *Nudge – Improving decisions about health, wealth and happiness* (Penguin Books, 2009), p. 24 et seq.

<sup>167</sup> R.H. Thaler and C. Sunstein, *Nudge – Improving decisions about health, wealth and happiness*, p. 24 et seq.

<sup>168</sup> *Ibid.*

<sup>169</sup> F.J. Zuiderveen-Borgesius, *Improving Privacy Protection in the area of Behavioural Targeting* (UVA, PhD Thesis, 2014), p. 291.



findings seldom warrant solutions – they point out problems but further research is necessary to identify an effective remedy.<sup>170</sup>

Nevertheless, behavioural economics can serve the function of adding critical thought to the analysis of notice and consent and may prove as a valid starting point for further empirical inquiry into the matter.<sup>171</sup> In the debate surrounding notice and consent, Ben-Shahar and Schneider attribute less weight to the findings of behavioural economics to the solving of legal problems.<sup>172</sup> They note that behavioural economics deals with the decision-making process within users, but cannot give solutions for the literacy problem or the problem with the sheer amount of notices users are confronted with.<sup>173</sup> Additionally, the number of biases and mental shortcomings that were identified let Ben-Shahar and Schneider doubt that there will be a means to overcome all of them.<sup>174</sup> Lastly, there is no average user – therefore, there will also not be a one-size-fits-all solution as to how information should be presented as too many factors such as education, age, technological affinity, culture, current mood or temper, and so on weigh in on the decision-making process.<sup>175</sup>

In light of the foregoing, a phenomenon described as the ‘privacy-paradox’ has been observed.<sup>176</sup> This phenomenon describes, on the one hand, individuals’ reported high value for data protection but, on the other hand, it shows that individuals do not act according to this valuation.<sup>177</sup> The underlying reasons are a combination of the lack of knowledge of the complex processes and individuals’ cognitive problems.

#### 4.1.3.2. Systemic Problems

Alongside the various individual problems illustrated above, users are also faced with systemic issues. These systemic issues are not detached from the individual issues and some systemic issues that are outlined in this subsection are more closely connected to individual problems than others are.

The length of data protection notices is an impediment to users reading them. In an often-cited study by McDonald and Cranor, it was found that ‘reading privacy policies carries costs

---

<sup>170</sup> See generally the criticism by R.A. Posner, ‘Behavioural Law and Economics’, in R.A. Posner (ed.), *Frontiers of Legal Theory* (Harvard University Press, 2001).

<sup>171</sup> See O. Ben-Shahar and C.E. Schneider, *More Than You Wanted To Know – The Failure of Mandate Disclosure*, p. 113-114.

<sup>172</sup> *Ibid.*, p. 114-117.

<sup>173</sup> *Ibid.*, p. 114.

<sup>174</sup> *Ibid.*, p. 115.

<sup>175</sup> S. Elahi, ‘Privacy and Consent in the digital era’, 14 *Information Security Technical Report* (2009), p. 114.

<sup>176</sup> F.J. Zuiderveen-Borgesius, *Improving Privacy Protection in the area of Behavioural*, p. 293 et seq.

<sup>177</sup> *Ibid.*

in time of approximately 201 hours a year'.<sup>178</sup> With the GDPR, the number of items that must be included in the data protection notices for websites is also increasing.

Further, and connected to the literacy problem, notices can serve other purposes that run counter to the aim of informing users, namely to offer data controllers the broadest legal basis possible to use the personal data collected while shielding the data controller from liability. Therefore, there might be an incentive to formulate data protection notices as vague and as complex as possible in order to undermine their effectiveness.

Data controllers might even draw on tools from behavioural economics by making use of users' biases, 'nudging' them to agree to terms and utilizing framing in order to elicit the reaction the controller wants (i.e. users consenting to the collection of data), although users might be inclined to deny consent if the information would have been provided differently. The framing of disclosure and the presenting of choices is quite dependent on external factors and on the way in which information is presented. This allows data controllers to 'nudge'<sup>179</sup> individuals to disclose larger amounts of personal data.<sup>180</sup> In cases where individuals were given even greater control of their data and in which they were confronted with complex choices, data controllers were therefore able to convince individuals to disclose more personal data by using these techniques.<sup>181</sup> Therefore, the amount of personal data that individuals are willing to disclose is strongly influenced by factors surrounding the presentation of information and choice architecture.<sup>182</sup>

In such cases, it must be asked whether the regulator is able to formulate a strategy to effectively monitor websites' practices and the connected data protection notices. This is rather unlikely as this would require an in-depth analysis of the notices, the practices and processes of each website – and there are currently over 1 billion websites.<sup>183</sup> Further, this would also presuppose that there should exist a broader policy line on the regulation of targeted behavioural advertisement along with a more detailed set of rules on the use of these tools in the context of informed consent for targeted behavioural advertisement.

Related to the systemic problem of the increasing amount of notice and consent situations is Ben-Shahar and Schneider's so-called 'quantity question', which encompasses an

---

<sup>178</sup> A.M. McDonald and L.F. Cranor, 'The Cost of Reading Privacy Policies', *A Journal of Law and Policy for the Information Society* (2012), p. 562.

<sup>179</sup> R.H. Thaler and C. Sunstein, *Nudge – Improving decisions about health, wealth and happiness*.

<sup>180</sup> I. Brown, 'Privacy Attitudes, incentives and behaviours', *SSRN* (2011), <http://ssrn.com/abstract=1866299>, p. 6

<sup>181</sup> *Ibid.*, p. 5, See also O. Lynskey, *The Foundations of EU Data Protection Law*, p. 237 et seq, on the conceptual and practical shortcomings of near absolute control over personal data.

<sup>182</sup> I. Brown, 'Privacy Attitudes, incentives and behaviours', *SSRN* (2011), <http://ssrn.com/abstract=1866299>, p. 5-6. See on the notion of 'choice architecture', R.H. Thaler and C. Sunstein, *Nudge – Improving decisions about health, wealth and happiness*, p. 12.

<sup>183</sup> See Internet Live Stats, <http://www.internetlivestats.com/total-number-of-websites/>.

‘accumulation problem’ and an ‘overload problem’.<sup>184</sup> The accumulation problem describes the rising amount of notices used not only for informed consent for targeted behavioural advertising but also in other areas, both offline and online.<sup>185</sup> The use of notice and consent has become so ubiquitous that individuals cannot cope with the amassed decision they have to take in their every-day lives.<sup>186</sup> It can be argued that, especially on the Internet, the increased use of notice and consent has inevitably reached a point where information scarcity is replaced by an information overload, this information overload in turn leads to an attention scarcity in users which undermines the effectiveness of notice and consent throughout the whole system and adversely impacts the way users deal with informed consent for targeted behavioural advertisement.<sup>187</sup>

Next to this, the overload problem illustrates the failure of individuals to cope with the massive amounts of information that are by law required to be present in a single notification: its composition includes information that is not necessary but also lacks necessary information; the information is displayed in such a form that individuals are not able to ‘mentally digest’ it.<sup>188</sup>

Lastly, notices and the data usage practices connected to them are also not static. Businesses change their process over time. This can happen when a business restructures itself or in the normal wake of technological change and adaptation. Yet, in recent years, a phenomenon called ‘privacy lurches’ caught the attention of US researcher Paul Ohm.<sup>189</sup> Ohm describes this as the practice of online service providers starting by offering their service to users without collecting personal data or with a robust data protection framework but then subsequently changing their stance on the use of personal data in incremental steps<sup>190</sup> to utilize more and more personal data.<sup>191</sup> Notices are slowly and incrementally adapted to inform users of these changes. By that time, users have invested a lot of time into a service, the costs of switching

---

<sup>184</sup> O. Ben-Shahar and C.E. Schneider, *More Than You Wanted To Know – The Failure of Mandate Disclosure*, Ch. 6.

<sup>185</sup> *Ibid.*

<sup>186</sup> *Ibid.*

<sup>187</sup> See on this the works of H.A. Simon, ‘Designing Organizations for an Information-Rich World’, in M. Greenberger (ed.), *Computers, Communication, and the Public Interest* (John Hopkins Press, 1971); and H.A. Simon, *The Sciences of the Artificial* (3<sup>rd</sup> edition, MIT Press, 1996), which criticizes most designers of systems for creating an environment that is based on the perception of an information scarcity but that in reality possesses information overload and thus users will suffer from attention scarcity. In this example, the online legal framework, as a whole, can be viewed as a system which relies heavily on notice and consent under the presumption of information scarcity but which at latest with the advent of personal computers has changed to a system of information overload. Hence, notice and consent should be limited to reduce the information overload.

<sup>188</sup> O. Ben-Shahar and C.E. Schneider, *More Than You Wanted To Know – The Failure of Mandate Disclosure*, Ch. 6.

<sup>189</sup> P. Ohm, ‘Branding Privacy’, 97 *Minnesota Law Review* (2013).

<sup>190</sup> They ‘pivot’ their business model – for example, a start-up company hosting an online service platform receives funding after having accrued a solid user base and now it is tasked with monetizing its service by, inter alia, drawing on the users’ personal data, which it did not previously do.

<sup>191</sup> *Ibid.*, p. 913 et seq.

– if there even is an alternative at all – would become incredibly high and it is doubtful that users would even notice the changes at all.<sup>192</sup> Coupled with the fact that the behavioural economics literature teaches us that users are averse to switching services or defaults (default bias), this incremental approach has proven effective in expanding the collection and use of personal data without users realizing the shift.<sup>193</sup>

## 4.2. The Tools in the Toolbox

The previous subsection has outlined the major impediments that users suffer in the context of informed consent for targeted behavioural advertising. These impediments were roughly grouped into individual and systemic issues. With the above in mind, one must ask whether the proposed tools in the EU data protection framework to regulate targeted behavioural advertising are effective at empowering individuals. The approach the regulator chose in the GDPR can be described as aiming to reduce search information costs for users by introducing simplified notices that make use of simplified language as well as the introduction of the possibility for the Commission to create an icon scheme. This subsection will analyse these strategies against the backdrop of the information provided in the subsection above.

### 4.2.1. Reducing Search and Information Costs

Viewing the communication between users and websites as a transaction of information, the act of rendering informed consent to targeted behavioural advertising can be framed as an exchange. In this regard, simplified notification and the use of icons can be viewed as a way to reduce transaction costs for users – the aim is to provide users with better understandable information and to make the information more easily accessible.

When scrutinizing the EU data protection framework applicable to the regulation of targeted behavioural advertising, we can observe that for the provision of information, there is a push to reduce users' transaction costs in this exchange. In the beginning, websites could provide the information in the fine print as part of the general terms of the website; this made it difficult for users to find the information and users accrued high information costs. The amendment of the e-Privacy Directive by the Citizens Rights' Directive and the subsequent obligation to implement prominent cookie notices on websites has reduced these search costs. With the GDPR, the EU regulator has taken further steps to facilitate the provision of information by introducing a simplification of notices and their (partial) replacement by visual keys such as icons. However, it is still unclear how this will transpire into reality, as the GDPR does not contain detailed rules necessary for the creation of these information tools and delegates the competence to the Commission. However, the Commission has yet to put forward these rules. The use of simplified-language, multi-tiered notices, machine-readable

---

<sup>192</sup> Ibid., p. 920-921.

<sup>193</sup> Ibid., p. 922 et seq.

text and icons poses a further shift to the reduction of search costs. However, the efficacy of the simplified notices and the use of icons is contingent on a number of considerations.

#### 4.2.2. Simplified Notices = Better Notices?

Does making notices simpler really help users understand them and overcome the individual and systemic problems they face? Simplification of written notices such as the proposed three-step notice may lower search and information costs, however, they have an inherent problem which they are unable to solve: how can complexity be boiled down to brief and simple language? The problem of information overload might be ameliorated by simplification, yet it may lead to the ‘sorting out’ of necessary and relevant information or even lead to the misrepresentation of information and processes that users would require to make a valid decision, but which fall prey to simplification amplified by the users’ inherent biases. Reducing the length of notices and introducing simplification may have adverse effects on the quality of the disclosure since a complex process can hardly be broken down into a simple sentence or an icon without losing its explanatory quality.<sup>194</sup> As Ben-Shahar and Schneider put it: ‘Simplicity, then, is usually in tension with full disclosure’.<sup>195</sup> In such cases, type I and type II errors in selecting the information to be displayed may occur: on the one hand, necessary information may be omitted while, on the other hand, unnecessary information may be retained or added to the notice. This is exacerbated by the growing amount of information that must be presented to individuals according to the GDPR.<sup>196</sup>

In the context of icons, the use of grades or scales in the form of symbols such as traffic lights can also lead to the misrepresentation of information as complex processes are ‘shoehorned’ into a limited number of qualifying categories. Linking one of the limited categories chosen to a complex process may result in a number of complex processes being bunched together, although these processes would otherwise require more differentiation.

What would the standards be to decide which information is included and which information is excluded from notices? The GDPR states that the three-step approach to simplified notices should be evaluated in its entirety, which is a necessary, as website publishers should then be hindered from hedging one layer in the notice against the others. To illustrate this, it could be in the interest of a website publisher to frame the wording of the simplified layer in such a way as to discourage users from opening the other layers.<sup>197</sup>

---

<sup>194</sup> D. Solove, 126 *Harvard Law Review* (2013), p. 1885.

<sup>195</sup> O. Ben-Shahar and C.E. Schneider, *More Than You Wanted To Know – The Failure of Mandate Disclosure*, p. 125.

<sup>196</sup> See the ‘quantity question’ posed by Ben-Shahar and Schneider, O. Ben-Shahar and C.E. Schneider, *More Than You Want To Know – The Failure of Mandated Disclosure*, Ch. 6.

<sup>197</sup> See Section 4.A.3. above.

Both the selection of the information that should be displayed and the form in which it should be displayed are not addressed. Who should have how much control over the design of the notices? How is compliance monitored and enforced? Self-regulation has not proven successful in this regard.<sup>198</sup> Crowdsourced initiatives that aim to make sense of websites' notices have largely failed.<sup>199</sup> But can the regulator effectively evaluate and micro-manage the enormous amount of notices? And what would be the yard-stick for the evaluation?

Related to monitoring and enforcement in this context, Calo states that the addressees of data protection notices may not be solely users; notices also serve two other purposes: when website publishers and ad network providers are mandated to draw up notices, they are inevitably forced to reflect and map their processes, which has a beneficial effect on the quality of the notice and thus the information the user gains.<sup>200</sup> Further, website publishers also signify accountability and transparency to regulators. Currently, efforts by Data Protection Agencies (DPA) in the Member States to monitor and enforce compliance exist, but it is an understatement to say enforcing compliance for targeted behavioural advertisement over the entirety of the Internet is a Herculean task (just consider the scope of the GDPR in this context).<sup>201</sup> Having machine-readable notices as a standard may facilitate the monitoring of compliance since the task of analysing notices can be partially automated. This could also help with detecting and revealing privacy lurches by automatically analysing websites' privacy policies over time and reporting changes. However, this is a standard that must still be established. Further, there is no guarantee that the notice reflects the actual practices of a website publisher or of an ad network provider.

#### 4.2.3. Some Iconoclastic Thoughts

---

<sup>198</sup> See for example the failure of the self-regulatory code on notification by industry players describe in Section 3.D.3.a. Also, D. Castro, 'Benefits and Limitations of Industry Self-Regulation for Online Behavioural Advertising', *ITIF* (2011).

<sup>199</sup> See for example the Terms of Service; Didn't Read, <https://tosdr.org/>, which is an initiative that crowdsources and rates general (i.e. not only data protection) notices of websites and gives short overviews using icons on the practices of websites. It also offers this information as a browser plug-in. Since the initiative operates as a platform, it requires individuals who make use of it and users to rate websites' notices. It has not reached the mainstream and it arguably does not reach the average users as one is more inclined to find and use the platform when one already has knowledge of the topic. Further, the non-profit nature does not support spending a lot of funds on publicity and advertising.

<sup>200</sup> R. Calo, 'Against Notice Skepticism in Privacy (And Elsewhere)', *87 Notre Dame Law Review* (2012), p. 1059 et seq.

<sup>201</sup> There have been efforts by the DPAs to monitor and check compliance in this regard. The most recent example is the so-called 'cookie sweep' which was an inquiry conducted by DPAs in the Czech Republic, Denmark, France, Greece, the Netherlands, Slovenia, Spain and the UK to check whether websites adhered to the EU data protection framework on cookies. Although the reliance on a partial automation of the scan of the websites poses a move in the right direction by the regulator, the sporadic and incomplete nature of the compliance check does not support effective enforcement. Further, not all Member States participated and it was the first, and currently, only event of this kind. Article 29 Working Party, Cookie Sweep Combined Analysis – Report, 3.2.2015, WP 229.

Next to the text-based forms of information, the GDPR also granted the Commission the mandate to create a framework for icons to convey information for notifications to users. Non-profit initiatives have also taken up the task of simplifying websites' policies by making use of icons.

Generally, icons and labels are used in various different contexts both offline and online. Examples of standardized icons and labels are the EU energy label, laundry labels or the Creative Commons icons.<sup>202</sup> A host of privacy and data protection-related icons and labels already exist.<sup>203</sup>

An earlier draft of the GDPR included a draft icon scheme by the European Parliament in its draft report on the GDPR, which consisted of a table with a number of icons reminiscent of traffic signs on the left side, a short one-sentence explanation in the centre and the option of one of two icons that indicate the state of compliance (green button with a check for compliance and a red button with a cross for non-compliance) (see *Figure 4* above).<sup>204</sup> Next to this, services such as *Terms of Service; Didn't Read* also make use of icons to grade various aspects of websites' general notices (*Figure 5* and *Figure 6*). The service introduces four visual scores to denote a certain quality. These are presented as a combination of a colour button with a small symbol as well as a word contained therein. The terms of a website are ranked in different classes; data protection is a part of the score but it also encompasses other issues such as copyright, terms of use, and so on.





---

<sup>202</sup> L. Edwards and W. Abel, 'The Use of Privacy Icons and Standard Contract Terms for Generating Consumer Trust and Confidence in Digital Services', *CREATE Working Paper Series 2014/15* (2014), <https://zenodo.org/record/12506/files/CREATE-Working-Paper-2014-15.pdf>.

<sup>203</sup> *Ibid.*

<sup>204</sup> European Parliament, Draft Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), Committee on Civil Liberties, Justice and Home Affairs, A7-0402/2013, 21.11.2013, ANNEX 1, p. 194-195.

Figure 5 – Overview of Terms of Service; Didn't Read icons and classes

Terms of service are reviewed by contributors and divided into small points that we can discuss, [compare](#) and ultimately assign a score with a badge:  Good,  Bad,  Blocker, or  Neutral.

Once a service has enough badges to assess the fairness of their terms for users, a class is assigned automatically by pondering the average scores.

**Class A** are the best terms of services: they treat you fairly, respect your rights and will not abuse your data.

**Class B** The terms of services are fair towards the user but they could be improved.

**Class C** The terms of service are okay but some issues need your consideration.

**Class D** The terms of service are very uneven or there are some important issues that need your attention.

**Class E** The terms of service raise very serious concerns.

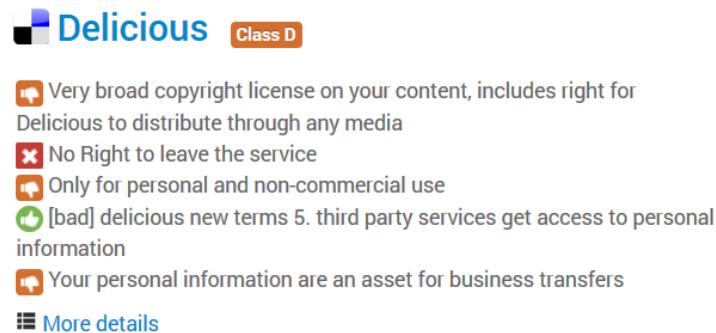
**No Class Yet** We haven't sufficiently reviewed the terms yet.

Right now, you will notice that not many services have a class assigned. That is because we need more data and more reviews before we can start assigning them. Moreover, we are still experimenting with how to apply classes.

More from the blog: [Why so many services have "No Class Yet"](#)

Source: <https://tosdr.org/>

Figure 6 – Example of a rated website on Terms of Service; Didn't Read



Source: <https://tosdr.org/>

The benefit of using icons is that individuals are more likely to view and understand icons than to read even the briefest of notices. The cost for communicating the information is therefore diminished. Icons, furthermore, do not suffer from the literacy problem as they give a visual cue to individuals.

For the sake of the analysis of icon schemes, it is helpful to draw on inspiration from semiotics in order to dissect the proposed icons (although this is done in a simplified manner).<sup>205</sup>

Semiotics is the study of the nature and function(s) of signs and symbols; it presents a frame of reference to dissect and analyse symbols.<sup>206</sup> One approach to analyse a symbol or a sign is to split it up into the so-called 'signifier' and the 'signified', which together make up the sign.<sup>207</sup> The signifier is the medium that individuals perceive – this can be an audio, visual,

<sup>205</sup> This approach has e.g. been taken in the context of trademark law, see B. Beebe, 'The Semiotic Analysis of Trademark Law', 51 *UCLA Law Review* (2004).

<sup>206</sup> *Ibid.*, p. 626 et seq.

<sup>207</sup> *Ibid.*, p. 633 et seq.



haptic or any other perceivable cue.<sup>208</sup> The signified is the concept or idea that individuals connect with this cue.<sup>209</sup>

This dichotomy is useful to analyse the icon schemes in relation to the insights gained on users as stated above. The signifier in this case is the visual icon design, i.e. how it looks, where it is placed, and so on. The signified is the message the icon conveys to individuals, for example the fact that your personal data is collected by means of 3<sup>rd</sup> party cookies.

#### 4.2.3.1. Understanding Icons

One of the problems with the use of icons is that the signifier must be designed in a way that users understand what it signifies. This either happens by using already familiar attributes of a signifier to design a new sign in which the signifier has some similar or familiar properties so that individuals can already attribute and transition these into a new context. An example would be the colours of a traffic light: individuals associate green with good or that something is permitted and red with bad or a prohibition. This is for example applied in the European Parliament's draft icons or the scoring by Terms of Service; Didn't Read. Other methods could consist of introducing a completely new sign and establishing it as a brand, however, this entails high costs. Alternatively, one could draw on individuals' instincts, such as fear, in designing a sign. However, this might be difficult to design and is possibly of limited usefulness due to the negative connotation it is confined to express – such as the fact that a sign cannot be designed to convey a more complex message.<sup>210</sup>

In the case of the European Parliament's draft icons, criticism was voiced that some of the icons were misleading and did not properly convey what they intend to express: (i) the encryption icon may mean that encryption is banned if it is combined with the green button due to its visual familiarity of traffic signs denoting maximum speed, which suggest a prohibitive stance, which is then affirmed by the green button (i.e. is a negative affirmed or is a positive affirmed?) and (ii) the purpose limitation icon is not understandable at all as the signifier fails to inform individuals of what it intends to signify.<sup>211</sup>

Here, it is interesting to make a differentiation. In the first case, the signifier was partly familiar (a lock) and can arguably be connected, with little cognitive effort, to the concept of

---

<sup>208</sup> Ibid.

<sup>209</sup> Ibid.

<sup>210</sup> E.g., the research on marking nuclear waste that will be dangerous for approximately 10,000 years or more. Researchers are trying to design a sign to mark the lethality of nuclear waste which people will understand in thousands of years in the future. In this context, the trefoil – the internationally known symbol for radiation - is viewed as ineffective as its meaning may be lost in the future. Therefore, a signifier that speaks to humans' primal fear should be designed. See K.M. Trauth, S.C. Hora and R.V. Guzowski, Expert Judgment on Markers to Deter Inadvertent Intrusion into the Waste Isolation Pilot Plant, Sandia Report, November 193, SAND92.

<sup>211</sup> See H. Roy, 'Some comments on the EU's draft Privacy Icons', *HRoy Blog* (2014), <https://hroy.eu/posts/encryptionEuDataIcons/>.

encryption. In the latter case, the sign - which is perhaps reminiscent of a roundabout – arguably fails to build a bridge with the concept of purpose limitation. But why is this the case? Compared to encryption, the concept of purpose limitation is less well-known and it is a specialized process in the field of data protection. Therefore, it can be argued that in cases where the signified is complex, novel or unfamiliar, the signifier fails to convey the message to individuals without the necessary consumer education. Therefore, simplification by boiling down complex concepts to signs has its limits.

Pettersson has put the European Parliament’s draft icons to the test with dismal results. In his experiment, individuals were tasked with describing what an icon meant and matching the icons with the legal data protection goals they are supposed to represent. Most participants failed at both tasks.<sup>212</sup>

In the context of icons, the use of grades or scales in the form of symbols such as traffic lights can also lead to the misrepresentation of information as complex processes are ‘shoehorned’ into a limited number of qualifying categories. Linking one of the limited categories chosen to a complex process may result in a number of complex processes being bunched together, although these processes would otherwise require more differentiation.

#### 4.2.3.2. A Digital Ocean of Icons, Trustmarks and Seals

Alongside the problem of designing icons that effectively communicate their message, the accumulation problem that also persists for simplified notices also persists for icons. Websites can be described as information-rich environments that lead to attention scarcity in users.<sup>213</sup> Content, ads and various elements vie for the user’s attention. In this context, website publishers may not have an incentive to give icons used for data protection purposes a space that guarantees visibility for users as it is more lucrative to host ad space. Even more, prominent notices that inform and dissuade users from being tracked for targeted behavioural advertising can be seen as running counter to the website publishers’ interests. In the Dutch cookie wall example, website publishers were so successful in making these cookie notices as annoying as possible that it resulted in users siding with advertisers against the regulator to abolish the tools that should protect users.<sup>214</sup> The same could easily be done with icons.

The Internet is like a vast ocean of icons, trustmarks and seals – all of which aim to convey a certain message, standard or quality. Examples are trustmarks for e-commerce or age

---

<sup>212</sup> J.S. Pettersson, ‘A Brief Evaluation of Icons in the First Reading of the European Parliament on COM(2012) 0011’, in J. Camerisch, S. Fischer-Hübner and M. Hansen (eds.), *Privacy and Identity Management for the Future Internet in the Age of Globalisation* (Springer, 2015).

<sup>213</sup> N. Koiso-Kanttila, ‘Time, attention, authenticity and consumer benefits of the Web’, 48 *Business Horizons* (2005), p. 65 and the references therein.

<sup>214</sup> R. Leenes and E. Kosta, 31 *Computer Law & Security Review* (2015), p. 331.

restriction in gaming.<sup>215</sup> Even when only constraining the analysis to the context of data protection and security, various privacy seal schemes that indicate compliance with certain standards exist.<sup>216</sup> The GDPR also mandates the creation of privacy seal schemes for the transfer of data to third countries and other purposes.<sup>217</sup> Although these are not the same as the icons proposed in Article 12(8) GDPR, there is a partial overlap since they compete with other, closely resembling visual cues for the user's attention. To put a number on it, a recent study has shown that in the context of data protection alone, there are at least 25 prominent privacy seals that communicate various traits of quality to users.<sup>218</sup> This illustrates that users are confronted with an increasing amount of icons and symbols that are mandated by law or that are used to show (voluntary) compliance with certain certification schemes. In turn, these icons and symbols also compete for the user's attention against other content, especially ads on websites.

### 4.3. Simplified Notifications and Icons Likely Do Not Address All Individual and Systemic Problems Related to Notice and Consent for Targeted Behavioural Advertising

The EU data protection framework has introduced new methods aimed at better informing users in order to improve the quality of user consent. The tools that the EU regulator envisions are guided by the goal to reduce information and search costs for users. Simplified notices and icons may achieve this goal to a certain extent. However, they still encounter problems related to the complexity of translating complex processes into small packages of information. In that respect, simplified notices and icons may help to mitigate some of the individual problems described in greater detail above. Depending on their design, icons might attract the attention of users in cases in which they would otherwise have not given attention to longer plain-text notices, thus increasing the chance that users are informed before giving their consent, as is required under the EU data protection framework. Further, if icons are established and become known to users, they would help tackle the literacy problem. The same holds true, to a lesser degree, with simplified notices. In the same vein, both icons and simplified notices could also do their part in mitigating the overload problem in notices.

In sum, the strategy to decrease search and information costs by utilizing icons and simplified notices will not be a panacea for informed consent in the context of targeted behavioural advertising. Some individual problems might be tackled if these tools are implemented in the right way. A cautious outlook would be that there is a chance to ameliorate the situation with regard to individual problems. Yet, some of the more systemic issues are left completely

---

<sup>215</sup> E.g., European Commission, EU Online Trustmarks – Building Digital Confidence in Europe, 2012.

<sup>216</sup> European Commission, EU Privacy Seals Project – Inventory and analysis of privacy certification schemes, 2013.

<sup>217</sup> Article 42 and Recital 100 of the Preamble to the GDPR.

<sup>218</sup> European Commission, EU Privacy Seals Project – Inventory and analysis of privacy certification schemes, 2013.

unscathed by this approach. If the Commission pushes on with the development of these tools, thought must be paid to users' cognitive shortcomings as well as the information environment on the Internet. Establishing these tools in the minds of users will take time and resources. It appears to be a daunting task to create these tools in the right way and a large amount of interdisciplinary research lies ahead.

## 5. Looking for Help Elsewhere – Competition Law as a Remedy for More Systemic Problems?

It has been stated above that there are novel approaches in the EU data protection framework that might be able to help tackle certain issues in the context of informed consent for targeted behavioural advertisement. These issues pertain mostly to problems that were classified as individual problems. The question arises that if the EU data protection framework does not hold the right legal response to tackle the more systemic issues connected to informed consent, is there perhaps a solution to be found in EU competition law? One way to achieve this would be to diminish the role of ad networks by means of EU competition law or to adopt an approach focusing on consumer welfare as well as commitments that take data protection goals into account.

As was noted above, the market for targeted behavioural advertising is quite complex and is still an under-researched area. Knowing that it is a multi-sided market may warrant a few presumptions on its traits, for example that ad networks require size on all ends of their platform to be sustainable, there are network effects between the different sides, and there is a tendency to form oligopolies or monopolies given the dynamics of operating in a multi-sided market.

In 2014, the EPDS issued a draft Opinion on the connection between data protection, consumer protection and competition law, which investigates 'free' online services that utilize users' personal data, for example for the purposes of offering targeted behavioural advertising.<sup>219</sup> In the draft Opinion, the EDPS calls on the inclusion of notions of data protection law in EU competition policy under the scope of consumer welfare.<sup>220</sup> This has produced mixed reactions.

On the one hand, it is argued that the purely economic approach should be applied and that one should refrain from encompassing goals which are not an inherent part of competition policy since this blurs the line between the different fields and undermines the 'internal coherence of the discipline'.<sup>221</sup> In essence, this criticism holds that problems in one discipline

---

<sup>219</sup> EDPS, Preliminary Opinion on Privacy and Competitiveness in the Age of Big Data – The Interplay between Data Protection, Competition Law and Consumer Protection in the Digital Economy, March 2014.

<sup>220</sup> Ibid.

<sup>221</sup> O. Lynskey, *The Foundations of EU Data Protection Law*, p. 264-265.

should be tackled by solutions in the same discipline.<sup>222</sup> Critics of this axiom point to the fact that the Commission and the CJEU have already decided the matter, citing the *ASNEF Equifax* judgment<sup>223</sup> by the CJEU and the *Google/DoubleClick*<sup>224</sup> and *Facebook/Whatsapp*<sup>225</sup> decisions by the Commission as their support. Next to this, from an economic perspective it is argued that such a practice would lead to the punishment of successful market participants.<sup>226</sup>

On the other hand, it is argued that the failure of data protection law and especially the consent requirement rests on a lack of alternative, more data protection-friendly services due to a lack of competition in digital markets.<sup>227</sup> The valuation of data in the analysis of markets has arguably been neglected. If this is the case, is the tenet that solutions for problems should be found in the same discipline still valid? If the lack of competition for data protection-friendly services poses a problem that has an adverse effect on data protection, would this not mean that the solution should be sought in the field of competition law, with an eye on the effects this has on data protection? It becomes harder to argue for a clear separation between the two fields. The argument could be that through increasing competition in digital markets, user choice would create a race to the top for data protection and would lead to more choice for consumers. This would then ideally result in the strengthening of the ‘business case’ for data protection. However, as has been outlined above, the convenience of free services and the desire for short-term gains mostly leads to users valuing data protection less in their decision-making process, albeit reporting that they value the protection of their personal data highly (i.e. the ‘privacy paradox’).<sup>228</sup>

The argument that it is ‘settled law’ by the Commission and the CJEU that the two disciplines are separate is scrutinized by Lynskey, who argues that the cited decisions were rendered pre-2009. Since then, the constitutional framework has changed, as has the general awareness of the topic of data protection.<sup>229</sup>

On the feasibility of this approach, Costa-Cabral argues that there are three possible trajectories for the Commission to follow: (i) clarifying the link between market power and the protection of personal data by investigating its link in digital markets; (ii) addressing discriminatory practices and unfair conditions for consumers by making this a priority and

---

<sup>222</sup> European Parliament, Challenges for Competition Policy in a Digitalised Economy, Study for the ECON Committee, July 2015, IP/A/ECON/2014-12, p. 42-44

<sup>223</sup> Case C-238/05 *ASNEF Equifax*, EU:C:2006:734.

<sup>224</sup> European Commission, COMP/M.4731 - *Google/DoubleClick*, C(2008) 927 final.

<sup>225</sup> European Commission, COMP/M.2717 – *Facebook/Whatsapp*, C(2014) 7239 final.

<sup>226</sup> O. Lynskey, *The Foundations of EU Data Protection Law*, p. 264-265.

<sup>227</sup> EDPS, Preliminary Opinion on Privacy and Competitiveness in the Age of Big Data – The Interplay between Data Protection, Competition Law and Consumer Protection in the Digital Economy, March 2014, p. 35.

<sup>228</sup> B. Schneier, *Data and Goliath – The Hidden Battles to Collect Your Data and Control Your World*, p. 49 et seq.

<sup>229</sup> O. Lynskey, *The Foundations of EU Data Protection Law*, p. 264-265.

issuing guidance on exploitative abuses and (iii) intervening in digital markets by introducing commitments that take data protection into account.<sup>230</sup>

Given its complexity and especially given the problems with multi-sided markets,<sup>231</sup> an in-depth inquiry in the market for targeted behavioural advertising is vital. If an investigation confirms oligopolistic or monopolistic structures, this should warrant closer scrutiny. Market intervention which incorporates notions of data protection is of course contingent on the Commission's willingness as well as robust economic findings relevant to competition law; however, it may be beneficial for users if the Commission were to have such a solution at hand in case ad network providers oppose regulatory change in the field of data protection. In any case, given the willingness of the Commission, it is arguably possible to incorporate some notions of data protection within competition policy. Whether this will be an adequate tool to tackle the more systemic challenges for informed consent in the context of targeted behavioural advertisement, however, is debatable. There is still uncertainty regarding how exactly the competition law rules apply in these situations, although there have been recent probes by national competition authorities in this ambit.<sup>232</sup> Further, it is hard to foresee if such an approach will lead to the envisioned results.

## 6. Conclusion

This paper has set out to investigate the effectiveness of the regulation of targeted behavioural advertising in the EU by analysing the tools proposed under the GDPR. It has outlined what targeted behavioural advertising is and how it functions: various parties are involved in a complex network which is used to serve online ads based on users' preferences over a network of websites which are connected by an ad network. Overcoming the matching problem that persists in advertising is done by the ubiquitous tracking of users on websites in an ad network. The information gained is subsequently used by ad network providers to profile users and to display tailored ads to users across websites in the ad network.

One of the findings is that the tracking tools do not give users options to decline tracking and that standardization initiatives in this regard, such as Do-Not-Track, have failed. Therefore, users cannot decide not to be tracked, but can merely decide not to use an online service.

---

<sup>230</sup> C. Costa-Cabral, 'The Preliminary Opinion of the European Data Protection Supervisor and the Discretion of the European Commission in Enforcing Competition Law', 23 *Maastricht Journal of European and Comparative Law* (2016), p. 512-513.

<sup>231</sup> Case C-67/13 P *CB v. Commission*, EU:C:2014:2204. See F. Pardelles and A. Scordamaglia-Tousis, 'The Two Sides of the Cartes Bancaires Ruling: Assessment of the Two-sided Nature of Card Payment Systems under Article 101(1) TFEU and Full Judicial Scrutiny of Underlying Economic Analysis', 10 *Competition Policy International* (2014).

<sup>232</sup> EDPS, Opinion 8/2016 on coherent enforcement of fundamental rights in the age of big data, 23.9.2016, p. 9, citing actions by the French, UK, Belgian and German competition authorities in matters related to the use of personal data.

The paper describes the way in which the EU data protection framework tries to cope with targeted behavioural advertising. The EU regulator relies on the regulatory tool of notice and consent to legitimize the processing of users' personal data for targeted behavioural advertising. However, the effective regulation of targeted behavioural advertising has been impeded by a lack of harmonization, ineffective enforcement and attempts to undermine the legal framework by intense lobbying by industry and some Member States. In the process of amending the EU data protection framework, the e-Privacy Directive is currently under review and the DPD will be replaced by the GDPR in the spring of 2018.

Even though improvements to the protection of users are made in the form of simplified notification (three-step notification and icons), the effectiveness of the prior informed consent requirement is still debatable. Here, the paper draws a distinction between *individual* and *systemic* problems that users face in the context of informed consent for targeted behavioural advertisement. The aim of the EU regulator to decrease search and information costs does not address the systemic issues and only addresses the individual issues to the extent that the design of these tools will be successful. This is an enormous challenge as the underlying problems are manifold – finding a legal strategy for tackling these problems will be a daunting task, which will require interdisciplinary research. At a more fundamental level, the lack of a clear policy line on the matter worsens the outlook, as the formulation of a policy goal is necessary to stake the legal route the regulator should take.

In view of the complexity of creating effective notification tools and the failure of the EU data protection framework to tackle the more systemic issues, it was proposed to contemplate the inclusion of data protection goals into competition policy under the auspices of consumer welfare. Even if this is a contested idea, it could provide for another tool that could be utilized as the *ultima ratio* and which could sway ad network providers to increase the effectiveness of the notice and consent requirement.

In any case, an in-depth analysis of the market for targeted behavioural advertising is necessary. Combined with further inter-disciplinary research on the efficacy of means to improve user notification, this could form the basis for the EU regulator to contemplate whether notice and consent is still a viable regulatory tool for targeted behavioural advertisement. As this paper has shown, the toolbox may also include other tools to protect users and regulate targeted behavioural advertisement.

## 7. Bibliography

### 7.1. Legislation

Article 29 Working Party, Cookie Sweep Combined Analysis – Report, 3.2.2015, WP 229

Article 29 Working Party Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites, WP 56, 5035/01/EN/Final, 30 May 2002

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (e-Privacy Directive), [2002] OJ L 201/37, as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (Text with EEA relevance) (The Citizen's Rights Directive), [2009] OJ L 337/11

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive), [1995] OJ L 281/31

EPDS, Opinion 5/2016 Preliminary EDPS Opinion on the review of the ePrivacy Directive (2002/58/EC), 22.7.2016

EDPS, Opinion 8/2016 on coherent enforcement of fundamental rights in the age of big data, 23.9.2016

EDPS, Preliminary Opinion on Privacy and Competitiveness in the Age of Big Data – The Interplay between Data Protection, Competition Law and Consumer Protection in the Digital Economy, March 2014

ENISA, Privacy considerations of online behavioural tracking, 2010

Federal Data Protection Act (*Bundesdatenschutzgesetz*; BDSG)



Opinion 1/2008 of the Article 29 Working Party on data protection issues related to search engines, 4.4.2008, WP 148

Opinion 1/2010 of the Article 29 Working Party on the concepts of “controller” and “processor”, 16.2.2010, WP 169

Opinion 2/2010 of the Article 29 Working Party on online behavioural advertising, 22.6.2010, WP 171

Opinion 15/2011 of the Article 29 Working Party on the definition of consent, 13.7.2011, WP187

Opinion 16/2011 of the Article 29 Working Party on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising, 8.12.2011, WP 188

Opinion 04/2012 of the Article 29 Working Party on Cookie Consent Exemption, 7.6.2012, WP 194

Opinion 9/2014 of the Article 29 Working Party on the application of Directive 2002/58/EC to device fingerprinting, 25.11.2014, WP 224

Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), [2016] OJ L 119/1

## 7.2. Case Law

Case C-67/13 P *CB v. Commission*, EU:C:2014:2204

Case C-131/12 *Google v. Agencia Espanola de Proteccion de Datos (AEPO) and Mario Costeja Gonzalez*, EU:C:2014:317

Case C-238/05 *ASNEF Equifax*, EU:C:2006:734

European Commission, COMP/M.2717 – *Facebook/Whatsapp*, C(2014) 7239 final

European Commission, COMP/M.4731 - *Google/DoubleClick*, C(2008) 927 final

LG Hamburg, Urt. V. 21.04.2015, Az. 416 HKO 159/14

LG Munich I, Urt. v. 27.05.2015, Az. 37 O 11673/14, 37 O 11843/14

Opinion of Advocate General Jääskinen in Case C–131/12 *Google v. Agencia Espanola de Proteccion de Datos (AEPO) and Mario Costeja Gonzalez*, EU:C:2013:424

Opinion of Advocate General Sánchez-Bordona in Case C-582/14 *Patrick Breyer v. Federal Republic of Germany*, EU:C:2016:339

### 7.3. Secondary Sources

Acquisti, A. and Grosklags, J., 'Privacy and Rationality in Individual Decision Making', *IEEE Security and Privacy* (2005)

Acquisti, A. and Grosklags, J., 'What can Behavioural economics Teach Us About Privacy?', in S. De Capitani di Vimercati et al. (eds.), *Digital Privacy - Theory, Technologies, and Practices* (Auerbach Publications, 2007)

Acquisti, A. et al., 'Sleights of Privacy - Framing Disclosures, and the Limits of Transparency', Proceedings of the Ninth Symposium on Usable Privacy and Security (2013), <http://dl.acm.org/citation.cfm?id=2501613>

Acquisti, A., 'Nudging Privacy – The Behavioural Economics of Personal Information', *IEEE Security & Privacy Economics* (2009)

Anderson, S.P. and Gabszewicz, J.J., 'The media and advertising: a tale of two-sided markets', in V. Ginsburgh and D. Throsby (eds.), *Handbook of the Economics of Arts and Culture – Vol. 1* (Elsevier, 2006)

Ayres, I. and Schwartz, A., 'The No-Reading Problem in Consumer Contract Law', 66 *Stanford Law Review* (2015)

Beebe, B., 'The Semiotic Analysis of Trademark Law', 51 *UCLA Law Review* (2004)

Ben-Shahar, O. and Schneider, C.E., *More Than You Wanted To Know – The Failure of Mandate Disclosure* (Princeton University Press, 2014)

Brkan, M., 'Data protection and European private international law: observing a bull in a China shop', 5 *IDPL* (2015)

Brown, I., 'Privacy Attitudes, incentives and behaviours', SSRN (2011), <http://ssrn.com/abstract=1866299>, p. 7.

Bullmore, J., 'Why it's time to Say Goodbye to IKTHTMISAIW\* - (\*I know that half the money I spend on advertising is wasted ...)', *WPP Annual Report & Accounts* (2013), <http://www.wpp.com/annualreports/2013/what-we-think/why-its-time-to-say-goodbye-to-ikthtmisoaiw/>

Bygrave, L.A., *Data Privacy Law – An International Perspective* (2014, Oxford University Press)

Calo, R., 'Against Notice Skepticism in Privacy (And Elsewhere)', *87 Notre Dame Law Review* (2012)

Casteluccia, C., 'Behavioural Tracking on the Internet: A Technical Perspective', in S. Gutwirth et al. (eds.), *European Data Protection: In Good Health?* (Springer, 2012)

Castro, D., 'Benefits and Limitations of Industry Self-Regulation for Online Behavioural Advertising', *ITIF* (2011)

Church, P., 'Should you care what the Article 29 Working Party says?', *60 Linklaters Technology Media and Telecommunications* (2011)

Clayton, R., 'The Phorm "Webwise" System', *Computer Laboratory, University of Cambridge* (2008), <http://www.cl.cam.ac.uk/~rnc1/080518-phorm.pdf>

Clifford, D., 'EU Data Protection Law and Targeted Advertising – Consent and the Cookie Monster – Tracking the crumbs of online user behaviour', *5 Journal of Intellectual Property, Information Technology and E-Commerce Law* (2014)

Costa-Cabral, C., 'The Preliminary Opinion of the European Data Protection Supervisor and the Discretion of the European Commission in Enforcing Competition Law', *23 Maastricht Journal of European and Comparative Law* (2016)

Eckersley, P., 'How Unique Is Your Browser?', *Electronic Frontier Foundation* (2014), <https://panoptickick.eff.org/browser-uniqueness.pdf>

Edwards, L. and Abel, W., 'The Use of Privacy Icons and Standard Contract Terms for Generating Consumer Trust and Confidence in Digital Services', *CREATE Working Paper Series 2014/15* (2014), <https://zenodo.org/record/12506/files/CREATE-Working-Paper-2014-15.pdf>

Edwards, L. and Hatcher, J., 'Consumer Privacy Law 2: Data Collection, Profiling and Targeting', in L. Edwards and C. Waelde (eds.), *Law and the Internet* (2009, Hart Publishing)

Elahi, S., 'Privacy and Consent in the digital era', 14 *Information Security Technical Report* (2009)

ETNO, Study on the ePrivacy Directive (DLA Piper, 2016)

European Commission, <https://ec.europa.eu/digital-single-market/en/news/eprivacy-directive-commission-launches-public-consultation-kick-start-review>

European Commission, Attitudes on Data Protection and Electronic Identity in the European Union, Special Eurobarometer 359, 2011

European Commission, Data Protection in the European Union: Citizens' perceptions – Analytical Report, Flash Eurobarometer Series no. 225, 2008

European Commission, Data Protection Report, Special Eurobarometer 431, 2015

European Commission, ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation, Final Report (European Commission, 2015)

European Commission, EU Online Trustmarks – Building Digital Confidence in Europe, 2012

European Commission, EU Privacy Seals Project – Inventory and analysis of privacy certification schemes, 2013

European Parliament, Challenges for Competition Policy in a Digitalised Economy, Study for the ECON Committee, July 2015, IP/A/ECON/2014-12

Friedman, L., 'Market Segmentation', *CUNY*, <http://academic.brooklyn.cuny.edu/economic/friedman/mmmarketsegmentation.htm>

Goldfarb, A. and Tucker, E., 'Privacy Regulation and Online Advertising', 57 *Management Science* (2011)

Härting, N., *Datenschutzgrundverordnung – Das neue Datenschutzrecht in der betriebliche Praxis* (Otto Schmidt Verlag, 2016)

Heckle, R. and Lutters, W.G., 'Re-examining User Perceptions of Online Privacy Notices: The Value of Real-Time Observation', Proceedings of the Symposium on Usable Privacy and Security (SOUPS) (2005), <http://cups.cs.cmu.edu/soups/2005/2005posters/17-heckle.pdf>

Helberger, N., 'Freedom of Expression and the Dutch Cookie-Wall', SSRN (2013), [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2351204](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2351204)

Hijmans, H., 'Right to Have Links Removed: Evidence of Effective Data Protection', 21 *Maastricht Journal of European and Comparative Law* (2014)

IAB and C3Research, 'Ad Blocking: Who Blocks Ads, Why and How to Win Them Back', *IAB Website* (2016), [www.iab.com/wp-content/uploads/2016/07/IAB-Ad-Blocking-2016-Who-Blocks-Ads-Why-and-How-to-Win-Them-Back\\_2016.pdf](http://www.iab.com/wp-content/uploads/2016/07/IAB-Ad-Blocking-2016-Who-Blocks-Ads-Why-and-How-to-Win-Them-Back_2016.pdf)

Internet Live Stats, <http://www.internetlivestats.com/total-number-of-websites/>

Jang, D. et al., 'An Empirical Study of Privacy-Violating Information Flows in JavaScript Web Applications', Proceedings of CCS (2010)

Jensen, C. and Potts, C., 'Privacy Policies as decision-making tools: an evaluation of online privacy notices', Proceedings of the SIGCHI conference on Human Factors in Computing Systems (2004)

Koiso-Kanttila, N., 'Time, attention, authenticity and consumer benefits of the Web', 48 *Business Horizons* (2005)

Kokott, J. and Sobotta, C., 'The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR', 4 *IDPL* (2013)

Kosta, E., 'The Netherlands – The Dutch Regulation of Cookies', 2 *EDPL* (2016)

Kosta, E., *Consent in European Data Protection Law* (Nijhoff, 2014)

Krebs, B., 'What you should know about History Sniffing', *KrebsonSecurity* (2010), <http://krebsonsecurity.com/2010/12/what-you-should-know-about-history-sniffing/>

Kreutzer, R.T., *Praxisorientiertes Online-Marketing – Konzepte, Instrumente, Checklisten* (2nd edition, Springer-Gabler, 2014)

Kristol, D.M., 'HTTP Cookies: Standards, Privacy, and Politics', *Lucent Technologies* (2001)

Kuner, C., 'Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law', 5 *IDPL* (2015)

Lamadrid de Pablo, A., 'The double duality of two-sided markets', 5 *Comp. Law* (2015)

Lee, P., 'The e-Privacy Directive - when and how does it apply exactly?', *FieldFisher Privacy, Security and Information Law* (2011),  
<http://privacylawblog.fieldfisher.com/2011/the-e-privacy-directive-when-and-how-does-it-apply-exactly/>

Leenes, R. and Kosta, E., 'Taming the Cookie Monster in Dutch Law – A Tale of Regulatory Failure', 31 *Computer Law & Security Review* (2015)

Letter of Mr Hanff to the President of the European Commission Jean-Claude Juncker of 25 February 2016

Long, W., 'Significant Impact of New EU Data Protection Regulation on Financial Services', *Global Banking & Financial Review* (2014),  
<https://www.globalbankingandfinance.com/significant-impact-of-new-eu-data-protection-regulation-on-financial-services/>

Lynskey, O., 'Track[ing] changes: an examination of EU Regulation of online behavioural advertising through a data protection lens', 36 *European Law Review* (2011)

Lynskey, O., *The Foundations of EU Data Protection Law* (OUP, 2015)

Markou, C., 'Behavioural Advertising and the "New Cookie Law" as a Victim of Business Resistance and a Lack of Official Determination', in S. Gutwirth, R. Leenes and P. de Hert (eds.), *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection* (Springer, 2016)

Mayer, J.R. and Mitchell, J.C., 'Third-Party Web Tracking: Policy and Technology', 2012 IEEE Symposium on Security and Privacy (SP) (2012),  
<http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6234427>

Mayer, J.R., 'Do Not Track as a Generative Approach to Web Privacy', *W3C* (2010),  
<http://www.w3.org/2011/track-privacy/papers/mayer.pdf>

McDonald, A.M. and Cranor, L.F., 'The Cost of Reading Privacy Policies', *A Journal of Law and Policy for the Information Society* (2012)

Moerel, L., 'The Long Arm of EU Data Protection Law: Does the Data Protection Directive Apply to Processing of Personal Data of EU citizens by Websites Worldwide?', 2 *IDPL* (2010)

O'Reilly, L., 'Google, Microsoft, and Amazon are paying Adblock Plus huge fees to get their ads unblocked', *Business Insider UK* (2015), <http://uk.businessinsider.com/google-microsoft-amazon-taboola-pay-adblock-plus-to-stop-blocking-their-ads-2015-2?r=US>

Ohm, P., 'Branding Privacy', 97 *Minnesota Law Review* (2013)

Özlem Atikcan, E. and Chalmers, A.W., 'The Business of Internet Privacy: Interest Group Lobbying and the European Union's General Data Protection Regulation', European Consortium for Political Research (ECPR) (2016), <https://ecpr.eu/Filestore/PaperProposal/292751a0-218d-4af9-a574-ff3298e7bcca.pdf>

PageFair and Adobe, 'Adblocking goes mainstream', PageFair and Adobe report 2014, <https://downloads.pagefair.com/wp-content/.../05/Adblocking-Goes-Mainstream.pdf>

Palfrey, J., 'The Public and the Private at the United States Border with Cyberspace', 78 *Mississippi Law Journal* (2008), <http://cyber.law.harvard.edu/publications>

Panopticklick, <https://panopticklick.eff.org/index.php?action=log&js=yes>

Pardelles, F. and Scordamaglia-Tousis, A., 'The Two Sides of the Cartes Bancaires Ruling: Assessment of the Two-sided Nature of Card Payment Systems under Article 101(1) TFEU and Full Judicial Scrutiny of Underlying Economic Analysis', 10 *Competition Policy International* (2014)

Parker, G.G. and van Alstyne, M.W., 'Two-Sided Network Effects: A Theory of Information Product Design', 51 *Management Science* (2005)

Pettersson, J.S., 'A Brief Evaluation of Icons in the First Reading of the European Parliament on COM(2012) 0011', in J. Camerisch, S. Fischer-Hübner and M. Hansen (eds.), *Privacy and Identity Management for the Future Internet in the Age of Globalisation* (Springer, 2015)

Posner, R.A., 'Behavioural Law and Economics', in R.A. Posner (ed.), *Frontiers of Legal Theory* (Harvard University Press, 2001)

Rochet, J.-C. and Tirole, J., 'Two-Sided Markets: A Progress Report', *Toulouse School of Economics* (2005),

[http://www.tse-fr.eu/sites/default/files/medias/doc/by/rochet/rochet\\_tirole.pdf](http://www.tse-fr.eu/sites/default/files/medias/doc/by/rochet/rochet_tirole.pdf)

Rochet, J.-C. and Tirole, J., 'Two-Sided Markets: An Overview', *MIT* (2004),

[http://web.mit.edu/14.271/www/rochet\\_tirole.pdf](http://web.mit.edu/14.271/www/rochet_tirole.pdf)

Roy, H., 'Some comments on the EU's draft Privacy Icons', *HRoy Blog* (2014),

<https://hroy.eu/posts/encryptionEuDataIcons/>

Schneier, B., *Data and Goliath – The Hidden Battles to Collect Your Data and Control Your World* (W.W. Norton & Company, 2015)

Schütze, R., 'Constitutionalism and the European Union', in C. Barnard and S. Peers (eds.), *European Union Law* (OUP, 2014)

Simon, H.A., 'Designing Organizations for an Information-Rich World', in M. Greenberger (ed.), *Computers, Communication, and the Public Interest* (John Hopkins Press, 1971)

Simon, H.A., *The Sciences of the Artificial* (3rd edition, MIT Press, 1996)

Smith, A., *What Internet Users Know about Technology and the Web – The Pew Research Center's 'Web IQ' Quiz* (PEW, 2014)

Solove, D., 'Privacy Self-Management and the Consent Dilemma', *126 Harvard Law Review* (2013)

Stange, M., 'Real-Time Advertising', *5 Wirtschaftsinformatik* (2014)

Sunstein, C., 'Empirically Informed Regulation', *78 University of Chicago Law Review* (2011)

Svantesson, D.J.B., 'Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation', *5 IDPL* (2015)

Tapscott, D., *The digital economy: promise and peril in the age of networked intelligence* (McGraw-Hill, 1997)

Taylor, M., 'The EU's human rights obligations in relation to its data protection laws with extraterritorial effect', *5 IDPL* (2015)



Tene, O. and Polonetsky, J., 'To Track or "Do Not Track": Advancing Transparency and Individual Control in Online Behavioural Advertising', 13 *Minnesota Journal of Law, Science & Technology* (2012)

Terms of Service; Didn't Read, <https://tosdr.org/>

Thaler, R.H. and Sunstein, C., *Nudge – Improving decisions about health, wealth and happiness* (Penguin Books, 2009)

Trauth, K.M., Hora, S.C. and Guzowski, R.V., Expert Judgment on Markers to Deter Inadvertent Intrusion into the Waste Isolation Pilot Plant, Sandia Report, November 193, SAND92

Ur, B. et al., 'Smart, Useful, Scary, Creepy: Perceptions of Online Behavioural Advertising', Proceedings of the SOUPS 2012 (2012), [http://www.cylab.cmu.edu/research/techreports/2012/tr\\_cylab12007.html](http://www.cylab.cmu.edu/research/techreports/2012/tr_cylab12007.html)

Ustaran, E. (ed.), *European Privacy – Law and Practice for Data Protection Professionals* (IAPP, 2012)

Website of Ghostery, <https://www.ghostery.com/en-GB/>

Williams, C., 'BT and Phorm: how an online privacy scandal unfolded', *The Telegraph*, 08.04.2011, <http://www.telegraph.co.uk/technology/news/8438461/BT-and-Phorm-how-an-online-privacy-scandal-unfolded.html>

Wolf, C., 'Impact of the CJEU's Right To Be Forgotten – Decisions on Search Engines and Other Service Providers in Europe', 21 *Maastricht Journal of European and Comparative Law* (2014)

Zuiderveen-Borgesius, F.J., 'Personal data processing for behavioural targeting: which legal basis?', 5 *IDPL* (2015)

Zuiderveen-Borgesius, F.J., *Improving privacy protection in the area of behavioural advertising* (PhD Thesis, IViR UV Amsterdam, 2014)