Some Considerations on Intelligent Online behavioural Advertising

Dr Guido Noto La Diega[1]

Online behavioural advertising refers to advertisements, which are tailored to the tastes and habits of the user who actually views them. It is an intricate phenomenon for a number of reasons, including a twofold regulatory interweave. Firstly, between top-down and self-regulation. Secondly, between the personal data perspective and the competition one. This paper aims to get the knots out in the belief that rising awareness about the issues in online behavioural advertising is pivotal to a fair online environment. The paper is particularly timely in light of new regulations (draft ePrivacy Regulation and General Data Protection Regulation), worrying industry moves (e.g. the Facebook / WhatsApp data synchronisation), and the advent of new technologies. In particular, it will be shown that artificial intelligence presents not only threats to consumers, but also opportunities for bespoke compliance mechanisms. As an appendix, the "Cooperative Charter for an Integrated Approach to Online Behavioural Advertising" is presented in order to facilitate the dialogue between the stakeholders and ensure a balanced regulation of online behavioural advertising.

I. BACKGROUND AND METHODS

In recent years, facilitated by the growth of artificial intelligence (e.g. machine learning and predictive analytics), cloud computing,[2] and big data,[3]

[1] Lecturer in Law (Northumbria University); President (Ital-IoT Centre for Multidisciplinary Research on the Internet of Things); *cultore della materia* in intellectual property and private law (Università degli Studi di Palermo). The author thanks the Journal's reviewer, as well as Tony Ward, Rebecca Moosavian, and the participants at the fourth Winchester Conference on Trust, Risk, Information and the Law for most helpful comments on previous drafts. Any mistakes or omissions are those of the author.

[2] It is positive that, under the Commission Regulation (EU) 2015/2003 of 10 November 2015 implementing Regulation (EC) No. 808/2004 of the European Parliament and of the Council concerning Community statistics on the information society [2015] *OJ* L294/32, para A(2)(g)(ii), the data to be transmitted for the production of European statistics on the information society include ubiquitous connectivity with particular regards to enterprises that pay for advertisements on the internet using targeted advertising.

[3] According to Commission, 'Impact assessment: Accompanying the document Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications

new tracking[4] and profiling[5] techniques have been developed. They have enabled the rise of online behavioural advertising (OBA),[6] that is the provision of advertisements, which are tailored to the tastes and habits of the user who actually views them.[7]

The main aim of the paper is to untangle OBA's knot, whose intricacy is due to a number of reasons, including a threefold regulatory interweave. Firstly, between top-down and self-regulation. Secondly, between the personal data perspective and the competition one.

The paper appears timely for at least four reasons. Firstly, the General Data Protection Regulation (GDPR)[8] will soon come into effect and it contains some relevant provisions, for instance the recognition that direct marketing

and repealing Directive 2002/58/EC' (Commission staff working document), SWD (2017) 3 final – 2017/03 (COD), para 4.2.1, a big contribution to big data "is made by online services that track users' online communications in order to build detailed commercial data-banks, which can be used for online behavioural advertising".

4 On the use of high-frequency sounds to covertly track across a range of devices see C. Calabrese and others, 'Comments for November 2015 Workshop on Cross-Device Tracking, Letter of the Center for Democracy & Technology to the Federal Trade Commission of 16 October 2015' (2015), https://cdt.org/files/2015/10/10.16.15-CDT-Cross-Device-Comments.pdf, accessed 11 June 2017. For a solution based on semi-supervised machine learning methods see R. Díaz-Morales, 'Cross-Device Tracking: Matching Devices and Cookies', *IEEE International Conference on Data Mining Workshop (ICDMW)* (IEEE 2015) 1699-1704. Cookie technologies may not be available in mobile application. Therefore, the advertiser may, for instance, link the identifier used for advertising on mobile applications to an advertising cookie on the same device in order to coordinate advertisements across the mobile apps and mobile browser. For example, it is common experience that while using a free app (usually with in-app purchases), at some point the screen is occupied by an ad and, if one clicks on it (perhaps inadvertently), which launches a web page in the mobile browser. Finally, one should keep an eye open on Flash cookies, which cannot be deleted through the traditional privacy settings of a web browser. Reportedly, they have been used precisely as a tool to restore "traditional cookies" that were refused or erased by the data subject (A. Soltani and others, 'Flash Cookies and Privacy' (2009) http://ssrn.com/abstract=1446862, accessed 11 June 2017). See also C. Bauer and others, 'Browsercookies und alternative Tracking-Technologien: technische und datenschutzrechtliche Aspekte' (2015) BVDW Whitepaper www.bvdw.org/medien/browsercookies-und-alternative-tracking-technologien-technischeund-datenschutzrechtliche-aspekte?media=7007, accessed 11 June 2017.

5 See EC Pallone, 'La profilazione degli individui connessi a Internet: "privacy online" e valore economico dei dati personali' (2015) 2 Ciberspazio e Diritto 295-327; K. Pandey and A. Mittal, 'User profiling on Tumblr through blog posts', *2016 International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT),*(IEEE 2016) 85-89; YC Fan and others, 'A Framework for Enabling User Preference Profiling through Wi-Fi Logs', *IEEE Transactions on Knowledge and Data Engineering* 3 (IEEE 2016) 592-603; S. Kanoje, S. Girase, and D. Mukhopadhyay, 'User Profiling Trends, Techniques and Applications' (2014) 1 International Journal of Advance Foundation and Research in Computer 1-6; A. Cufoglu, 'User Profiling-A Short Review' (2014) 3 *International Journal of Computer Application* 1-9.

6 OBA is the most important species of the genus 'targeted advertising'. There are several ways a prospective customer can be targeted: for instance, by analysing its previous behaviour (behavioural advertising), the page or the content the user is displaying (contextual advertising) or advertising based on known characteristics of the data subject (age, sex, location, etc.), or the information provided by the data subject at the registration stage (segmented advertising). Recently, it is becoming fashionable to call the phenomenon "interest-based advertising" (see, for instance, Advertising Standards Canada, 'ASC AdChoices Accountability Program: 2016 Compliance Report' (2017) http://adstandards.com/en/OBA/2016AdChoicesComplianceReport.pdf, accessed 11 February 2017).

7 There are several ways to provide targeted advertisements, but reasons of brevity suggest not going into details. A good reading is J. Yan and others, 'Behavioral targeted online advertising', in X.-S. Hua, T. Mei, and A. Hanjalic (eds), *Online multimedia advertising* (Premier Reference Source 2010) 213-232.

8 Regulation (EU) 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 or GDPR) [2016] *OJ* L119/1.

is a legitimate interest for the processing of personal data. Therefore, consent would not (always) be necessary.

Secondly, the draft ePrivacy Regulation[9] has been recently presented and it would change some relevant rules, such as the (no longer compulsory) cookies notice. The ePrivacy Regulation is aimed to ensure consistency with the GDPR.[10] It is important to keep in mind that this is a *lex specialis* and it will compthe GDPR as regards electronic communications data that qualify as personal data.[11] The ePrivacy Regulation, like the ePrivacy Directive is particularly important for the confidentiality of communications including non-personal data and data of legal persons.[12]

Thirdly, yet importantly, the update to WhatsApp's terms by enabling the use of Facebook users' data for advertising purposes has brought back to the academic scene the interweave of competition law and data protection. Better said, it is a reminder of how the public discourse[13] on personal data is affected by a sort of hemispatial neglect,[14] whereby one does not see that the space surrounding data is composed of interwoven legal bodies, such as not only data protection and privacy, but also competition, consumer protection, and intellectual property[15]. For instance, it cannot be denied that the increasing monopolisation of big data has competitive implications.[16] The argument may be put forward, that if a dominant company denies access to its dataset, they would be liable under the essential facility doctrine.[17] To make another example, a privacy policy that enables a digital platform to extract a huge amount of data without obliging itself to provide any actual service may fall under

9 Commission, 'Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)', COM (2017) 10 final (hereinafter draft ePrivacy Regulation).

10 Explanatory Memorandum to the draft ePrivacy Regulation, para 1.1.

11 *Ibid*., para 1.2.

12 Commission Staff Working Document, 'Ex-post REFIT evaluation of the ePrivacy Directive 2002/58/EC Accompanying the document Proposal for a Regulation of the European Parliament and the Council on the protection of privacy and confidentiality in relation to electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)', SWD/2017/05 final – 2017/03 (COD).

13 For instance, some respondents to the public consultation on the Commission's Communication on a Comprehensive Approach on Personal Data Protection in the European Union, submitted that "identification is not the only element in defining personal data and suggested to keep the personal data definition broad in order to anticipate possible evolution of new technologies and behavioural profiling" (Commission, 'Impact Assessment' (Commission staff working paper) SEC (2012) 72 final, annex 5, para 1.1).

14 Hemispatial neglect is a neuropsychological condition in which patients are not aware of itmes to one side of space. Patients with hemispatial neglect fail to 'report, respond, or orient to novel or meaningful stimuli presented to the side opposite to a brain lesion when this failure cannot be attributed to either sensory or motor defects' (Jonathan D. Trobe, *The Neurology of Vision* (Oxford University Press 2001) 326-327). This parallel has been first presented by Guido Noto La Diega, 'Hemispatial neglect and data protection' (Personal data in competition, consumer protection and IP law – Towards a holistic approach? Max Planck Institute for Innovation and Competition Conference, Munich, 21 October 2016).

15 Other areas might be involved as well. Discrimination law is certainly one of them. See, for instance, G. Angwin and T. Parris Jr., 'Facebook Lets Advertisers Exclude Users by Race' (ProPublica, 28 October 2016) https://www.propublica.org/article/facebook-lets-advertisers-exclude-users-by-race, accessed 12 February 2017.

16 *Cfr* M. Bourreau, A. de Streel, and I. Graef, *Big data and competition policy: Market power, personalised pricing and advertising* (CERRE 2017) and, more generally, M. Stucke and A. Grunes, *Big Data and Competition Policy* (Oxford University Press 2016).

17 I. Graef, *EU Competition Law, Data Protection and Online Platforms: Data as Essential Facility* (Wolters Kluwer 2016).

the Unfair Terms Directive.[18] The isolationist axiom is usually accompanied by the corollary whereby data protection tools are the best ones to protect the users' data. The hemispatial neglect has a number of other consequences, generally related to an over-protection of personal data. An example[19] might be the European Data Protection Supervisor's recommendation to ban altogether the use of advertising identifiers.[20] From a regulatory and legislative standpoint, the hemispatial neglect has led to cumbersome rules, sometimes hard to comply with and often useless.[21] Whereas some regulation is needed, regulations that do not attempt to understand data holistically risk to stifle innovation and fail to protect the data subjects.

The fourth reason is that artificial intelligence's role is becoming increasingly important. One need only mention that, one the one hand, artificial intelligence enables better-tailored and less intrusive advertisements. On the other hand, and this is the main suggestion of this paper, it enables advertising networks, publishers, advertisers (collectively 'OBA companies') to put in place bespoke compliance mechanisms based on the knowledge of the users' profiles. In simple terms, for certain users (e.g. tech-savvy and well-educated) agile seamless tools will be sufficient (e.g. no cookie notice). However, a more cautious approach (more information provided in an interactive and straightforward way) could be necessary for more vulnerable[22] categories of users.[23] Whereas the GDPR provides an increased protection for children, the needs of other segments of vulnerable population are not addressed (e.g. old non tech-savvy users, disabled people, etc.). Co-regulation[24] should address this gap. On the one hand,

18 The reference is to the significant imbalance in the parties' rights and obligations as provided by Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts [1995] *OJ* L95 (Unfair Terms Directive), art. 3(1).

19 For an example in literature, see inter alia C Schreiber, 'Google's Targeted Advertising: An Analysis of Privacy Protections in an Internet Age' (2015) 24 Transnat'l L. & Contemp. Probs. 269, 291, who calls for stronger data protection regimes, because, it would seem, "there is a desperate need, with today's technological advancements, to take measures to ensure that the fundamental right to privacy is not lost forever – regardless of whether it is knowingly relinquished or not".

20 "The EDPS also recommends that the future provisions should specify that interception and surveillance must be interpreted in the broadest technological meaning, including the addition of unique identifiers in the communication such as, for example, advertising identifiers, audio beacons or super cookies" (European Data Protection Supervisor, 'Opinion 5/2016 on the review of the ePrivacy Directive (2002/58/EC)' para V.1, https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2016/16-07-22_Opinion_ePrivacy_EN.pdf, accessed 9 February 2017. Fortunately, the recommendation has been ignored by Art. 5 of the draft ePrivacy Regulation.

21 For instance, Commission, 'Online services, including e-commerce, in the Single Market' (Commission staff working document) SEC (2011) 1641 final, para 4.2.2., recognises that "the application of data and privacy protection rules on cookies and behavioural targeting has sometimes been perceived as excessive by internet companies".

22 European Parliament, 'Strengthening the rights of vulnerable consumers' (resolution) 2011/2272(INI), para 26 voice the institution's concern "about the impact on vulnerable consumers of the routine use of online behavioural advertising and the development of intrusive online advertising practices, especially through the use of social networks".

23 For certain categories of users, OBA could be excluded altogether. This could be the children's case, as recommended by European Parliament, 'Resolution on the impact of advertising on consumer behaviour', 2010/2052(INI) para 30.

24 Co-regulation 'encompasses a range of different regulatory phenomena, which have in common the fact that the regulatory regime is made up of a complex interaction of general legislation and a self-regulatory body.' (Christopher T. Marsden, 'Internet co-regulation and constitutionalism: Towards European judicial review' (2012) 26(2-3) *International Review of Law, Computers & Technology* 211). In turn, self regulation refers to a body that dictates the rules that regard the body itself; however, pure self-regulation rarely exist, particularly on the Internet (Monroe E. Price and Stefaan G. Verhulst, *Self-regulation and the Internet* (Kluwer Law 2005) 3).

self-regulation is hard to enforce[25] and it sometimes tends to side-step traditional regulations (e.g. the opt-in/opt-out discussion). On the other hand, data protection is heavily regulated through the GDPR and the ePrivacy Directive, which do not take a holistic approach to personal data and which flexible enough to foresee every scenario, as proved by the exclusion of many categories of vulnerable people from the scope of the GDPR.

The structure of this paper is as follows. The starting point is the regulatory framework in Europe, with particular regard to the ePrivacy Directive,[26] currently under revision, the Data Protection Directive and the General Data Protection Regulation, with a focus on direct marketing. Moving from the observation that actors in cyberspace tend to ignore top-down regulations, the work critically analyses the International and European self-regulatory initiatives of the International Chamber of Commerce (ICC), the European Advertising Standards Alliance (EASA) and the Interactive Advertising Bureau (IAB). Great attention is then paid to the update to WhatsApp's policies that enable the use of their users' data by Facebook for advertising purposes. This is an ideal prism also to reconsider the relation between data protection and competition. Subsequently, a descriptive and prescriptive discourse on the couple artificial intelligence – OBA is presented. As an appendix, a pragmatic cooperative proposal is presented, with the aim of empowering the users, yet striking a balance between their interests and the OBA companies' ones.

As to the methods, alongside a literature, legislative, case law, regulatory, self-regulatory, and contractual review, qualitative empirical research was carried out to critically assess how OBA works in practice in scenarios involving companies such as Facebook, WhatsApp, and Google.[27]

II. THE EUROPEAN REGULATION OF TARGETED ADVERTISING. THE RESTRICTIVE INTERPRETATION OF THE EPRIVACY DIRECTIVE AND THE MORE FLEXIBLE DRAFT EPRIVACY REGULATION

Data are commonly seen from the perspective of the data subject's rights to privacy and data protection, which have undoubtedly (albeit debatably, from a theoretical standpoint) reached the status of fundamental human rights.[28] However, phenomena such as OBA shed light on the other face of data: users' data are becoming one of the most important assets in the IP portfolios of several businesses.[29] Therefore, a balance, as it happens, has to be stricken between competing interests.

Arguably, the European regulators have favoured privacy and data protection over the other perspectives. The first – and currently

25 The lack of enforceability may lead to an ineffectiveness of the initiative. See, for instance, KM Potvin L. Dubois, A. Wanless, 'Self-regulation by industry of food marketing is having little impact during children's preferred television' (2011) (6) Int J Pediatr Obes 401.

26 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 or ePrivacy Directive) [2002] *OJ* L 201/37.

27 A use case approach is quite common in the research on OBA. See, for instance, Schreiber (n. 18) 269 and C. Scott, 'Our digital selves: Privacy issues in Online Behavioural Advertising' (2012) 17 Appeal 63-82.

28 It is noteworthy that Commission, 'Report on the Application of the EU Charter of Fundamental Rights' (Commission staff working document) SEC (2011) 396 final, in the section on data protection, for the first time dedicates significant attention to OBA.

29 One of the first and most visible manifestations of this phenomenon has been the *sui generis* right on databases. However, the commodification of big data has created assets and rights non-subsumable under the traditional IP categories.

most important – guidance has been provided by the Article 29 Working Party's opinion on "online behavioural advertising" (OBA).[30] Unlike the US, that take a soft approach to OBA, in the EU there is a quagmire of laws and regulations.[31]

According to the advisory body, the main[32] provision to take into consideration is Art. 5(3) of the ePrivacy Directive, whereby,

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

Therefore, in the mainstream interpretation of the provision, advertising network providers can place cookies or similar devices on users' terminal equipment or obtain information through such devices only with the informed consent of the users, with limited non-mandatory exceptions.[33]

In order to review the ePrivacy Directive, the European Commission has launched a public consultation,[34] whose results have been published in December 2016.[35] There are mainly three points that are particularly relevant for targeted advertising.

Firstly, the cookies. According to 77% of citizens and civil society and 70% of public authorities, information service providers should not have the right to prevent access to their services if users refuse the storing of cookies. Three quarters of industry on the other hand disagree with this statement. This is a hot issue. For instance, if one disables the cookies, Twitter prevents users from accessing, though it explains that they and their partners use cookies for statistics, personalisation and advertising. To make a long story short, sometimes the tools the users theoretically have to prevent cookies and advertisements are more apparent than real.[36]

30 Article 29 Working Party, 'Opinion 2/2010 on online behavioural advertising' 00909/10/EN WP 171.

31 *Cfr* Commission (n. 2) para 4.2.2.

32 Other provisions may well apply. For instance, Art. 5(1) of the ePrivacy Directive would be relevant if an Internet Service Provider inspected traffic and content data in order to offer customers a reduced rate for Internet access in return for receiving OBA, using deep packet inspection, and thus communication data. See European Data Protection Supervisor, 'Opinion on net neutrality, traffic management and the protection of privacy and personal data' 2012/C 34/01, para 48.

33 The Directive allows two exceptions: i. Technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network; ii. If strictly necessary in order to provide an information society service explicitly requested by the subscriber or user. According to Article 29 Working Party, 'Opinion 04/2012 on Cookie Consent Exemption' 00879/12/EN WP 194, paras 4.2-4.3, third-party cookies used for OBA and first party analytics are not exempted from consent.

34 On 6 May 2015, the Commission adopted the Digital Single Market (DSM) Strategy, which announced that, following the adoption of the GDPR, the ePrivacy rules would also be reviewed. Therefore, on 11 April 2016, the European Commission has launched a public consultation to seek stakeholders' views on the current text of the ePrivacy Directive as well as the possible changes to the existing legal framework to make sure it is up to date with the new challenges of the digital area. The consultation has been closed on 5 July 2016.

35 'Synopsis report on the public consultation on the evaluation and review of the ePrivacy Directive' (2016, https://ec.europa.eu/digital-single-market/en/news/full-report-public-consultation-eprivacy-directive, accessed 8 February 2017).

36 To be precise, one can use Google Chrome's settings to block third-party cookies and retaining the access to most websites including Facebook if, instead of ticking 'Block sites from setting any data', they tick 'Keep local data only until you quit your browser'. However, this might not be sufficient and, anyway, a user without the relevant technological expertise would not be able to understand the mechanism.

Secondly, the majority of citizens, consumers, and civil society organisations support the option whereby information society services should be required to make available paying service (without behavioural advertising) as an alternative to the services paid by users' personal information. The fact that, conversely, the industry disagrees or strongly disagrees with this option (78.7%) confirms that data are fundamental digital assets, the real fuel of the online economy, and they are preferred to real "traditional" currency. The argument can be put forward that presenting the consumers with the option as to whether paying with traditional currency or personal data may increase the consumers' awareness of the importance of said data.

Another relevant issue is the option between opt-in and opt-out. Even though the question concerned marketing calls, the concept is the same, since OBA is the premise for targeted marketing. All groups of respondents agree that Member States should not retain the possibility to choose between a prior consent (opt-in) and a right to object (opt-out) regime for direct marketing calls to citizens. Unsurprisingly, the stakeholder groups are split on which regime should apply: whereas close to 90% of citizens, civil society and public authorities favour an opt-in regime, 73% of industry favour an opt-out regime. The draft ePrivacy Regulation, being binding in its entirety (once adopted and effective) adequately addresses this concern.

The Article 29 Working Party stressed that opt-out mechanisms do not in principle deliver data subjects' consent.[37] Assertedly, only in very specific, individual cases, implied consent could be argued.[38] Therefore, they demand advertising network providers to create prior opt-in mechanisms requiring an affirmative action by the data subjects indicating their willingness to receive cookies or similar devices and the subsequent monitoring of their surfing behaviour for the purposes of serving tailored advertising. Since the GDPR has further heightened the standard for consent, it becomes all the more true that implied consent does not meet the compliance requirements. Amongst other things, it is worth it to remember that consent must be specific.[39] As noted recently by the Article 29 Working Party, if a data controller obtained consent to process personal data e.g. to suggest new movies based on the viewing habits, if the controller decided to enable third parties to send or display OBA based on said habits, they would need to obtain ad-hoc consent.[40]

Even though, to meet the requirements of art. 5(3),[41] it would not be necessary to request prior consent for each reading of the cookie, to keep data subjects aware of the monitoring, advertising network providers are invited to:

i) limit in time the scope of the consent;
ii) offer the possibility to revoke it easily;[42] and
iii) create visible tools to be displayed where the monitoring takes place.

One should ask oneself why the expressed consent-opt in scheme has not been adopted by the main actors of the Web. Moreover, it has been submitted that "more appropriate or less onerous mechanisms exist to address most

37 Article 29 Working Party (n. 29) para 4.1.2.

38 Different rules apply to sensitive data, e.g. health and sex data. Indeed, the only available legal ground for the data processing is explicit, separate prior opt-in consent (no opt-out, no browser settings).

39 GDPR, arts 5(1)(b) and 6(1).

40 Article 29 Working Party, 'Guidelines on Consent under Regulation 2016/679' 17/EN WP259, para 3.2.

41 ePrivacy Directive.

42 One of the innovations of the GDPR is that consent must be easy to withdraw. Article 7(3) of the GDPR prescribes that ' the controller must ensure that consent can be withdrawn by the data subject as easy as giving consent and at any given time (as well as) free of charge or without lowering service levels' (Article 29 Working Party (n. 39) para 5.2).

of the harms stemming from the problems of inaccurate profiling, inadvertent disclosure and opaque data processing".[43]

Notwithstanding the said narrow interpretation to the ePrivacy Directive, national implementations[44] do not always require expressed consent i.e. the cookie notice. For instance, in the UK, s 6 of the Privacy and Electronic Communications (EC Directive) Regulations 2003 allow for implied consent, especially in the form of browsing settings. Therefore, opt-out mechanisms are accepted if the users indicate "in some way they [are] happy with the default".[45] The pillars of these regulations are clear and comprehensive information and the right to refuse the cookie (or kindred technology). In Italy, where the cookie banner is mandatory, it is nonetheless clarified that even if one does not expressly accept the policy, if one keeps browsing, that will be interpreted as implied consent.[46]

The British approach has been followed by the new ePrivacy Regulation,[47] whose draft has been recently released in January 2017. The strategy is threefold. Firstly, browser settings shall replace the cookie notice. Secondly, the exceptions to consent are clarified and expanded. Thirdly, there is a (long overdue) shift from the right to consent to the right to withdraw. Particularly the first pillar is to be welcomed and it helps overcome the uncertainty as to whether browser settings could be deemed to deliver the user's informed consent or not.[48] If adopted, it would constitute also the partial overcoming of the European Parliament's position whereby OBA would constitute "a serious attack on the protection of privacy when it […] has not first been freely and explicitly consented to by the consumer".[49]

Another reason why the step would be commendable is that it would help overcome the excessive emphasis on cookies, that are no longer the only or the most important tool to track users across platforms[50] and devices, as it has become fundamental in an Internet of Things world. One could think, for instance, of the recent move of Google to centralise their users' data in "My Account". In presenting the last update to their privacy policy in August 2016, Google have clarified that "this change makes it possible to use a single identifier

43 O. Lynskey, 'Track[ing] changes: an examination of EU Regulation of online behavioural advertising through a data protection lens' (2011) *European Law Review* 874, 885. However, she debatably believes that "only the most stringent regulatory measure (opt-in) could quell the general feeling of unease and apprehension caused by behavioural advertising" (*ibid*).

44 For a recent study on the national implementations with some interesting behavioural economics considerations, see IN Cofone, 'The way the cookie crumbles: online tracking meets behavioural economics' (2017) 25 (1) Int J Law Info Tech 38-62.

45 Information Commissioner's Office, 'Guidance on the rules on use of cookies and similar technologies' (2012) 15.

46 Garante per la Protezione dei Dati Personal, 8 May 2014, No. 229 *Individuazione delle modalità semplificate per l'informativa e l'acquisizione del consenso per l'uso dei cookie*. The implementation kit put together by DMA Italia and others, 'Cookie: Istruzioni per l'uso' ()2015), https://s3.amazonaws.com/iprs/files/attachments/20155/17bfe609-832b-4eb5-bd95-55239b5ae4f1__O.pdf, accessed 13 February 2017, interpreted this order by suggesting that non-technical cookies cannot be released without the user's prior consent.

47 Unlike the GDPR, there is currently no statement that confirms the intentions of the UK Governement about the ePrivacy Regulation. However, since it does not need to be transposed, once adopted the regulation will be effective in all the Member States (and it is likely that the UK will still be one of them).

48 For this problem, related also to the opacity of privacy policies, see Commission, 'A comprehensive approach on personal data protection in the European Union' (communication) COM (2010) 609 final, para 2.1.5.

49 European Parliament (n. 21) para I (see also *ibid.* para 20).

50 See Commission (n. 2) para 5.1.

associated with your account that gets used in Google products and across the web".[51]

Thirdly, the ePrivacy Regulation seems soundly based on the most recent studies of behavioural economics, that have concluded that there is clear evidence for "[r]econsidering the opt-in system, relying on web browsers instead of websites for the choice design, and taking into consideration the differences in privacy costs between permanent and session cookies".[52]

This paper will not analyse the proposal in details, also because it is likely that it will be significantly amended during the law-making process. However, it is noteworthy that even though the principle of privacy by default is referred to, art. 10(2) clearly enables an opt-out mechanism.[53] As long as the settings are visible and intelligible, it will be sufficient for software providers to offer the mere "option to prevent third parties from storing information on the terminal equipment" (recital 23). In so doing, the Commission has followed the Article 29 Working Party's recommendation to encourage "manufacturers of browsers and other software or operating systems […] to develop, implement and ensure effective user empowerment, by offering control tools within the browser".[54]

The draft ePrivacy Regulation further stresses that the information provided should concern

> *the risks associated to allowing third party cookies to be stored in the computer, including the compilation of long-term records of individuals' browsing histories and the use of such records to send targeted advertising* (recital 24).

Finally, given the circumventing practices highlighted in *Google* v. *Vidal-Hall,*[55] one can but welcome the precision whereby "[t]he choices made by end-users when establishing its general privacy settings of a browser or other application should be binding on, and enforceable against, any third parties" (recital 22).

In the explanatory memorandum, the Commission recognise that the consent rule did not reach its objectives, as users do not understand the meaning of the requests to accept tracking cookies. Moreover, they admit that the approach of the ePrivacy Directive is both over-inclusive and under-inclusive. Indeed, on the one hand the consent rule covers practices that do not intrude privacy. On the other hand, it can be interpreted as not applying to some tracking techniques, such as device fingerprinting. From the perspective of this paper, it is also noteworthy that, even though the primary focus is on data protection, the Commission is not affected by hemispatial neglect insofar as they justify the change of rules also by admitting that the implementation cookie rules are at present costly for businesses.

The proposal aims to take into account both competitiveness and data protection. Its likely impact will be that "a significant proportion of businesses would be able to do away with cookie banners and notices, thus leading to potentially significant cost savings and simplification". Those who serve OBA may indeed

51 'New options for your Google account' https://accounts.google.com/signin/newfeatures?cbstate=1&cbflow=promo-2-EN, accessed 10 February 2017.

52 Cofone (n. 43) 57.

53 Under Article 10(2) of the draft ePrivacy Regulation, "Upon installation, the software shall inform the end-user about the privacy settings options and, to continue with the installation, require the end-user to consent to a setting".

54 Article 29 Working Party, 'Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC)' 16/EN WP 240, para 3.

55 *Vidal-Hall & Ors* v. *Google Inc* [2014] EWHC 13 (QB) (16 January 2014); *Google Inc* v. *Vidal-Hall & Ors* [2015] EWCA Civ 311 (27 March 2015). On 30 June 2016, Google withdrew its appeal from the Supreme Court.

find it "more difficult […] to obtain consent if a large proportion of users opt for 'reject third party cookies' settings".[56] The centralization of consent, however, will leave it open to the website operators to obtain consent by means of individual requests to users.

Worryingly, whereas in the original version of the draft ePrivacy Regulation consent to OBA was linked to the GDPR, the current version[57] discussed within the Council of the EU no longer refers to the GDPR.[58] It is hoped that said reference will be reinstated.

The electronic communications regime is only an element of the data protection jigsaw puzzle. In the European regulator's view, "[b]ecause behavioural advertising is based on the use of identifiers that enable the creation of very detailed user profiles which, in most cases, will be deemed personal data, Directive 95/46/EC [soon the Regulation (EU) 2016/679] is also applicable".[59] The relevant obligations should be complied with not only by the ad network providers, but also by publishers. They can be both considered data controllers.[60] The Article 29 Working Party considers transparency as a key condition for individuals to be able to consent to the collection and processing of their personal data and exercise effective choice. However, what matters is not the information, but the actual possibility to dissent, which is usually denied[61]. Therefore, as a policy recommendation, one should go back to the version of art. 5(3) prior to the 2009 amendment[62] to the ePrivacy Directive. Indeed, the old provision recognised "the right to refuse such processing by the data controller".

There are two main ways of profiling users. One can distinguish between predictive profile and explicit profile. The former is created by observing individual and collective user behaviour over time, the latter from personal data that data subjects themselves provide to a web service. The privacy needs in the two scenarios are different. In the first one, indeed, users may not be aware of the fact they are being observed. Therefore, transparent and user-friendly information is critical. The role of this kind of profiling will increase exponentially given the developments of artificial intelligence and predictive analytics.[63] In the second one, an anti-paternalistic approach should

56 Explanatory memorandum to the draft ePrivacy Regulation, para 3.4.

57 Council of the European Union, doc. 1533/17 of 5 December 2017.

58 *Ibid.*, recital 18.

59 This is due, according to the Article 29 Working Party, to two reasons. On the one hand, behavioural advertising normally involves the collection of IP addresses and the processing of unique identifiers. On the other hand, the information collected in the context of behavioural advertising relates to a person's characteristics or behaviour and it is used to influence that particular person.

60 As clarified by the Article 29 Working Party, the publisher's responsibility does not cover all the processing activities necessary to serve behavioural advertising, for example, the processing carried out by the ad network provider consisting of building profiles, which are then used to serve tailored advertising. However, the publishers' responsibility covers the first stage, i.e. the initial part of the data processing, namely the transfer of the IP address that takes place when individuals visit their websites.

61 *Cfr* CJ Hoofnagle and others, 'Behavioral Advertising: The Offer You Cannot Refuse' (2012) 6 *Harvard Law & Policy Review* 273.

62 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 [2009] *OJ* L337/11.

63 *Cfr* S. Neelam and others, 'Artificial intelligence for designing user profiling system for cloud computing security: Experiment', in *2015 International Conference on Advances in Computer Engineering and Applications (ICACEA)* (IEEE 2015) 51; IR Kerr and M. Bornfreund,

avoid imposing too heavy information burdens on the profilers. The free choice to give away certain data eases the data protection-related obligations, as long as it is given the users the possibility to delete the account and/or the data any time and as long as the 'legals' are readable.[64] It is worth noting that the English and Wales High Court in *Spreadex* v. *Cochrane*[65] has clarified that the clauses of such never-ending legals are not binding for noncompliance with the unfair terms regime.[66]

The opinion sets out the information obligations of advertising network providers/publishers vis-à-vis data subjects. In particular, an ad network provider who wishes to store or gain access to information stored in a user's terminal equipment is allowed to do so in two events. Firstly, if it has provided the user with clear and comprehensive information in accordance with GDPR, inter alia, about the purposes of the processing. Secondly, if it has obtained the user's consent to the storage of or access to information on their terminal equipment, after having provided the information requested.

The Article 29 Working Party went on reasoning that, based on the definition and requirements for valid consent under art. 2 (h) of Dir 95/46/EC, "data subjects cannot be deemed to have consented simply because they acquired/used a browser or other application which by default enables the collection and processing of their information". This seems to be confirmed by the GDPR. Under recital 32, indeed, "[s]ilence, pre-ticked boxes or inactivity should not […] constitute consent." Art. 4(11) further provides that

> *'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.*

The opinion further clarifies the obligations set forth by the applicable legal framework, by pointing out that for browsers settings to be able to deliver informed consent, it should not be possible to circumvent the choice made by the user in setting the browser. We have already shown how the option to disable cookies is unworkable. Moreover, deleted cookies may be "respawned" by Flash cookies,[67] enabling the ad network provider to continue monitoring the user. New tracking vectors pop up constantly. For instance, HTML5 local storage and Cache Cookies via eTags. The latter is "capable of unique tracking even where all cookies are blocked by the user and 'Private Browsing Mode' is enabled".[68]

Finally, consent by browser setting to receive cookies in bulk is invalid, because it implies that users will accept future processing, possibly

'Buddy Bots: How Turing's Fast Friends Are Undermining Consumer Privacy' (2005) 6 *Presence* 647.

64 Guido Noto La Diega, 'Uber law and awareness by design. An empirical study on online platforms and dehumanised negotiations' (2016) *2 European Journal of Consumer Law* 383-413, suggests a practical tool to overcome the opaqueness of the legals: the "awareness by design" app.

65 *Spreadex LTD* v. *Cochrane* [2012] EWHC 1290. According to the court "[i]t would have come close to a miracle if [the defendant] had read" a specific sentence of a close, "let alone appreciated its purport or implications, and it would have been quite irrational for the claimant to assume that he had" (*ibid.* para 19).

66 The Court applied the Unfair Terms in Consumer Contracts Regulations 1999 (S.I. 1994/3159), which has now been replaced by the Consumer Rights Act 2015.

67 See MD Ayenson and others, 'Flash cookies and privacy II: Now with HTML5 and eTag respawning' (2011), https://fpf.org/wp-content/uploads/2011/07/Flash%20Cookies%20and%20Privacy%20II%20Now%20with%20HTML5%20and%20ETag%20Respawning.pdf, accessed 8 February 2017.

68 *Ibid.* 14. HTML5 may be used as well to enhance privacy.

without any knowledge of the purposes or uses of the cookie.

Not long after the above analysed opinion, the European Data Protection Supervisor delivered a speech in the same vein, where it called on the European Commission to ensure that art. 5(3) of the ePrivacy Directive is fully respected. The Supervisor pointed out that "systematic tracking and tracing of consumer behaviour online is a highly intrusive practice and is now rightly subject to more stringent requirements. Although initiatives for increased transparency and consumer control in the online environment are most welcome, this should not result in a limitation of consumer rights".[69] The statement criticises the European Commission for commending the EASA-IAB[70] Best Practice Recommendation[71] and Framework on behavioural advertising[72] and a US driven 'do-not-track' initiative,[73] because they do not adopt the consent rule. This cast (then proved on this point baseless) doubts on the position of the European Commission on this subject.

III. PROFILING, DIRECT MARKETING AND ALGORITHMIC DECISION-MAKING IN THE GENERAL DATA PROTECTION REGULATION

Under art. 14(1) of the Data Protection Directive, Member States shall grant the data subject the right "to object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing, or to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses". Moreover, Member States shall take the necessary measures to ensure that data subjects are aware of the existence of the right referred to in the first subparagraph of (b)" (art. 14(2)). Given that OBA is usually based on predictive

69 European Data Protection Supervisor, 'EDPS calls on the European Commission to ensure that safeguards for online behavioural advertising are respected' (Press release, 11 July 2011), https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/PressNews/Press/2011/EDPS-2011-08_Behavioural%20advertising_EN.pdf, accessed 8 February 2017. For the full speech, see P. Hustinx, 'Do not track or right on track? – The privacy implications of online behavioural advertising' (2011), https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Speeches/2011/11-07-07_Speech_Edinburgh_EN.pdf, accessed 8 February 2017.

70 European Advertising Standards Alliance and Interactive Advertising Bureau.

71 European Advertising Standards Alliance, 'Best Practice Recommendation on Online Behavioural Advertising' (2011), www.edaa.eu/wp-content/uploads/2012/10/EASA_BPR_OBA_12_APRIL_2011_CLEAN.pdf, accessed 11 June 2017.

72 Interactive Advertising Bureau, 'Europe EU Framework for Online Behavioural Advertising' (2011), www.edaa.eu/wp-content/uploads/2012/10/2013-11-11-IAB-Europe-OBA-Framework_.pdf, accessed 11 June 2017.

73 The reference is to the NAI (Network Advertising Initiative)'s self-regulatory framework. Subsequently, the framework was replaced by Network Advertising Initiative, 'Code of Conduct' (2015), www.networkadvertising.org/sites/default/files/NAI_Code15encr.pdf, accessed 8 February 2017. See also Network Advertising Initiative, 'Guidance for NAI Members: Use of Non-Cookie Technologies for Interest-Based Advertising Consistent with the NAI principles and Code of Conduct' (2015), www.networkadvertising.org/sites/default/files/NAI_BeyondCookies_NL.pdf, accessed 8 February 2017 and Federal Trade Commission, 'Self-Regulatory Principles for Online Behavioral Advertising' (2009), www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf, accessed 8 February 2017. The US framework, which revolves around the concept of interest-based advertising, will not be analysed. It should be said, however, that, under the current regime (para II.C.1 of Network Advertising Initiative, 'Code of Conduct'), companies should provide an opt-out mechanism for the collection and use of non-personally identifiable information for interest-based advertising purposes, whilst opt-in mechanisms are required for the use of sensitive data and precise location data.

analytics and algorithmic decisions, art. 15 ("Automated individual decisions") applies as well. Under its first paragraph, "Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc." This provision is particularly relevant, because it is not limited to direct marketing (OBA may be considered as different from, albeit connected to, direct marketing) and because thanks to its generic reference to automated decisions affecting (not necessarily from a pecuniary point of view) the user, it well fits OBA scenarios.

Nothing is expressly said on advertising, even though the same rules should apply to the processing carried out for both the purposes, since they are intrinsically connected and sometimes hardly distinguishable.

Conversely, one has to appreciate that at least the GDPR deals expressly with online advertising, even though it will not constitute a Copernican revolution.[74] Under its recital 58, it is stressed the importance, in order to comply with the transparency principle, that the information is concise, easily accessible, easy to understand, clear, in plain language and, where appropriate, accompanied by visualisation. Transparency is deemed to be "of particular relevance in situations where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him or her are being collected, such as in the case of online advertising".

Going on to the substantive law, the regulation of the right to object is not radically different from the one of the Data Protection Directive. Indeed, under art. 21(2) GDPR, "[w]here personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing". On the one hand, some elements seem to lower the user's protection. For instance, there is no longer reference to the fact that the exercise of the right to object should be free of charge[75] and that the data subject should be informed before personal data are disclosed to third parties or used on their behalf for the purposes of direct marketing. Moreover, no mention is made of the duty to ensure the users' awareness of the right to object. On the other hand, commendably, there are at least four elements which constitute evidence of an increased protection. Firstly, and more importantly, there is a shift from a subjective approach to an objective one. Under the directive, what mattered was the marketing purpose as anticipated by the controller. Under the GDPR, in turn, what matters is the marketing purpose per se, thus not allowing defenses whereby the controller asserted that they did not anticipate the use of the data for marketing purposes. Secondly, profiling is now expressly covered by the right to object (no reference whatsoever to profiling was contained in the directive). Thirdly, under

74 *Cfr* Ch. Kuner, *The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law* (2012) Bloomberg BNA Privacy and Security Law Report (2012) 1-15.

75 However, national lawmakers, regulators and judges may clarify this aspect. For instance, Information Commissioner's Office, 'Overview of the General Data Protection Regulation (GDPR)', (2016), 23, points out that "You must deal with an objection to processing for direct marketing at any time and free of charge".

art. 21(3), "[w]here the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes". From a policy point of view, it is a peculiar provision. Indeed, if the data subject has the right to object to the processing of its data for direct marketing purposes, it is in the nature itself of things that further processing for marketing purposes would be illegal. Therefore, it could be interpreted in a twofold way: either it is the sign of the lawmaker's awareness of the commonplace circumvention of anti-tracking tools, or it is a backdoor for the controllers that can leverage the provision to retain the data and use them for other purposes. In this case, they could keep using the data, without the user's consent, for purposes "compatible with the purpose for which the personal data are initially collected".[76] Fourthly, whereas under the directive the right to object could be exercised "on request", now the data subject "may exercise his or her right to object by automated means using technical specifications" (art. 21(5)). A sort of objection by design (e.g. through adblockers[77]). Even though that "may" weakens the provision, yet it may constitute an element adblocking companies could use against companies purporting to circumvent adblockers.

There are other unclear provisions. For instance, the right to object to direct marketing should be "explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information" (art. 21(4)). This risks to be the classic case of overload of information. For instance, should every website present the user with, say, separate notices for cookies and direct marketing? Let us see if the revision of the ePrivacy Directive will take account of these issues.[78]

Furthermore, it is debatable that the new provision on automated individual decision-making constitutes a step forward. The European Data Protection Supervisor has clarified that the "problem is not targeted advertising or the practice of profiling, but rather the lack of meaningful information about the algorithmic logic which develops these profiles and has an effect on the data subject".[79] Indeed, under art. 22(1) GDPR. The "data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her". This "similarly" may narrow the scope of the provision, if compared with the previous wording. However, two new aspects are to commend. Firstly, in principle automated cannot be taken on the basis of sensitive personal data. Secondly, even in the cases when the right not to be subject to automated decision-making does not apply, now the "data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his

[76] See art. 6(4) GDPR on the scenarios where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent.

[77] On the legality of these tools, see, for instance, J. Mullin, 'German judges explain why Adblock Plus is legal' (Ars Technica, 12 September 2016), https://arstechnica.com/tech-policy/2016/12/german-judges-explain-why-adblock-plus-is-legal/, accessed 12 February 2017.

[78] According to Commission Staff Working Document 'Online Platforms' accompanying the document Communication on Online Platforms and the Digital Single Market (SWD/2016/172 final) para 3.5.5.2, following the adoption of the GDPR, "which includes provision regarding the right of individuals to object, including to direct marketing, there is a review of the ePrivacy directive, which must be in line with the new data protection rules".

[79] European Data Protection Supervisor, 'Recommendations on the EU's options for data protection reform' (2015/C 301/01), para 3.1.

or her point of view and to contest the decision". A victory for those who think that human decision-making can still be better than the automated one.

A target of specific interest for the European legislator are children. Indeed, under recital 38, "specific protection should […] apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child". But how is this specific protection structured? Where the child is below the age of 16 years, "such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child" (art. 8(1)). One can hardly imagine a 15-year-old person calling his or her parents every time Facebook or Google are processing his or her data. However, this is not the most notable bit. Under art. 8(2), indeed, the controller "shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology". This might be used to justify the use of biometrics (such as face recognition, gait recognition, etc.) to verify the age of the user[80]. The remedy risks to be worse than the disease. Moreover, it has been submitted that "teenagers sometimes have a better understanding of online privacy challenges than their parents",[81] even though it is underlined that "some restrictions may be needed for children especially regarding sharing of information online and exposure to behavioural advertising".[82]

A cursory reading of the GDPR may give the impression that OBA no longer requires consent, because direct marketing is a 'legitimate interest' to process the users' personal data without their consent.[83] This may be interpreted as the result of a balance between data protection and freedom of enterprise. Indeed, competitiveness may be hampered, should an undertaking be required to obtain the users' consent, prior to any processing for OBA and direct marketing.[84] It is noteworthy, nonetheless, that companies that rely on legitimate interest for direct marketing purposes must ensure an absolute right to object.[85] Therefore, if a data subject objects, it is not left to the company the possibility to keep processing data by showing the legitimate interest override the individual's rights.[86]

However, recently the Article 29 Working Party has pointed out that, in light of the heighted standard for consent, it is likely that organisations will "need consent under the ePrivacy instrument for most online marketing messages or marketing calls, and online tracking methods including by the use of

80 See, for instance, BioPay biometric payments system to verify the age of customers of retail shops. According to JD Woodward Jr., *Is Biometrics an Age Verification Technology?* (RAND 2000) 2 however, "there are no age verification biometrics"

81 Commission (n. 12) annex 4, para 1.2.

82 *Ibid.*

83 GDPR, recital 47.

84 As pointed out by the UK Information Commissioner's Office (ICO), companies can rely on the legitimate interest justification for marketing if the use of the data is proportionate, if it has a minimal privacy impact, and if they can show that users 'would not be surprised or likely to object' (ICO, *Guide to the General Data Protection Regulation (GDPR)* (ICO, 21 November 2017) 39). Consent, however, may be required under under regimes such as The Privacy and Electronic Communications (EC Directive) Regulations 2003, SI 2003/2426.

85 *Ibid.* 41.

86 As further observed, the direct marketer "must stop processing personal data for direct marketing purposes as soon as you receive an objection. There are no exemptions or grounds to refuse." (*ibid.* 59).

cookies or apps or other software."[87] This can be explained in light of two considerations. First, the legitimate interest is not a *carte blanche*: it cannot be used to violate the data subject's fundamental rights, including data protection and privacy.[88] Second, direct marketing is not the same as OBA and it is likely to be the second step in a process where consent has already been acquired (e.g. when the advertisement had been served).[89]

Alongside consent and legitimate interest, another justification for the processing of personal data for OBA purposes might be the necessity in view of the performance of a contract.[90] Providers of online services having OBA as the key of their business model may argue that without OBA their business would not be sustainable and that, in this sense, OBA is necessary for the performance of a contract. However, it seems unlikely that this interpretation will prevail. In explaining what 'free consent' means, the Article 29 Working Party makes the example of a photo editing app that collects data about the GPS localization and for OBA purposes. The advisory body points out that '(n)either geo-localisation or online behavioural advertising are necessary for the provision of the photo editing service.'[91] It is hard to imagine many scenarios where this justification may apply. Even more clearly, the UK Information Commissioner's Office[92] has observed that even though OBA is a useful part of the customer relationship and may be necessary for one's business model, still it is not necessary to perform the contract e.g. in online purchases of goods.

More generally, there are provisions which are not directly focused on direct marketing, but that will affect it nonetheless[93]. For instance, the GDPR, unlike the directive, will apply to the processing carried out also by a controller or processor not established in the Union of personal data of subjects who are in the Union, whenever (i) the processing activities are related to either the offering of goods or services, irrespective of whether a payment by the data subject is required, and (ii) the processing activities relate to the monitoring of their behaviour as far as their behaviour takes place within the Union.[94]

Overall, an increased protection of the data subject, with some flaws. Alongside what said above, regulating OBA instead of direct marketing would have been preferable. For instance, it seems rather unfair that one can prevent companies from selling them prod-

87 Article 29 Working Party (n. 39) para 1. See also Commission, 'Guidance on the implementation/application of Directive 2005/29/EC on unfair commercial practices: Accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "A comprehensive approach to stimulating cross-border e-Commerce for Europe's citizens and businesses' (Commission Staff Working Document) SWD (2016) 163 final, para 3.3.4.7: "cookies should only be placed on a user's device after consent has been given".

88 Indeed, the legitimate interest goes with the proviso that "the interests or the fundamental rights and freedoms of the data subject are not overriding" (GDPR, recital 47, see also Art. 6(1)f).

89 Along the same lines, the latest version of the draft ePrivacy Regulation points out that direct marketing does not include 'displaying advertising to the general public on a website which is not directed to any specific identified or identifiable end-user' (Council of the European Union (n. 56) recital 32).

90 GDPR, art. 6(1)(b).

91 Article 29 Working Party (n. 39) para 3.1. In this scenario, consent itself would not comply with the GDPR because it would not be freely given, since one cannot access the app without consenting to said processing.

92 ICO (n. 83) 25.

93 On some other aspects s. C. Bauer and F. Eickmeier, 'GDPR: What's Relevant for the Use of Cookies & Identifiers in Online Marketing' (ExchangeWire, 24 May 2016), www.exchangewire.com/blog/2016/05/24/gdpr-whats-relevant-for-the-use-of-cookies-identifiers-in-online-marketing/, accessed 11 June 2017.

94 Commission (n. 86) para 5.2.13.

ucts, but cannot avoid OBA aimed to influence their voting preferences.

IV. EUROPEAN AND INTERNATIONAL SELF-REGULATION OF TARGETED ADVERTISING

In Europe, the public debate on OBA started as a sort of spin-off of the general debate on the 2009 amendment to the ePrivacy Directive. In 2010, then Digital Agenda Commissioner Neelie Kroes challenged the advertising industry to provide the European citizens with greater empowerment through transparency, consent, user-friendliness, and effective enforcement.[95] In a wise speech, the Commissioner underlined that one has to strike a balance between protection of personal data and enabling innovation in advertising and that "privacy regulation does not exist in a values vacuum".[96] Therefore, one has to take into account the effects of the regulation on industry, their practicality, and "we have to consider the long-term health of digital environments".[97] Hence, she called on a self-regulatory solution, with the caveat that "it will need to be one clearly based on the applicable EU legislation". More generally, the Commission has actively promoted "self and co-regulatory actions, including the 'Online Behavioural Advertising Roundtable' and the development of the W3C Do-Not-Track Standard".[98]

The IAB is a Global non-profit group open to companies engaged in the sale of interactive advertising and marketing. In April 2011, the group has developed a European self-regulatory framework for OBA (henceforth "the Framework"). The Framework lays down a structure for codifying industry good practices and establishes some principles to increase transparency and choice for web users within the EU/EEA which are binding upon the companies and associations part of IAB.

The pillars of the Framework are: notice, user choice, data security, sensitive segmentation, education, compliance and enforcement, and review. These principles apply consumer-friendly standards to OBA and the collection of online data in order to facilitate the delivery of advertising based on the preferences or interests of web users.[99]

Let us have a quick look to the second principle, that is user choice over OBA. Explicit consent is required only when a company collects and uses "data via specific technologies or practices that are intended to harvest data from all or substantially all URLs traversed by a particular computer or device across multiple web domains and use such data for OBA" (II.B).[100] Explicit consent is required as well if one seeks "to create or use such OBA segments relying on use of sensitive personal data" (IV.B). As to the other scenarios, third parties "should make available a mechanism for web users to exercise their choice with respect to the collection and use of data for OBA purposes and the transfer of such data to Third Parties for OBA" (II.A).

95 It should be noted that EASA interprets Kroes's pillars differently and it refers to them as "transparency, choice and control" (http://www.easa-alliance.org/issues/oba, accessed 11 June 2017).

96 N. Kroes, 'Towards more confidence and more value for European Digital Citizens' (European Roundtable on the Benefits of Online Advertising for Consumers, 17 September 2010), http://europa.eu/rapid/press-release_SPEECH-10-452_en.htm, accessed 8 February 2017.

97 *Ibid.*

98 Commission (n. 11), para 5.2.

99 The regulation of the content of online advertisements and the advertisement delivery are out of the scope of the Framework.

100 Under principle II.C of the Framework, then, companies "that have obtained Explicit Consent pursuant to II.B should provide an easy to use mechanism for web users to withdraw their Explicit Consent to the collection and use of such data for OBA".

Such choice should be made available in two ways. Firstly, third parties "should give clear and comprehensible notice on their web sites describing their Online Behavioural Advertising data collection and use practices" (I.A.1).[101] Secondly, can manage their consent to OBA on the YourOnlineChoice.eu website (also "OBA User Choice Site").

It is commendable the adoption of a user-friendly icon that contains a hyperlink to the OBA User Choice Site or to the third party notice, even though future quantitative research should assess how many users understand the meaning of the icon.[102]

Anyway, this tool can be used to turn off OBA by some or all companies. However, the said site is not very clear, since it does not show the user's status with regard to most of the companies and the majority of the displayed companies were encountering technical issues, thus impeding the retrieval of the status. Moreover, it is not easy to assess the reliability of the tool.

The IAB's frameworks, based on an opt-out mechanism with minor exceptions, is complemented by the EASA Best Practice Recommendation on OBA (hereinafter, also "the Recommendation"). EASA is non-profit organisation dealing with advertising self-regulation issues and bringing together thirty-four national advertising self-regulatory organisations and sixteen organisations representing the advertising industry.

The Recommendation provides "a pan-European, industry-wide self-regulatory standard for OBA, which empowers consumers across Europe".[103] Even though self-regulation can be a positive option, it presents a number of shortcomings, including its problematic enforceability. This is an argument for resisting a complete deregulation of the phenomenon.

It recommends the industry members to a) Clearly support the adoption at local level of rules on OBA based on the Recommendation; b) Clearly support the adoption at local level of the new remit and rules for the handling of complaints on OBA by self-regulatory organisations; c) Establish a clear agreement with the ad networks regarding the handling of complaints of a non-technical nature by the advertising self-regulatory bodies; d) Ensure adequate industry and consumer awareness of the above; e) Ensure the necessary linkup with the consumer controls page to create a one stop shop for consumer feedback and complaints; f) Ensure the necessary linkages between industry compliance monitoring reports and the complaint handling processes; g) Establish robust measures for sanctions related to repeat offenders or rogue traders.

[101] The notice should include: (a) The identity and contact details of the third party; (b) The types of data collected and used for the purpose of providing OBA, including an indication or whether any data is "personal data" or "sensitive personal data"; (c) The purposes for which OBA data are processed and the recipients to whom such data might be disclosed; (d) An easy to use mechanism for exercising choice with regard to the collection and use of the data for OBA purposes and to the transfer of such data to Third Parties for OBA; (e) The fact that the company adheres to these Principles; and (f) A link to www.youronlinechoices.eu, a consumer-focused website and education portal.

[102] European Parliament (n. 21) para 39 called on "the insertion of the clearly readable words 'behavioural advertisement' into the relevant online advertisements, as well as a window containing a basic explanation of this practice". Possibly a positive improvement, even though the said future research should also assess if users know what OBA is. TRUSTe and EDAA, 'European Advertising Consumer Research Report 2016' (2017) http://www.edaa.eu/wp-content/uploads/2017/01/EDAA-Report-2016-Final-13012017.pdf, accessed 11 February 2017, celebrate the increase of awareness, but the respondents were asked whether they had seen the icon before, not whether they understood what it meant.

[103] http://www.easa-alliance.org/issues/oba, accessed 11 June 2017.

The Recommendation draws its principles from the ones of the IAB Framework; however, it leaves out data security and education. EASA adopts the same opt-out mechanism with limited exceptions proposed by IAB, with the (unnecessary?) precision that when "a web user exercises his/her choice and objects to OBA data collection, OBA processes should no longer be used by that entity to facilitate the delivery of targeted online advertising to that user's browser".[104]

Probably the most interesting part of the Recommendation regards the enforcement. Consumers provide feedback or complain either directly to a company, to a third party or website operator, a regulatory authority, a self-regulatory body or a similar local alternative dispute resolution body. These different routes could all transit a one-stop shop for compliance. This consists of a web page where the transfer of feedback and complaints is passed to the relevant process and organisations. One has to distinguish two scenarios. On the one hand, consumer feedback regarding technical issues on OBA (e.g. about who is serving OBA) would be handled by an industry web-based interface. On the other hand, consumer complaints arising from dissatisfaction with the way their initial feedback or complaint have been handled via the industry interface or complaints about more general privacy issues or issues related to the content of advertising would be handled by a process involving the advertising self-regulatory bodies.

Given the growing importance of non-European advertising companies, one should have a look at the international self-regulation of advertising. The EASA has contributed to the revision process of the ICC Code on Marketing Communication and Advertising.[105] It is interesting that, when commenting the most significant changes to the Code, the first example done by the ICC is that "[f]or the first time the Code addresses responsibility with respect to the use of online behavioural targeting in the delivery of advertisements". Indeed, now art D7 regulates "Provisions for online behavioural advertising (OBA)", in a way which is unsurprisingly very similar to the one of IAB and EASA. Limiting the focus on the notice mechanism, it is provided that third parties and website operators should give "clear and conspicuous notice on their websites describing their OBA data collection and use practices".[106] It is not commendable that "notice should be provided through deployment of *one or multiple* mechanisms for clearly disclosing and informing Internet users about data collection and use practices".[107] This could lead to an overload of information. Explicit consent is limited to "[t]hose collecting and using data via specific technologies or practices that are intended to harvest data from all or substantially all websites traversed by a particular computer or device across multiple web domains, and use such data for OBA".[108] Two provisions of the Code deserve a particular mention. Firstly and more importantly, under art D8, "[a]nyone taking part in the planning, creation or execution of digital marketing communications including OBA, has a degree of responsibility […] for ensuring the observance of the Code towards those affected, or likely to be affected". This provision is flexible enough to

104 European Advertising Standards Alliance (n. 70), Principle II.A.

105 International Chamber of Commerce, 'Advertising and Marketing Communication Practice Consolidated ICC Code' Document No. 240-46/660 of August 2011, www.codescentre.com/media/2083/660%20consolidated%20icc%20code_2011_final%20with%20covers.pdf, accessed 11 June 2017 (hereinafter also 'ICC Code').

106 ICC Code, Art D7.1.

107 *Ibid.* (italics added).

108 *Ibid.* Art D7.2.

fit the intricate supply chain of advertising[109] (with responsibilities mainly shared[110] between the different OBA companies). Secondly and appropriately, "[t]ransparency of data information collection and use, and the ability for users and consumers to choose whether to share their data for OBA purposes is vital".[111]

The international and European self-regulation OBA systems are based on an opt-out mechanism which does not seem entirely compliant with the ePrivacy Directive[112] and with the GDPR. What is worse, the analysed self-regulation initiatives "create the wrong presumption that it is possible to choose not be tracked while surfing the Web".[113] Moreover, the opt-out tools can be and are sometimes ineffective. For instance, as one can read from the last report[114] on cross-border complaints,[115] in all the cases which regard OBA, the users were complaining about the opt-out mechanism because "they had continually been unable to opt out of OBA data collection and use"[116] or "[d]espite selecting the 'Off' mode, the website kept on reverting to 'On' mode".[117] As already said, even if the right to consent is critical, one should start from ensuring the right to dissent, which is hardly effective. Furthermore, even though there seems to be an increasing percentage of users clicking on the OBA icon,[118] there is no evidence that users actually know and understand what OBA is. On the contrary, a large-scale study[119] found that only 11% of the users understand the cookies policies and 61% do not believe that there are advertisements based on email content. A more recent study,[120] finally, confirmed that the knowledge on what OBA is and how it works is still insufficient and that groups of Internet users did not differ in terms of knowledge, although they did differ in terms of privacy concerns.

A. Filing a complaint in the UK. Non-judicial remedies: rules and hurdles

What if a UK user wants to file a complaint because, for instance, a company circumvented their "do not track" option and covertly tracked them in order to serve them with OBA. As in

109 See Commission (n. 2) para 5.1.

110 Commission (n. 12) para 10.1.2, presents OBA as an example of joint controllership, because "publishers rent website-advertising space and network providers collect and exchange information on users".

111 ICC Code, Art D7.

112 This is the main conclusion of Article 29 Working Party, 'Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising' 02005/11/EN WP 188.

113 *Ibid.*

114 In the previous report, European Advertising Standards Alliance, 'Cross-Border Complaints Quarterly Report no. 67 January – March' (2015), www.easa-alliance.org/sites/default/files/2015%20EASA%20Cross-Border%20Complaints%20Report%20No.%2067.pdf, accessed 8 February 2017, the only case about OBA regards the opt-out mechanism, because the user "had continually been unable to opt out of OBA data collection and use". The Autorité de Régulation Professionnelle de la Publicité resolved the complaint informally.

115 European Advertising Standards Alliance, 'Cross-Border Complaints Quarterly Report no. 68 April – June' (2015), www.easa-alliance.org/sites/default/files/2015%20EASA%20Cross-Border%20Complaints%20Report%20No.%2068.pdf, accessed 8 February 2017.

116 2914-5 Rubicon Project; 2916-7 AudienceScience; 2922-3 Xaxis, 2920-1 Infectious Media, 2918-9 Captify. The Advertising Standards Authority upheld the complaints.

117 2969 Eyeota Ltd. The Deutsche Datenschutzrat Online-Werbung decided that the problem lied with the complainant: their technical device, privacy setting or Internet connection.

118 One in four surveyed users (excluding Hungary) in TRUSTe and EDAA (n. 101) have engaged with the OBA icon.

119 A. McDonald and L. Faith Cranor, 'Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising' (2010) TPRC https://ssrn.com/abstract=1989092, accessed 13 December 2016.

120 EG Smith, G. Van Noort, and H. Voorveld, 'Understanding online behavioural advertising: User knowledge, privacy concerns and online coping behaviour in Europe' (2014) 32 *Computers in Human Behavior* 15-22.

Google v Vidal-Hall,[121] one could decide to go for the judicial root mainly founding oneself on the misuse of private information. Here a brief overview of the non-judicial route is presented and its effectiveness is assessed.

In the UK, the Advertising Standards Authority (ASA) is the independent advertising regulator; they enforce the codes drafted by the Committee of Advertising Practice (CAP). ASA administers the non-broadcast Advertising Code ('CAP Code') and its Appendix 3 regards OBA.

These are the main rules, whose breach can found an action. Third parties should provide clear and comprehensive notice about the collection and use of web viewing behaviour data for the purposes of OBA. Moreover, they should make available a link to a relevant mechanism that allows the consumer to opt out (31.1.1-2 CAP Code). Furthermore, third parties are not allowed to create interest segments designed for children aged 12 or under (31.1.3 CAP Code). Finally, "explicit consent" is required only if the third parties collect information about substantially all websites visited by web users on a particular computer (31.1.4 CAP Code).

The reference to "third parties" makes already clear that the scope of the rules is very limited. Indeed, they do not apply to the collection and use of information for OBA purposes by web site operators on their own website (first-party OBA). Out of the scope of the CAP code are also mobile advertising and advertising on smart devices (allegedly for technical reasons), as well as interactive display advertisements, contextual advertising, and complaints falling under the remit of other authorities (e.g. about data protection and discrimination).

If the complaints falls within the scope of the CAP code, the user can file it on the ASA's website.[122] Uncommendably, the number and nature of the requirements of the complaint make the assistance of a qualified lawyer necessary. The complaints shall indicate: i. The URL the user was visiting; ii. The identity of the 'ad network' (the brand will not do); iii. A screenshot of the advertisement; iv. If the advertisement carried the OBA notice, a screenshot of the webpage the notice linked to; v. The name of the browser; vi. Confirmation of having attempted to opt-out of OBA.

Browsing the ASA's website, it was not possible to find rulings concerning OBA. This could be for a number of reasons. Firstly, the scope of the CAP code is very narrow. Secondly, filing a complaint is not straightforward. Thirdly, OBA illiteracy is commonplace: users do not know what OBA is and, if they do, they do not know how to react.

Education campaigns might be helpful in raising the necessary awareness. Alongside teaching what OBA is, what are the user's rights (also in terms of judicial and non-judicial remedies), it would be critical to explain what are the technical controls available to the users. For instance, it should be clarified how to set the different browsers in order to opt out of OBA and point out that one needs to repeat the operation from all the devices and browsers in use. Moreover, one should explain that deleting the cookies is not an effective reaction. Indeed, the process of opting out of OBA requires a cookie itself: by deleting all cookies, the user is opting in again. Furthermore, it should be

[121] *Google* (n. 54).

[122] https://www.asa.org.uk/make-a-complaint.html. This is a form of alternative dispute resolution. If they ASA finds that their rules have been breached, they issue an order to change or withdraw the advertisement and they make the findings available to the media. In case of persistent lack of compliance, the ASA can refer the advertiser to other bodies for further action (i.e. Trading Standards and Ofcom). For more information, see ASA, *Making a complaint* (Advertising Standards Authority 2017).

illustrated how to opt out of a large number of businesses via www.youronlinechoices.com. A good advice would be, then, to use tools that show who is traking the users (e.g. Lightbeam), as well as adblockers (e.g. Privacy Badger, Disconnect, Adblock Plus, Ghostery). Lastly, it should be made clear that these controls are not completely reliable (they can be circumvented) and that they have limitations.

V. THE USE OF PERSONAL DATA TO HINDER COMPETITION. FACEBOOK AND WHATSAPP: FROM THE CONCENTRATION TO THE TRANSFER OF THE LATTER'S USER DATA TO THE FORMER'S IP PORTFOLIO

OBA companies can leverage the data in their IP portfolio to carry out unfair commercial practices and, more generally, to jeopardise competition.[123] Too many data can mean too much power.[124]

The OBA market is clearly skewed and oligopolistic with Google, Facebook, and few other companies leading it.[125] Economics literature[126] has shown that advertising may operate as a barrier to entry and the Commission consider the relevant expenditure as sunk costs.[127] This was confirmed by *United Brands* v. *Commission*[128] that accepted that consumers chose Chiquita bananas instead of the competitors' ones because of the preference induced by very large-scale advertising campaigns, which acted as a barrier to entry.

Coming more specifically to OBA, exploiting the users' data without them knowing it or, more generally, using the users' data illegally does not only damage the consumers, but it can also harm competitors. Price discrimination and dynamic pricing based on profiling activities (e.g. offering a different price if one accesses a website from an old desktop or from an iPhone) might as well seem an unfair practice. However, the Commission has clarified that under the Unfair Commercial Practices Directive[129] "traders are free to determine their prices if they duly inform consumers about the prices or how they are calculated".[130] One should note that some provisions of the said directive do not entirely fit the reality of OBA. For instance, under art. 5 para 3,

123 The European regulation of competition in the field of advertising still sees targeted advertising as the advertising targeted to a specific Member State, not the one that singles out a user usually based on its behaviour. For instance, the Court of Justice stated that social, linguistic and cultural features, which can be specific to a given Member State, may justify a different interpretation of the message communicated in the commercial practice by the competent enforcement authority or court (Case C-220/98 *Estée Lauder Cosmetics GmbH & Co. OHG* v. *Lancaster Group GmbH* [2000] ECR 117, para. 29). On 25 May 2016, it has been adopted Commission (n. 86), an updated version of the 2009 Guidance on the application of the Unfair Commercial Practices Directive. This seems to allow an extension to the newly understood targeted advertising, when the Commission observes that "[w]hen designing their commercial messages, traders may, at times and in light of the specific nature of the products at stake, need to take certain social, linguistic and cultural features into account which are typical of the average consumers to which the products are targeted" (*ibid.,* para 2.5).

124 This is also the viewpoint of A. Vetrò and F. Ruggiero, 'Internet delle cose, troppi dati danno troppo potere: ecco i rischi per la concorrenza' (2017), www.agendadigitale.eu/smart-cities-communities/cittadinanza-vetro---internet-delle-cose-correggere-le-distorsioni-o-si-rischiano-effetti_2915.htm, accessed 13 February 2017, that refer the idea to the Internet of Things (but it can be easily generalised).

125 Commission (n. 2) para 5.1.

126 See, for instance, JS Bain, *Barriers too New Competition* (Harvard University Press 1956), but *contra* G. Stigler, 'The economics of information' (1961) 69 J. Polit. Economy 213, quoted by A. Jones and B. Sufrin, *EU Competition Law* (5th edn, OUP 2014) 92.

127 *Nestle/Perrier* (Case M.17) [1992] *OJ* L356/1, para 97.

128 Case 27/76 [1978] ECR 207 para 248.

129 The Unfair Commercial Practices Directive is complemented, as to the business-business relations, by the Misleading and Comparative Advertising Directive.

130 Commission (n. 86) paras 5.2.11-5.2.12.

> *[c]ommercial practices which are likely to materially distort the economic behaviour only of a clearly identifiable group of consumers who are particularly vulnerable to the practice or the underlying product […] in a way which the trader could reasonably be expected to foresee, shall be assessed from the perspective of the average member of that group*.

With artificial intelligence and current tracking and profiling techniques, it is highly problematic to assert that the company cannot foresee the vulnerability of the target. Therefore, one should not look at the average member of the group, but at the single user. The definition itself of unfair commercial practices, with its reference to the average consumer, might need to be adapted accordingly.[131]

Another issue is the persistency of unwanted targeted advertisements. This may be covered by Point No. 26 of Annex I of the Unfair Commercial Practices Directive (on "Commercial practices which are in all circumstances considered unfair", which prohibits making persistent and unwanted commercial communications to consumers ('spam').[132]

Lastly, it has been suggested that "an undue increase in the use of personal data may very well be compared to excessive prices",[133] thus amounting, potentially, to a practice constituting abuse of dominant position.

Another common practice that is relevant from a competition law perspective, then, is tying. As noted by the European Data Protection Supervisor, indeed, in digital two-sided markets where free services are paid for through data and OBA, "marginal costs of supplying online services in a new market are low, and there is a distinct tendency towards tying of services".[134]

An interesting competition law case related to OBA is *Attrakt s.r.l.* v. *Google Ireland Ltd*.[135] Attrakt was a search engine whose revenues depended on advertising based on Google AdWords and Google AdSense contracts. In 2013, Google disabled Attrakt's AdSense account (and retained €503.400 of advertising revenues) following a supposed breach of the AdSense policy, but they refused to justify the decision, regardless of Attrakt's requests. Consequently, the latter had to shut down

131 For a clear explanation of the functioning of the system with regard to the average consumer and the average member in the UK has been provided by Department of Business Innovation & Skills, 'Misleading and Aggressive Commercial Practices – New Private Rights for Consumers. Guidance on the Consumer Protection (Amendment) Regulations 2014' (2014), paras 26 ff www.gov.uk/government/uploads/system/uploads/attachment_data/file/409334/bis-14-1030-misleading-and-aggressive-selling-rights-consumer-protection-amendment-regulations-2014-guidance.pdf, accessed 8 February 2017.

132 The main categories of unfair commercial practices are misleading practices and aggressive ones. Targeted advertising can be misleading inasmuch it is based on a deep knowledge of the consumers, hence allowing companies to exploit their weaknesses in order to mislead them. Targeted advertising may be aggressive as well. However, the wording of art. 8 of the Unfair Commercial Practices Directive is rather narrow, referring to "harassment, coercion, including the use of physical force, or undue influence [which] significantly impairs or is likely to significantly impair the average consumer's freedom of choice or conduct".

133 A. Gebicka and A. Heinemann, 'Social Media & Competition Law' (2014) 2 *World Competition* 149, 165. However, one joins G. Surblyte, 'Competition Law at the Crossroads in the Digital Economy: Is it All About Google?' (2015) 5 *EuCM* 170, in saying that "although data could be considered the 'currency' of the Digital Economy in very general terms, it cannot precisely be equaled to the concept of a 'price'".

134 European Data Protection Supervisor, 'Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy' (2014), para 66. https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2014/14-03-26_competitition_law_big_data_EN.pdf, accessed 9 February 2017.

135 Tribunale di Milano sez spec impresa, 5 May 2016 no 7638, www.attrakt.com, accessed 10 February 2017.

for lack of funds.[136] Alongside the breach of contract (for the unfair way the withdrawal was exercised) and its partial invalidity (liability caps in standard contracts must be specifically accepted in writing), the *Tribunale di Milano* found there had been an anti-competitive conduct called abuse of economic dependence. Under art. 9 of the *legge* no 192/1998,[137] there is economic dependence when an undertaking can determine, in the trade relations with another undertaking, an excessive imbalance of rights and obligations. The expressly makes the example of the arbitrary interruption of trade relations. Alongside the said excessive imbalance, judges are required to take into account the possibility to find satisfactory alternatives on the market. In this case, there was evidence of dependence in the contracts, the emails, the exclusivity of the relation, and the fact that Attrakt's revenues come exclusively from Google. The abuses consisted in the burdensome imposed contractual terms, the arbitrary withdrawal, and the retention of due revenues. Finally, the *Tribunale* held Google liable for the said contractual breaches and anti-competitive behaviours, which were sanctioned with a considerable fine and the declaration of partial invalidity of the contract. Thus, the oligopolistic and imbalanced structure of the advertising market was confirmed, while reaffirming that "advertising is an essential part of the competitive process".[138]

As a side note, it is interesting to see that intellectual property was the (asserted) reason why Google did not provide a justification for the withdrawal. Indeed, they denied this information "because we have a need to protect our proprietary detection systems, we're unable to provide our publishers with any details about their account activity". However, the court struck a balance between the interests of competition and those of intellectual property, and it favoured the former. Along the same lines, in the first case of pay-for-delay in the pharmaceutical industry,[139] the General Court has reaffirmed, competition law can be used as a tool to prevent some of the IPRs holders' abuses. Let us see if this could be the case in a recent event regarding the transfer of WhatsApp users' data to Facebook and let us assess if data protection considerations could be taken into account in competition law cases.

Thanks to the big data controlled by Facebook (directly and through its subsidiaries), the popular social network platform can be considered one of the strongest actors in the targeted advertising world.[140] Indeed, in 2016, Facebook's advertising revenue has been

136 For a comment to the ruling see Marco Lo Bue, 'Google held liable in Italy for abuse of economic dependence' (Trust in IP, 20 October 2016), http://trustinip.com/google-italy-abuse-economic-dependence, accessed 10 February 2016.

137 *Legge* 18 June 1998, no 192, G.U. 143/1998.

138 R. Whish and D. Bailey, *Competition Law* (8th edn, OUP 2015) 583. For an example, see Commission Decision (EU) 2016/1698 of 20 February 2014 concerning measures SA.22932 (11/C) (ex NN 37/07) implemented by France in favour of Marseille Provence Airport and airlines using the airport (notified under document C (2014) 870), para 199.

139 Case T-472/13 *H. Lundbeck A/S and Lundbeck Ltd* v. *European Commission* (General Court, 8 September 2016). The Danish pharmaceutical company Lundbeck's basic patent for the blockbuster antidepressant medicine citalopram had expired. Some generic producers were, hence, preparing cheaper generic versions of citalopram. Therefore, in order to prevent competition, Lundbeck paid them not to enter into the market, thus harming patients and health care systems. This allowed Lundbeck to keep the price of its blockbuster drug citalopram artificially high. Consequently, upholding the Commission's decision, the General Court found that the agreements eliminated the competitive pressure from the generic companies and are "a restriction of competition by object". There are several examples of use of competition law to limit IPRs, but the classic one is the exhaustion principle.

140 Google remains the main player, but it is less relevant from the perspective chosen. For some considerations on it with regards to OBA, see, for instance, Noto La Diega (n. 13).

nearly USD 27 billion, which means a growth of 57% if compared to 2015.[141]

One may take many approaches in choosing Facebook as a use case to talk about targeted advertising. The most overlooked perspective from which one can observe the said phenomenon is competition. There are many aspects of the Commission's decision[142] on the Facebook / WhatsApp concentration that offer a sample of the relevance of targeted advertising[143] from a competition law perspective. This decision should be read again today in light of the use Facebook has started to do of WhatsApp users' data for targeted advertising purposes in August 2016.[144]

To briefly recap the facts, in the summer of 2014, the European Commission received notification of a proposed concentration pursuant to art. 4 of the Merger Regulation,[145] and following a referral pursuant to art. 4(5) of the Merger Regulation, by which Facebook, Inc. acquired within the meaning of art. 3(1)(b) of the Merger Regulation control of the whole of WhatsApp Inc. by way of purchase of shares (the "Transaction"), for a price of USD 19 billion.

I assume that the vast majority of the readers are familiar with the companies and services involved in the concentration. One of the main differences between Facebook and WhatsApp is that the former provides online advertising services, the latter does not. One could have been surprised by the news of the Transaction, given that Facebook had already its own instant messaging app, i.e. Messenger. In assessing the closeness to competition, however, the Commission explains that Messenger is a stand-alone app that has been developed from functionalities originally offered by the Facebook social network. From the above, some differences follow. According to the Commission, one of them is that, contrary to WhatsApp, "Messenger enables Facebook to collect data regarding its users that it uses for the purposes of its advertising activities".[146] This is no longer the case after the update to the "legals" of WhatsApp occurred on 25 August 2015.[147] The main news is that Facebook will use the WhatsApp account information for targeted advertising purposes. What is worse is that: i. The chosen mechanism is an opt-out one. ii. The opt-out procedure is not straightforward.[148] iii. The users have only 30 days after the update to opt out. iv. New users have no right to opt out. Especially the last bit seems hardly enforceable.

141 'Facebook Reports Fourth Quarter and Full Year 2016 Results' https://investor.fb.com/investor-news/press-release-details/2017/Facebook-Reports-Fourth-Quarter-and-Full-Year-2016-Results/default.aspx, accessed 11 June 2017.

142 *Facebook/WhatsApp* (Case COMP M.7217).

143 The decision refers mainly generally to 'online advertising', but given that the company involved carries out mainly targeted advertising, the author believes that *Facebook* (n. 141) can constitute a good prism through which one can observe the competition implications of targeted advertising.

144 https://www.whatsapp.com/legal/#key-updates.

145 Council Regulation (EC) No. 139/2004 of 20 January 2004 on the control of concentrations between undertakings [2004] *OJ* L24/1 (the Merger Regulation).

146 *Facebook* (n. 141) para 102.

147 https://www.whatsapp.com/legal/#terms-of-service and https://www.whatsapp.com/legal/#privacy-policy. For the previous versions, see https://www.whatsapp.com/legal/?doc=terms-of-service&version=20120707 and https://www.whatsapp.com/legal/?doc=privacy-policy&version=20120707. In the old version of the terms, no reference was made to advertising (be it Facebook's advertising or WhatsApp's one). In the old privacy notice, in turn, it was said that "[w]e are (not fans of advertising). WhatsApp is currently ad-free and we hope to keep it that way forever. We have no intention to introduce advertisement into the product, but if we ever do, will update this section".

148 *Cfr* N. Lomas, 'WhatsApp to share user data with Facebook for ad targeting – here's how to opt out' (TechCrunch, 25 August 2016), https://techcrunch.com/2016/08/25/whatsapp-to-share-user-data-with-facebook-for-ad-targeting-heres-how-to-opt-out/, accessed 8 February 2017.

Finally, it is not clear which information Facebook will be able to use. Indeed, even though in the "key updates" recap, WhatsApp refers only to the account information, in the new ToS it is said that

> *Facebook and the other companies in the Facebook family also may use information from us to improve your experiences within their services such as making product suggestions (for example, of friends or connections, or of interesting content) and showing relevant offers and ads. However, your WhatsApp messages will not be shared onto Facebook for others to see. In fact, Facebook will not use your WhatsApp messages for any purpose other than to assist us in operating and providing our Services.*

The wording suggests that WhatsApp messages are not shared, but all the rest of information can be used (and shared). This includes, for instance, phone number, profile name and photo.

With regard to assessment as to whether Facebook and WhatsApp were direct competitors, the Commission considered they were not and, therefore, it authorised the concentration. It can be argued that, if the Commission was notified today of the said transaction (Why?), the conclusion would be different. Indeed, at that time it had been said that Facebook could be considered as in direct competition with Twitter or Google Hangouts, but not with WhatsApp, which was in turn closer to Viber.[149] However, if one of the main differences between Facebook Messenger and WhatsApp was that the latter's data were not used for the advertisements served by the former, which is no longer the case, it is clear that the forecast capabilities of the Commission failed.

Whereas other "free" consumer communications apps monetise thanks to advertising, in-app purchases and stickers, "Messenger is not currently monetised: it is funded by the monetisation of Facebook's networking platform through advertising",[150] therefore, it is to believe that the use of the data created through the use of Messenger is the main reason for the existence itself of this app. This could be criticised, since users are hardly aware of their private conversations being exploited for targeted advertising purposes. It is not casual that, as seen above, this has been the subject of a written question to the Commission.[151]

In the concentration, there are three relevant markets: consumer communications services, social network platforms, and online advertising. Let us have a look at the latter, which is more relevant to the topic of this paper.

Facebook's activities in the advertising sector consist of the provision of online (non-search) advertising services on Facebook's core social networking platform and on Instagram[152] (which is its subsidiary as well), both on computers and on mobile devices. As noted above in the Facebook / Mrb&b use case, Facebook collects its users' data (also through its subsidiaries[153]) and analyses them in order to

149 *Facebook* (n. 141) paras 106-107.

150 *Ibid.* fn 42.

151 M. Tarabella, 'Question for written answer E-000850/13 to the Commission' (28 January 2013).

152 See section "Rights", § 2 of Instagram Terms of Use, effective as of 19 January 2013, https://help.instagram.com/478745558852511, accessed 8 February 2017: "Some of the Service is supported by advertising revenue and may display advertisements and promotions, and you hereby agree that Instagram may place such advertising and promotions on the Service or on, about, or in conjunction with your Content. The manner, mode and extent of such advertising and promotions are subject to change without specific notice to you".

153 Facebooks owns Instagram, WhatsApp, PrivateCore, and Oculus VR.

serve targeted advertisements on behalf of advertisers.

The Commission has investigated the market definition as regards advertising. The product market definition is quite straightforward. Following its precedent assessments,[154] the Commission distinguishes between the provision of online and offline advertising space. The market investigation carried out in the *Facebook / WhatsApp* case supported the existence of a further sub-segmentation of the online advertising market between search and non-search advertising. Indeed, most advertisers see search and non-search advertisements as non-substitutable, since they serve different purposes (search advertisements mainly generates direct user traffic to the merchant's website, while non-search advertisements mainly build brand awareness).[155]

From our perspective, what is more relevant is the assessment with regard to a further sub-sub-segmentation. Indeed, the Commission examined whether a separate product market should be defined for the provision of online non-search advertising services on social networking websites. A number of respondents considered that other forms of non-search advertising are not as effective as advertising on social networking websites and "notably on Facebook, due to Facebook's large and highly engaged audience and its ad targeting opportunities".[156] Nonetheless, the Commission decided to leave to question open "because the Transaction would not give rise to serious doubts as to its compatibility with the internal market under any[157] such narrower product market definition".[158]

Therefore, from a product perspective, the relevant market is online advertising. As to the geographic market, most respondents to the Commission's market investigation stated that advertisers typically purchase online advertising space and conduct advertising campaigns on a national (or linguistic) basis.[159] Therefore, In line with the *Google / DoubleClick* and *Microsoft / Yahoo! Search Business* decisions, the Commission reached the questionable conclusion that the online advertising market and its possible sub-segments should be defined as national in scope or alongside linguistic borders within the EEA.[160]

The Commission took a rather formalistic approach,[161] by rigidly distinguishing between a competition law approach and a privacy law approach. This approach is open to criticism, because data are digital assets that live at the crossroads of privacy, intellectual property, competition, and consumer protection; therefore, an integrated one should have been more appropriate.[162] The Commissions seems

154 *Microsoft/Yahoo! Search Business* (Case COMP/M.5727) [2004] *OJ* L24/1 para 61; *Google/DoubleClick* (COMP/M.4731) [2008] OJ C 184/10 paras 45-46, 56.

155 *Facebook* (n. 141) para 76.

156 *Ibid.,* para 77.

157 Another question which has been left open regards a possible distinction between online advertising on different platforms (essentially on computers or on mobile devices).

158 *Facebook* (n. 141) para 79.

159 However, a number of respondents also pointed out that, depending on the type of campaign, global companies may also procure advertising space on a broader (sometimes global) geographic scale.

160 *Facebook* (n. 141) para 83.

161 "Any privacy-related concerns flowing from the increased concentration of data within the control of Facebook as a result of the Transaction do not fall within the scope of the EU competition law rules but within the scope of the EU data protection rules" (*Facebook* (n. 141) para 164).

162 One joins the European Data Protection Supervisor's opinion whereby it would be "sensible for the Commission and the EDPS at EU level together with national competition, consumer protection and data protection authorities to agree upon a more holistic

to suggest that there may privacy concerns emerging from the merger, but this is not a matter of competition law, which deals merely with the likeliness that the data concentration strengthens Facebook's position in the online advertising market. If it is true that, generally speaking, not every privacy-threatening merger is anti-competitive, given the growing importance of data as commodities, such a formalistic approach should not be taken. On the contrary, the Commission should assess on a case by case basis, if there is an overlap. Such overall became particularly evident after the terms update of 25 August 2016. It has, indeed, become clear that one of the main ways Facebook is profiting by the (unwisely?) authorised merger is the access to the gigantic amount of data once controlled by WhatsApp. Anyway, even if the Commission kept adopting the said formalistic approach, if the Commission decided today, one could expect that the merger would not be authorised. Indeed, it is no longer true that the "Transaction does not increase the amount of data potentially available to Facebook for advertising purposes".[163] However, the Commission assessed also the possibility that, in the future, Facebook started using WhatsApp users' data for targeted advertisements served on the social network platform. The Commission ended up espousing Facebook's allegations whereby: i. "the data that WhatsApp has access to is at best of marginal utility for Facebook's advertising purposes and would not enhance Facebook's ability to target advertisements on its services"[164]; ii. "Facebook has publicly made it clear that it has no current plans to modify WhatsApp's collection and use of user data"[165]; iii. The CEO of WhatsApp commented by saying that privacy was in its company's DNA and that "if partnering with Facebook meant that we had to change our values, we wouldn't have done it"[166]; iv. Facebook pointed out, debatably, that it was technically nearly impossible "to match each user's WhatsApp profile with her/his Facebook profile"[167]; v. There would have been no incentive to use the WhatsApp users' data, because they would have abandoned the famous app, preferring more privacy-friendly competitors such as Telegram. It could be said that some or all of these assertions were wrong. For instance, the last one ignores some basic concepts such as lock-in and network effect. However, what is decisive is that, given that leading position of Google (also) in the online advertising market, the only merger that would not be authorised, possibly, would be the Google / Facebook one.[168]

In the US, the Federal Trade Commission (FTC) in 2014 had reminded[169] the merging companies that if WhatsApp failed to honour their promises also regarding privacy, both companies could be in violation of Section 5 of the FTC Act and possibly of the their order against Facebook.[170] In August 2016, two consumer privacy organisations files a complaint with the FTC.[171] Therefore, there is the possibility that the FTC will re-assess the acquisition in light of the update.

approach to enforcement" (European Data Protection Supervisor (n. 78) para 84.

163 *Facebook* (n. 141) para 166.

164 *Ibid.* para 181.

165 *Ibid.* para 182.

166 http://blog.whatsapp.com/529/Setting-the-record-straight, accessed 11 June 2017.

167 *Facebook* (n. 141) para 185.

168 *Cfr* Graef (n. 15).

169 Federal Trade Commission, 'Letter from Jessica L. Rich, Director of the Federal Trade Commission Bureau of Consumer Protection, to Erin Egan, Chief Privacy Officer, Facebook, and to Anne Hoge, General Counsel, WhatsApp Inc.' (2014) www.ftc.gov/system/files/documents/public_statements/297701/140410facebookwhatappltr.pdf, accessed 11 June 2017.

170 In the Matter of Facebook. Inc., Decision and Order, No. C-4365 (2012).

171 In the Matter of WhatsApp, Inc., (Aug. 29, 2016) (EPIC, CDD Complaint, Request for Investigation, Injunction, and Other Relief).

In September 2016, the European Commissioner for Competition Margrethe Vestager has declared she has asked some follow-up questions to Facebook, in relation to the change of WhatsApp privacy policy. The Commissioner declared "[t]hat they didn't merge data wasn't the decisive factor when the merger was approved, but it was still a part of the decision".[172] Subsequently, the Commission has sent a Statement of Objections[173] to Facebook alleging the company intentionally or negligently provided incorrect or misleading information during the investigation. The point is that, in Facebook's notification of the transaction and in a reply to a request of information, the social network indicated that it would be unable to establish reliable automated matching between the two companies' user accounts. The current evidence leads the Commission to think that this was feasible also back in 2014. One should not expect, however, a future invalidation of the 2014 decision. Indeed, even though the Commission took that information into account, they did not rely only on it when clearing the merger. Therefore, in case the preliminary concerns were confirmed, the Commission could impose a fine of up to 1% of Facebook's turnover under art. 14(1) of the Merger Regulation. From our perspective, it is interesting to stress that, in reiterating the validity of the merger's authorisation, the Commission does so by underlying that "[t]he current investigation is also unrelated to neighbouring privacy, data protection or consumer protection issues". Arguably another symptom of hemispatial neglect and subsequent lack of integrated approach to data.

Finally, in October 2016, after some national initiatives,[174] the Article 29 Working Party have sent a letter to WhatsApp's CEO.[175] They point out that marketing and advertising are not purposes that were included within the Terms of Service and Privacy Policy when existing users signed up to the service. Moreover, the update is in contrast with the previous public statements of the merged companies. The concerns are threefold. Firstly, the user's consent may be invalid as a consequence of the way the information about the update was given. Secondly, control mechanisms offered to users to exercise their rights do not seem effective. Thirdly, the update will affect also non-users (therefore, the contractual justification could hardly apply to them). Unlike the Commission (with its stress on fines), the Working Party focus more on the need not to proceed to the data synchronisation and, as to the remedies, they suggest that WhatsApp's policy and terms may need to be amended.

172 A. White and P. Levring, 'Facebook Grilled by EU's Vestager Over WhatsApp Merger U-Turn' (*Bloomberg*, 9 September 2016), www.bloomberg.com/news/articles/2016-09-09/facebook-grilled-by-eu-s-vestager-over-whatsapp-merger-u-turn, accessed 11 June 2017.

173 'Mergers: Commission alleges Facebook provided misleading information about WhatsApp takeover' (Europa.eu, 20 December 2017), http://europa.eu/rapid/press-release_IP-16-4473_en.htm, accessed 11 June 2017.

174 The timeliest initiative seems the German one. Indeed, on 27 September 2016, the Hamburgische Beauftragte für Datenschutz und Informationsfreiheit issued a *Verwaltungsordnung* that prohibited Facebook to collect and store data of German WhatsApp users and ordered them to delete all data already forwarded by the messaging company. The full text of the decision is available at https://www.academia.edu/29363159/EXCLUSIVE_the_German_decision_against_Facebook_WhatsApp.pdf. For the initiatives of the UK and Italy see, respectively, https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2016/08/statement-on-changes-to-whatsapp-and-facebook-s-handling-of-personal-data/ and http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/5498297, all accessed 11 June 2017.

175 Article 29 Working Party, 'Letter from the Art. 29 WP regarding WhatsApp updated Terms of Service and Privacy Policy' (27 October 2016), http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2016/20161027__letter_of_the_chair_of_the_art_29_wp_whatsapp_en.pdf, accessed 11 June 2017.

Since competition law can be used to effectively limit intellectual property (as the *Lundbeck* case suggests) and given that data protection considerations ought to be taken into account in competition law cases, then there would be some evidence there is some hemispatial neglect when it comes to data protection, but there might emerge as well a trend towards the recognition of the need for an integrated and balanced approach to data. Some positive news comes from Italy, where the Antritrust Authority (Autorità Garante della Concorrenza e del Mercato) has initiated two investigations against WhatsApp, based on the *codice del consume*.[176] The first one is aimed to assess whether the company has forced the users to accept the update, by making them believe that they would not be able to keep accessing the service, should they not agree with the new terms and policy. The pre-ticked box may play a role in this. The second investigation is in order to assess the unfairness of some sections of WhatsApp's terms. In particular, it is questionable the enforceability of a number of sections, including those concerning unilateral contractual changes, right to withdraw, liability disclaimers and limitations, unjustified service interruption, jurisdiction. The outcome is hard to foresee, but it is commendable that a competition authority is dealing with a data protection case using consumer protection tools.

VI. ARTIFICIAL INTELLIGENCE AND ONLINE BEHAVIOURAL ADVERTISING

Companies are increasingly embracing artificial intelligence.[177] Its role in harnessing the users' data for OBA purposes has become so critical that in a few years those companies that will not serve intelligent OBA will be put out of business.[178]

In this section, a descriptive and prescriptive approach will be taken in discussing how artificial intelligence is used in advertising and how it could or should be used.

One of the main applications of artificial intelligence in an OBA environment is predictive analytics. Indeed, predictive analytics will enable the companies to foresee the purchasing behaviour of users, machine learning algorithms will enable them to provide an increasingly tailored and human-like experience. Machines will learn what we like and, what is more important, they will try to leverage those data to make the user predictable. The best consumer, indeed, is the predictable one. An example of intelligent advertising is M&C Saatchi, Clear Channel and Posterscope's poster "let loose to entirely write itself, based on what works, rather than just what a person thinks may work".[179] In particular, machine learning plays a crucial role in the ad optimization process, thanks to "the simultaneous availability of (i) massive, very fine-grained data on consumer behavior, (ii) data on the brand-oriented actions of consumers, via instrumentation of purchase systems, and (iii) the ability to make advertising decisions and deliver advertisements in real time".[180]

176 *Decreto legislativo* 6 September 2005 no 206, G.U. 235/2005.

177 BS Bulik, 'Brands embrace AI to enhance the brand experience' (2016) 21 Advertising Age 18.

178 The use of AI techniques for advertising purposes tends to be overlooked. For a couple of interesting studies see C. Perlich and others, 'Machine Learning for Targeted Display Advertising: Transfer Learning in Action' (2013) NYU Working Paper No. 451/31829, http://ssrn.com/abstract=2221761, accessed 11 June 2017 and, with more general regard to industrial marketing, F. Martínez-López and J. Casillas, 'Artificial intelligence-based systems applied in industrial marketing: An historical overview, current and future insights' (2013) 42(4) Industrial Marketing Management 489.

179 Still (2015).

180 Perlich (n. 178) 2.

As a second application, one may mention the use of artificial intelligence for better tailored and less intrusive advertisements. Indeed, artificial intelligence is improving the quality of OBA and, enabling a better knowledge of the user, it should make possible a prompter and more customised response to the user's behaviour showing not appreciation for an advertisement. A basic example is offered by Yandex's machine learning complaint button for annoying advertisements.[181] Online experiences are built in order not to disrupt according to the principle of least astonishment and artificial intelligent can be a precious tool therefor.

A third application, is to serve more engaging advertisements. A use case could be Strike Social, a new shop in Chicago that anticipates this year to increase its revenues by $100 million by using "artificial intelligence to drive social advertising".[182]

One could mention, moreover, the use of neural networks and deep learning for the analysis of past failures and successes in order to spot trends and patterns and, therefore, to design the optimal advertising campaign. For an example using associative semantic search technology one could think of the services provided by Omnity, Inc.[183]

Any discussion on artificial intelligence, then, cannot fail to include unemployment. Indeed, there is the genuine concern that intelligent agents may over time replace creative people. A use case could be Adgorithms, with its second release of the intelligent system 'Albert', which enables customers to find new audiences, as well as getting advertising campaigns with a simple click, thus bypassing the human creative process.

Finally,[184] it is noteworthy the use of artificial intelligence in order to offer the same services and products at different prices,[185] depending on a number of factors that can influence demand elasticity. It should be noted that under art. 102 of the Treaty on the functioning of the European Union,[186] these practices could be considered illegal if they take the form of price discrimination and excessive pricing, if carried out by undertaking in a dominant position.

There are several threats related to the use of artificial intelligence in OBA. Firstly, most of the artificial intelligence algorithms are "black boxes".[187]

Therefore, transparency[188] and accountability[189] play a critical role. The General Data Protection

181 The company receives a report every time an advertisement is blocked. Therefore, it filters irrelevant advertisements utilising machine learning technology. See Totaltele.com (2016).

182 C. Heine, 'AI Upstarts Take On Big Tech' (2016) 57 Adweek 28.

183 Omnity, Inc. is a company based in San Francisco. Its service enables searchers to efficiently find related documents, even if those documents do not cite or link to one another.

184 This list of applications is by no means exhaustive. For instance, see the use of artificial intelligence in virtual assistants, as described by Sloane (2016).

185 According to Martínez-López and Casillas (n. 178) 490, "management and pricing account for about half the intelligent systems applications".

186 *OJ* C 326, 26/10/2012 P. 0001-0390.

187 D. Castelvecchi, 'Can we open the black box of AI?' (2016) 538 Nature 21-23.

188 Commission (n. 47) para 2.1.2, stresses the importance of transparency to ensure the users' control over their data, with particular regards to OBA, where "both the proliferation of actors involved in the provision of behavioural advertising and the technological complexity of the practice make it difficult for an individual to know and understand if personal data are being collected, by whom, and for what purpose".

189 Positively, in February 2017, Advertising Standards Canada (n. 5) has evidenced that companies are increasingly complying with Digital Advertising Alliance of Canada, 'Canadian Self-Regulatory Principles for Online Behavioural Advertising' http://youradchoices.ca/files/DAAC-ThePrinciples.pdf, accessed 11 February 2017. In 69% of reviews, Advertising Standards Canada found that participants had in

Regulation would seem to provide a legal basis for this. Moreover, in certain circumstances, it would prevent the entirely automated (or algorithmic) decision-making. The recently adopted French Loi pour une République numérique,[190] with its principle of loyalty of platforms, is along the same lines.

Another tool that could be used to open the black box could be the exception provided by art. 5(3) of the Software Directive.[191] According to this rule, if one has the right to use a copy of a computer program, then they do not have to ask for the right holder's permission in order to observe, study or test the functioning of the program in order to determine the ideas and principles which underlie any element of the program. It is not clear if the new Trade Secrets Directive[192] could limit the use of this exception and, therefore, close the black boxes. Indeed, under its art. 4(2)(a), the acquisition of trade secrets is unlawful if carried out by "unauthorised access to, appropriation of, or copying of any documents, objects, materials, substances or electronic files, lawfully under the control of the trade secret holder, containing the trade secret or from which the trade secret can be deduced". Moreover, the use itself (and the disclosure) of a trade secret is unlawful, even in the event of a lawful acquisition, if there is a confidentiality agreement or breach of contract. It is still to clarify if anti-decompilation sections in terms of service, licenses, etc. are enforceable or not.

When using artificial intelligence to carry out automated processing (including tracking and profiling), then, data controllers shall comply with the principle of lawful, fair and transparent processing. However, it has been noted that this "may be difficult to achieve due to the way in which machine learning works and / or the way machine learning is integrated into a broader workflow".[193] As to the right to a human intervention under art. 22 of the GDPR, moreover, it has been interestingly contented that sometimes "it might be more beneficial for data subjects if a final decision is, indeed, based on an automated assessment".[194]

Artificial intelligence could be used to overcome both a legal and a practical problem. Contract law is traditionally based on the assumption that negotiating parties are on the same level; the axiom has several corollaries, e.g. *ignorantia juris non excusat*. Particularly with the advent of the EU-based consumer law, this presumption has been reversed. Therefore, many laws (not necessarily consumer laws) have been adopted putting in place mechanisms to protect one of the parties that is considered more vulnerable. This has let sometimes to paternalistic excesses and the cookie notice is one of the clearest examples of this. The ePrivacy Directive has been interpreted as meaning a duty to notify the users of websites of the use of cookies.[195] However, one could hardly find anyone who could show that this has led to an improvement to the condition of users who do not read the notice, cannot

place compliant transparency and consumer control mechanisms, up from 20% of the initial review in 2015.

190 Loi no 2016-1321 of 7 October 2016 "*pour une République numérique*".

191 Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs [2009] *OJ* L111/16 (Software Directive).

192 Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure [2016] *OJ* L157/1 (Trade Secrets Directive).

193 D. Kamarinou, Chr. Millard, and J. Singh, 'Machine Learning with Personal Data' (2016*) Queen Mary School of Law Legal Studies Research Paper* No. 247/2016, 22 https://ssrn.com/abstract=2865811, accessed 9 February 2017.

194 *Ibid.*

195 See, for instance, in Italy, Garante per la Protezione dei Dati Personali (n. 45).

understand it, and cannot access the services without accepting it.

This paper suggests to crunch the big data advertising companies collect while tracking and profiling users in order to diversify the mechanisms of legal compliance. Companies are in the position to understand if a user is actually vulnerable and in need of more information, provided in a clear and interactive way. Moreover, particularly vulnerable users, such as children, could be excluded altogether from OBA, as it is already feasible.[196] Equally, OBA companies should be able to understand if a user is tech-savvy, well educated, and, therefore, not in need of a paternalist over-protective approach. Thus, amongst other things, one would follow the European Parliament's recommendation to "empower consumers by providing them with useful, targeted and understandable information"[197].

This would apply to the cookie notices, as well as to the opt-in mechanisms for OBA. Since it clear that all the main actors are putting in place opt-out mechanisms, instead of repeating that this is illegal, maybe one should understand that companies need not to disrupt the user's experience and, therefore, they should not be bound by cumbersome regulation. Conversely, artificial intelligence could be used to provide mechanisms of legal compliance which are tailored to the actual profile and needs of users. This could lead ultimately to a substantial deregulation and to a better user experience.

Complicated algorithms are used by machines to know us better[198] and sell us what we desire (or sometimes what we do not even know to desire). However, one should not be inclined to (entirely) allocate the responsibility on autonomous artificial agents. As shown by the recent news regarding Facebook 'trending list', whereby the human agents were selecting the posts to show in a non-neutral way[199], one cannot always blame an algorithm for the policies of these platforms. Therefore, an integrated approach to OBA shall strike a balance between the need to take into account the actual autonomy of artificial agents, and the necessity not to let this act as an absolute disclaimer of human liability.

VII. CONCLUSIONS. A PRAGMATIC APPROACH TO DATA AS DIGITAL ASSETS AND THE "COOPERATIVE CHARTER ON ONLINE BEHAVIOURAL ADVERTISING"

The technical and legal intricacies of OBA are the main reason of the current lack of awareness on the side of the users. Awareness and empowerment are paramount, especially if one considers that it is often the user's behaviour that leaves the door open to data protection breaches and abuses[200]. Should a user know what OBA is and how it works, accessing and understanding the relevant regulations is

196 It is already possible to understand if an online user is a child by analysing the text of their chats, but artificial intelligence could increase the accuracy of the identification. See, for instance, M. Ashcroft, L. Kaati, and M. Meyer, 'A Step Towards Detecting Online Grooming – Identifying Adults Pretending to be Children', in *2015 European Intelligence and Security Informatics Conference* (IEEE 2015) 98.

197 European Parliament, 'Resolution on a new strategy for consumer policy', 2011/2149(INI), para 21.

198 Automated decisions do not always work. For instance, on 29 August 2016, Facebook blocked the accounts of many Italian LGBT advocates because their posts had been judged…homophobic.

199 M. Nunez, 'Former Facebook Workers: We Routinely Suppressed Conservative News' (2016), gizmodo.com/former-facebook-workers-we-routinely-suppressed-conser-1775461006, accessed 11 June 2017.

200 For instance, the use of simple password would have prevented a hacker from using a baby monitor to shout at a child. See Dave Lee, 'Hacker 'shouts abuse' via Foscam baby monitoring camera' (BBC News, 14 August 2013), www.bbc.co.uk/news/technology-23693460, accessed 9 February 2017.

not easy. Indeed, they should make their head around a threefold regulatory interweave, whose knots this paper aimed to get out.

Being aware of what is OBA is and what are the relevant regulations and the remedies is necessary, but it is not sufficient. Trust is key. Users need to trust that OBA companies will always act transparently, that they will make the opt-out easy, that they will not circumvent the users' options. To this end, building on the empirical data gathered on OBA, this paper presents a "Cooperative Charter on Online Behavioural Advertising", that the author will send in the form of a policy sheet to the main stakeholders[201] in order to inform the future co-regulation of OBA (please see appendix).

In order to ensure awareness and trust, then, users must be in a position to trust that OBA companies will process their data fairly and use artificial intelligence not to manipulate them, but to offer them a better online experience and bespoke compliance mechanisms.

OBA can be a positive phenomenon, inasmuch as it helps the user experience to be less disrupted by uninteresting advertisements. Nonetheless, there can be several problems for the consumer, for instance in terms of price discrimination, influence on the voting preferences, distress for having the feeling that one cannot entirely escape the advertising net. Indeed, if the OBA is effective, data protection laws will apply, because the clear purpose of the former is to single out a consumer. If a user is singled out, data protection laws shall apply.[202] The principles at stake are of the utmost importance; they include autonomy[203] and self-determination.[204] The point is that the best consumers are the most predictable ones. Therefore, it is understandable that companies are doing their best to influence our present and future behaviour in subtler and subtler ways, especially through subliminal messages[205] and machine learning algorithms which users do not have access to.[206]

201 The European Parliament's JURI Committee, the European Commission's DG Connect, the European Advertising Standards Alliance, the Interactive Advertising Bureau, the International Chamber of Commerce, the Advertising Standards Authority, the House of Commons relevant committees (Business, Innovation and Skills Select Committee, Science and Technology Select Committee, Culture, Media and Sport Select Committee), the Electronic Frontier Foundation, the European Digital Rights, Politico Europe, the European Consumer Organisation, the European Consumer Centres Network, the International Association of Privacy Professionals, and the European Privacy Association.

202 *Cfr* FJ Zuiderveen Borgesius, 'Singling out people without knowing their names – Behavioural targeting, pseudonymous data, and the new Data Protection Regulation' (2016) 2 *Computer Law & Security Review* 256. This does not mean, however, that consent is always required.

203 Especially when we try to ignore the advertisements, the effects of the so-called affective conditioning increase. We do not freely choose a product because it is the best one, but because the advertising has paired it with positive items, thus creating a false desire for a product, notwithstanding its intrinsic characteristics. According to MA Dempsey and AA Mitchell, 'The Influence of Implicit Attitudes on Choice When Consumers Are Confronted with Conflicting Attribute Information' (2010) 37(4) *Journal of Consumer Research* 614, 622, this "can occur even when consumers have both the motivation and the opportunity to retrieve product attribute information from memory".

204 The problem is not limited to OBA, but it applies to the more general online aspect of our everyday life, especially with regard to the Internet of Things. To put it in the alarming words of MG Michael, 'The Paradox of the Uberveillance Equation' (September 2016) *IEEE Technology and Society Magazine* 14, 20, "[w]e are losing our ability to make decisions for ourselves, to make a choice based on our preferences, not imposed by computer systems."

205 *Cfr* PM Merikle, 'Subliminal perception', in E. Kazdin (ed), *Encyclopedia of Psychology* 17 (Oxford University Press 2000) 497.

206 The problem of algorithmic transparency is pressing and it has palpable legal implications also in terms of competition. For instance, J Angwin and S Mattu, 'Amazon Says It Puts Customers First. But Its Pricing Algorithm Doesn't' (ProPublica, 20 September 2016), www.propublica.org/article/amazon-says-it-puts-

At the same time, however, it is not possible to ban OBA altogether by saying that it conflicts with data protection, privacy, and consumer protection. Simply banning OBA would rule out well-established business models and it would be contrary to the principles of competition and freedom of enterprise.

Too many times compliance with the data protection rules has proven to be impossible, fictitious, or useless (the ePrivacy Directive with its mechanism on cookies provides robust evidence on this).[207] Data protection laws should be simplified and compliance should be made easier. Firstly, in a world where the economy is global and the space is virtual, it is not possible for all the national systems to demand compliance with their own (sometimes radically different) rules. Secondly, because data have become the key commodity for several markets and companies.

Opt-in mechanisms would provide a stronger protection for the users, but the international and European self-regulatory frameworks[208] have made clear that there is little chance that the companies will adopt the opt-in mechanism. At the same time, the ePrivacy Directive shows how useless can be certain legal burdens based on pure consent. Hence, one may take a pragmatic approach and try to make the former work. The draft ePrivacy Regulation, with its shift from cookies to browser settings, seem a positive improvement.

One can (and has to) require transparency, accountability, fairness, and good faith in the handling of the private information, but closing all the valves will only make the dam blow up.

From the above analysis, three policy recommendations can be drawn up. Firstly, co-regulation seems the way forward. Consequently, after simplifying and cutting down current top-down regulations, regulatory interventions should be kept at a minimum (general framework) and ex post (effective judicial and non-judicial remedies). Thus, one could hope to overcome the European legal quagmire. Regulators should monitor that self-regulations follow the said cooperative and integrated approach.

Secondly, governments should launch educational campaigns to make the users understand the value of their data, the meaning and consequences of OBA, as well as the relevant rights and remedies.

Thirdly, research on artificial intelligence should be a top priority in the funding agenda of governments. In particular, there is the need to explore how we can use the related developments in order to simplify laws and ensure compliance. The above-presented bespoke

customers-first-but-its-pricing-algorithm-doesnt, accessed 8 February 2017, have recently revealed that the "Best Deal" algorithm of Amazon does not show the users the actual best deal, but the one where it is Amazon itself selling the products. See the antitrust proceedings opened by the European Commission on 14 July 2016, against Alphabet in case AT.39740 within the meaning of Art. 11(6) of Council Regulation (EC) No. 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Arts 81 and 82 of the Treaty [2003] *OJ* L1/1 and Art. 2(1) of Commission Regulation (EC) No. 773/2004 of 7 April 2004 relating to the conduct of proceedings by the Commission pursuant to Articles 81 and 82 of the EC Treaty [2004] *OJ* L123 /18 (it deals with the way Google shows its comparison shopping service and that of its competitors in its search results).

207 For instance, FJ Zuiderveen Borgesius, 'Personal data processing for behavioural targeting: which legal basis?' (2015) 5(3) *International Data Privacy Law* 163-176 argues that the cookie consent requirement does not provide a legal basis for the processing of personal data.

208 European Advertising Standards Alliance (n. 70); International Chamber of Commerce (n. 104); Interactive Advertising Bureau (n. 71).

mechanisms could be taken into consideration. Companies that track and profile users should invest in artificial intelligence not only in order to serve bespoke advertisements, but also to tailor the data protection information, both as to its quality and its quantity. For some users an opt-out mechanism may be sufficient, but the behaviour of a user may show that there is the need for some form of more protective approach. Thus, artificial intelligence could constitute a solution to the problem of paternalistic regulation in data protection, with some potential of application to consumer law.[209]

However, artificial intelligence should not be embraced blindly. Indeed, it is an extremely powerful tool currently controlled by a limited number of (usually) big corporations. Opening the black boxes of artificial intelligence algorithms would help democratising the Internet and it would empower the users.

There are some technical tools and legal rights and obligations that can enhance privacy in a ubiquitous surveillance environment, like the one necessary for OBA to thrive. Some of these means can be easily circumvented (see the AdBlock Plus v. Facebook war)[210] or they are more apparent than real (see the experiment on the consequences of blocking all cookies).[211]

Tracking and profiling, however, can be useful. To receive suggestions of music we could enjoy on YouTube, to be shown news we are interested in or search results that answer precisely to our questions, badly formulated as they can sometimes be. These are some of the reasons why machine learning-enabled and predictive analytics-based algorithmic decision-making can improve the quality of our lives.[212] Even OBA, if freely and actively chosen, with the possibility to withdraw the consent at any time, can reduce our search costs and imagination costs, thus making our life easier.

The GDPR constitutes a step forward if compared with the Data Protection Directive, but much will depend on the draft ePrivacy Regulation and on the adoption of an integrated cooperative approach to OBA. It is to be hoped that trust, awareness, transparency, algorithmic accountability, and right to dissent will be the North Star that the online sailors shall follow.[213]

209 Data protection and consumer law move from the assumption of a subject (the consumer and the data subject) who is depicted as structurally weak. Thanks to AI, companies could use the data they collect while profiling the users in order to provide a bespoke legal compliance.

210 The frantic duel has received large coverage, see, for instance, Josh Constine, 'Facebook rolls out code to nullify Adblock Plus' workaround again' (TechCrunch, 11 August 2016), https://techcrunch.com/2016/08/11/friendblock/, accessed 9 February 2017.

211 More generally, Hoofnagle (n. 60) 273, observe that "the combination of disguised tracking technologies, choice-invalidating techniques, and models to trick the consumers into revealing data suggests that advertisers do not see individuals as autonomous beings".

212 There are a number of cons. One of them is social network homophily, that is the fact that we list and speak only to the like-minded while online, with the risks of "excessive confidence, extremism, contempt for others, and sometimes even violence" (CR Sunstein, *Republic.com 2.0* (Princeton University Press 2007) 10). Along the same lines, it has been said that algorithms used to rank search results and social media posts create "filter bubbles," in which only ideologically appealing content is surfaced (E Pariser, *The Filter Bubble: What the Internet Is Hiding from You* (Penguin Press 2011)). E. Bakshy, S. Messing, and L. Adamic, 'Exposure to ideologically diverse news and opinion on Facebook' (*SciencExpress*, 7 May 2015), 1-4, http://cn.cnstudiodev.com/uploads/document_attachment/attachment/681/science_facebook_filter_bubble_may2015.pdf, accessed 8 February 2017, have presented evidence that people are exposed to a substantial amount of content from friends with opposing viewpoints.

213 Whereas this paper's solution empowers the user, most solutions are focused on the role of the public institutions and on regulation. Along those lines, for instance, see WEJ Klein, 'Can We Trust ForProfit Corporations to Protect Our Privacy?' (September 2016) *IEEE Technology and Society Magazine*, 17, 19, according to whom, given that corporations have no

APPENDIX

Cooperative Charter on Online Behavioural Advertising

Article 1

Users have the right to opt out from online[214] advertising altogether, as well as from its single types.[215] Circumvention of these measures is in breach of the ePrivacy Directive, of the Unfair Commercial Practices Directive, as well as general tort laws. If the circumvention is grounded on a contract, the Directive on unfair terms in consumer contracts shall apply, in case of business-to-consumer transactions.

Article 2

Users have the right to know which companies are tracking, profiling, and serving advertisements to them. They have the right to know the basis whereupon the advertisements are served,[216] as well as the purpose for which data are used, the retention time, and the measures put in place to comply with applicable laws. All information is provided in a brief, clear, and interactive gamified way.

Article 3

Companies are held accountable for the algorithmic decision-making occurring with regards to the services provided. Accountability includes transparency on the reasoning of the artificial agents.

Article 4

Personal data are digital assets in the data subjects' IP portfolios. Users can issue data licenses, which can be terminated at any time. Personal data cannot be assigned and the relevant remedies cannot be waived.

Article 5

Companies responsible for online behavioural advertising (primarily, advertising networks, publishers, advertisers) act in good faith.[217] Good faith and transparency pose inter alia an obligation to provide information in a brief, clear, and interactive gamified way also beyond the scope of Article 2 of this Charter.

Article 6

If feasible with regards to the development of the technologies involved, companies use the data collected in connection to online behavioural advertising in order to put in place forms of bespoke legal compliance. Online behavioural advertising carried out without the users' awareness is unlawful. These technologies are developed also with the purpose of increasing said awareness.[218]

real incentive to protect privacy, "it is time to think about independent, international, publicly funded, and democratically legitimized institutions to either run and provide, or at least oversee and finance the lower level digital infrastructures, the social networks, and the messaging apps, etc., that we rely on as well". One can agree with the premise, not quite with the top-down solution.

214 The characteristics of online advertising make the "change the channel" remedy often unviable.

215 Users should be made aware, for instance, that the opt out from interest-based advertising might still allow some form of OBA.

216 Including, for instance, when and where they have consented, which data were used to serve it, etc.

217 This means, in the first place, to ensure the right to dissent by, for example, not circumventing ad-blockers and browser settings which block OBA.

218 The reference is to the so-called "awareness by design". The concept has been introduced by Noto La Diega (n. 63) 410, where it is defined as "the use of technologies (especially design) to empower the user and make them aware of risks, rights, and obligations". For instance, instead of pre-ticking the "I have read/I have understood" boxes, providers should pre-tick an "I have not read/I have not understood" box. A noteworthy project of awareness by design is led by Rossana Ducato at the Université catholique de Louvain.

Article 7

Companies make available optional[219] online dispute resolutions, and refrain from mandatory binding arbitration.

[219] One of the main problems in Internet-related disputes is the attempt of online platforms and other strong intermediaries to prevent the access to public justice by means of compulsory alternative dispute resolution. It is a problem that goes beyond OBA, but this could be the opportunity to address the issue.