**Data as Digital Assets. The Case of Targeted Advertising**

**Guido Noto La Diega[[1]](#footnote-1)\***

“To many it will occur, that an important means of doing good is thus opened up; and certainly good advices, on the most interesting subjects, might in this way occasionally be tendered. By some, such a system of advertising may be considered as rather disreputable”

Fraser, W. (1834)

**Abstract.** Facilitated by the growth of cloud computing, artificial intelligence (e.g. machine learning), and big data (e.g. predictive analytics), new tracking and profiling techniques have been developed. They have enabled the rise of targeted advertising, that is the provision of advertisements tailored to the tastes and habits of the user who actually views them. If targeted advertising is effective, data protection laws still apply. Most regulations look at the phenomenon from the data protection perspective, whilst in this paper it is argued that a holistic approach should be sought.Indeed, intellectual property, competition law, and consumer protection come necessarily into play. A general idea in this paper is that one should treat the data as digital assets in the users’ IP portfolio, thus leading the users to care more about the way their data are processed, shared, and sold. The starting point is the regulatory framework in Europe, with particular regard to the ePrivacy Directive. After critically analysing some international and European self-regulatory initiatives, case studies on Facebook and the use of data on sexual orientation will be presented to display how these systems work in practice if an Italian user files a claim with the Istituto di Autodisciplina Pubblicitaria that his rights have been violated. The chapter goes on to compare the Data Protection Directive and the General Data Protection Regulation, with a focus on direct marketing. Given that Google is the main actor of the targeted advertising world, it will be explained how the platform works and this work analyses its privacy policy to assess how data are treated with regard to this form of advertising. Before concluding, the chapter looks at targeted advertising from an intellectual property and competition law perspective. The chosen prism is the Facebook / WhatsApp concentration. The paper aims *inter alia* to evaluate whether the decision of the Commission, which authorised the concentration, would be different today, in light of the change in WhatsApp’s privacy policy allowing the use by Facebook of certain data of WhatsApp’s users. The chapter assesses, more generally, whether targeted advertising can be prevented or somehow regulated through the unfair commercial practices regime. This chapter concludes with a pragmatic proposal which aims to empower the users, yet strike a balance between their interests and rights and those of the ad networks, publishers, and advertisers (advertising companies). In general, one should recognise that the opt-in regime required by some regulators is not implemented by the targeted advertising companies; cumbersome regimes such as the notice and consent provided for by the ePrivacy Directive have been a failure. Therefore, one should impose on businesses a more reasonable opt-out mechanism, provided that the right to dissent is actually enforced (as opposed to the current practice of circumventing adblockers and similar tools) and that the information is clear, brief, and provided in an interactive and gamified way. The user has to be at the centre of the system, but data protection rules may not be the best means therefor.

**Keywords:** targeted advertising, direct marketing, behavioural advertising, OBA, interest-based advertising, behavioural targeting, profiling, tracking, algorithmic decisions

**Table of contents**

1. Introduction
2. The European Regulation of Targeted Advertising
3. European and International Self-Regulation of Targeted Advertising.
4. Profiling, Direct Marketing and Algorithmic Decision-Making in the General Data Protection Regulation
5. “It’s a Google Market”: AdSense, a Recent Change to the Google Privacy Policy and Related Details
6. The Use of Digital Assets to Hinder Competition. The Facebook / WhatsApp Merger
7. 7. Conclusions. A more balanced approach to data as digital assets and the “Cooperative Charter on Online Behavioural Advertising”8. Afterword. Of chocolate chips and lavender buds

Reference list

**1. Introduction.**

Advertising plays a critical role in the keeping the Internet free, especially by enabling the development of new business models that are flexible and dynamic enough to accommodate the constantly evolving needs of online users.[[2]](#footnote-2) One need only mention the “freemium” model, whereby basic services are free thanks to advertising placements to third parties.[[3]](#footnote-3) As recently observed with regard to the proposal for a new Copyright Directive, “access ‘free’ for users and the service draws its revenues, directly or indirectly, from advertising and user data”.[[4]](#footnote-4)

In recent years, facilitated by the growth of cloud computing, artificial intelligence (e.g. machine learning), and big data (e.g. predictive analytics), new tracking[[5]](#footnote-5) and profiling[[6]](#footnote-6) techniques have been developed. They have enabled the rise of targeted, or behavioural, advertising,[[7]](#footnote-7) that is, the provision of advertisements that are tailored to the tastes and habits of the user who actually views them.[[8]](#footnote-8) Users may expect their browsing behaviour to be analysed to serve them with ads; therefore, they may not be surprised if the first thing they are shown when accessing Amazon is a group of goods similar to items they have previously viewed. What users may not be aware of, on the contrary, is the use of facial recognition techniques to mine their photos. For instance, a Northern California District Court[[9]](#footnote-9) has recently considered that the Illinois Biometric Information Privacy Act is applicable to Facebook, which is likely to mean that the social network has breached the law by not requiring explicit consent for its activity of facial recognition.[[10]](#footnote-10) The importance of photos for Facebook has been confirmed by its recent attempt to force[[11]](#footnote-11) its users to download “Moments”, a separate app to sync their private photos. The ordinary Terms of Service (ToS) and privacy policy apply to Moments, which means that Facebook will also leverage this kind of data in order to use “the information we have to improve our advertising and measurement systems so we can show you relevant ads”.[[12]](#footnote-12)

It is a common experience, for instance, to look for something on Google’s search engine and then to see related advertisements popping up after logging in on Facebook. One is rarely aware of the quality and degree of tracking one is subject to. A tool that can improve such awareness is the LightBeam add-on. The below chart shows an experiment this author carried out. On 12 August 2016, at 16:45 GMT, after installing this add-on, the Mozilla browser was used to search for a video (The Chainsmokers - Don't Let Me Down ft. Daya) on YouTube. This simple operation, which lasted 20 seconds, made this author inadvertently interact with 19 third-party sites, mainly owned or controlled by Google (for instance, google.com, google.co.uk, content.googleapis.com, googlesyndication.com, googleusercontent.com, googlevideo.com, etc.). LightBeam showed 0.5 cookies being activated per second. After two hours of moderate activity this author interacted with 229 third-party sites by visiting 32 sites. 44 cookies were from adform.net, 44 from smh.com.au 38 from Google’s DoubleClick, 34 from adnxs.com. Some of these results came as a surprise, because this author had never (knowingly) visited Adform or Adnxs, which are, respectively, a global digital media advertising technology company and a portal for publishers to the AppNexus online auction exchange used to sell advertising space. Nor had he been aware of DoubleClick’s operations.

This experiment also allowed this author to discover which advertisers target him through Facebook. There are eleven “Advertisers with your contact info” and five “Advertisers whose website or app you've used”.[[13]](#footnote-13) The first group[[14]](#footnote-14) is formed by advertisers who have paid to access some data of the user’s profile. It is not entirely clear which data Facebook can sell the advertisers, since the only thing it declares not to share is the user’s name and contact info,[[15]](#footnote-15) But there is for sure access to sensitive data, such as gender data. Now, the use case presented is a bike seller who wants to narrow the target to all the women aged 18-35 who live in Sydney and are interested in cycling. What if one is a pharmaceutical industry that wants to target all the people in a certain hospital? This involves no personal data, only location data, yet they are nevertheless intrusive and from them one can easily infer health data, which are indeed sensitive. Take for example the case of women in abortion clinics targeted with anti-abortion ads.[[16]](#footnote-16) No worries, though. Facebook tells us that we are in control over the ads thanks to a supposedly user-friendly tool.[[17]](#footnote-17) Indeed, in the ads preferences page this author discovered he was being granularly profiled, his activities and interests have been broken down into 683 audiences (as the platform calls them), from the BFI London Film Festival to the Italian Social Movement, which was quite in dissonance with the actual political beliefs of this author.[[18]](#footnote-18) Anyway, relying on an opt-out mechanism, this author had been tracked and profiled and the fact that the tool offered by Facebook is to opt out individually from each of the audiences does not seem fair.[[19]](#footnote-19) Also, users should have the right to know on which basis people and companies that they do not know serve them with ads? After an afternoon spent in being redirected from one page to another, eventually this author landed on one which seemed to be more helpful.[[20]](#footnote-20) There it was found out that this author’s current (never autonomously chosen) ad preferences can be used to show him ads on apps and websites both on Facebook and off of the Facebook Companies. At the end of the day, this author decided to turn off the ads altogether. However, the popular social networking site discourages this choice by saying that who opts out will see “the same number of adverts, but they may be less relevant to you”. Moreover, opting-out users may, nonetheless, “see adverts based on things that you do on Facebook”. This could come as a surprise, because the things that users do can be defined as their behaviour and it does not make much sense that if one opts-out of the behavioural advertising, they will keep receiving ads based on the things they do, i.e. their behaviour. It seems impossible to opt out of Facebook targeted advertising: they have cleverly changed the name to “online interest-based ads”. And when it comes to the law, changing names has practical consequences: it is not true that a rose by any other name would smell as sweet.[[21]](#footnote-21)

Even though targeted advertising can benefit consumers,[[22]](#footnote-22) most surveys show that users oppose the provision of this kind of advertising,[[23]](#footnote-23) and even those surveys that evidence a positive approach towards this kind of advertising indicate that most users feel that it violates their privacy.[[24]](#footnote-24) For instance, a Pew survey shows that 73% of the search engine users surveyed do not agree “with a search engine keeping track of your searches and using that information to personalize your future search results because [they] feel it is an invasion of privacy”.[[25]](#footnote-25) Moreover, 68% of all Internet users do not feel comfortable “with targeted advertising because I don’t like having my online behavior tracked and analysed”[[26]](#footnote-26).

On closer look, the complimentary character of the Internet is merely apparent. Indeed, not only is a price paid to the advertisers (albeit not by the end-users), but there might be a non-financial cost in terms of jeopardisation of privacy, competition, intellectual property, and consumer protection. As an experiment presented above shows, users who try to disable the cookies and the ads will find out that they are no longer able to access most of the online services. This proves that users of (apparently) free services are actually paying with their data and are acquiescing to being tracked and profiled. As has been observed with regard to the popular augmented-reality game Pokémon Go, “even gamers who never spend a cent on in-app purchases or promotions are effectively producing information that becomes a commodity owned by Niantic”.[[27]](#footnote-27)

Intrinsically connected to other pressing issues, such as those related to cookies, profiling, and direct marketing, targeted advertising is no longer just the use of “information linked through cookies to create a profile of a user [in order to send] adverts which are likely to interest them,”[[28]](#footnote-28) since the concept of the digital fingerprint goes clearly beyond cookies, and new tracking techniques such as cross-device tracking[[29]](#footnote-29) are being developed every day.

If targeted advertising is effective, data protection and privacy laws will apply. Indeed, data are personal if they enable the identification of a person, regardless of the knowledge of the name of the person. For targeted advertising to be effective, the advertiser has to be able to single out a user and serve that user with bespoke commercial messages. If a user is singled out, data protection laws will apply.[[30]](#footnote-30)

Data protection is just one of the prisms through which to observe targeted advertising. Indeed, targeted advertising shows how personal data have become a critical digital asset of the intellectual-property portfolio of a few strong actors[[31]](#footnote-31) that can leverage them in order to, on the one hand, carry out potentially unfair commercial practices, and on the other hand, turn the users into digital labourers and carry out discriminatory policies of targeted pricing, today tackled by the European Commission in the context of the Digital Single Market Strategy.[[32]](#footnote-32) One of the solutions suggested here is to treat data as digital assets in the IP portfolio of consumers, as a way to lead them to understand the importance of their data, without necessarily preventing any kind of aware economic exploitation of these assets. There are several indicia of the current transformation of data into digital assets. This is underpinned by an understanding of privacy no longer as a human right (static and non-transferable), but as property (dynamic and transferable). Data portability, as introduced by the General Data Protection Regulation (GDPR),[[33]](#footnote-33) is probably the clearest example of this development. Accordingly, data controllers (e.g. Facebook) are obliged to transfer the personal data to the data subject who provided them “in a structured, commonly used and machine-readable format.”[[34]](#footnote-34) Moreover, the data subject has “the right to transmit those data to another controller.”[[35]](#footnote-35) The shift towards data as digital assets was confirmed amongst othersby the recent regulation on cross-border portability of online content services.[[36]](#footnote-36) Indeed, the regulation does not allow the licence, communication, transfer, sharing, transmission and disclosure of personal data to the online content service provider[[37]](#footnote-37) (e.g. Netflix when accessed by a German subscriber temporarily in England). Thus, *a contrario*, the regulation confirms that, outside this specific context, personal data can be licensed like any other intellectual property right.[[38]](#footnote-38) **Users would better realise the value of their data if they had to license them, rather than accept a privacy policy.** In a draft regulation of September 2017, [[39]](#footnote-39) finally, the European Commission recognised the principle of free movement of non-personal data. Correspondingly, they noted that obstacles to the free flow of data are in violation of the free movement of services and that data value chains are built on “data analysis, marketing, and distribution.”[[40]](#footnote-40)

Many perspectives will be left out of this paper, including the political campaign teams increasingly using the ability offered by social media platforms “to deliver targeted advertisements to selected lists of individual voters”.[[41]](#footnote-41)

The Article 29 Working Party[[42]](#footnote-42) has clarified that the legal basis of processing for targeted advertising purposes is consent and that the only mechanism that is fully compliant with the then-effective Data Protection Directive[[43]](#footnote-43) is a strong ‘opt-in’ one. Some judges[[44]](#footnote-44) have followed this approach, thus considering illegal soft ‘opt-in’ mechanisms, such as a pre-ticked box that the user has to untick in order not to authorise data processing.

The *Vidal-Hall v. Google* case[[45]](#footnote-45) has shown, on the one hand, how targeted advertising is an ideal prism to observe the intersection between data protection, competition, intellectual property, and consumer protection; on the other hand, it has spelt out the principle whereby it is not a requirement of data protection regimes that the loss be pecuniary; therefore, one can claim damages even for mere distress. This confirms that the nature of the interests involved in targeted advertising is not only financial, but also pertains to the user as a person. Moreover, *Vidal-Hall v Google* has confirmed that technological enforcement is not always sufficient. Indeed, in that case the users set Apple’s Safari browser to block third-party cookies, but a Safari workaround operated by Google allowed it to record and use information about the users for the purposes of its advertising service.

Complicated algorithms are used by machines to get to know us better[[46]](#footnote-46) and sell us what we desire (or sometimes what we do not even know we desire). However, one should not be inclined to (entirely) allocate the responsibility to autonomous artificial agents. As shown by the recent case of the Facebook ‘trending list’, where the human agents were selecting the posts to show in a non-neutral way, one cannot always blame an algorithm for the policies of these platforms. Therefore, a savvy framework for targeted advertising will 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.

The structure of this paper is as follows. The starting point is the regulatory framework in Europe as clarified by the Article 29 Working Party and the European Data Protection Supervisor, with particular regard to the ePrivacy Directive.[[47]](#footnote-47) Moving from the observation that actors in cyberspace tend (sometimes understandably) to ignore top-down regulations, since they prefer peer regulation, the International and European self-regulation initiatives of the International Chamber of Commerce (ICC), the European Advertising Standards Alliance (EASA), and the Interactive Advertising Bureau (IAB) will be critically analysed. A case study on Facebook and the use of data on sexual orientation is presented with regards to a hypothetical Italian user who lodges a complaint before the Istituto di Autodisciplina Pubblicitaria. This chapter goes on to compare the Data Protection Directive and the General Data Protection Regulation, with a focus on direct marketing, but touching also on profiling and algorithmic decision-making. Given that Google is the main actor in the targeted-advertising world, this chapter explains how the platform works and analyse, its terms, privacy policy (hereinafter ‘legals’) and settings options, to assess how data are treated with regard to this form of advertising. Before concluding, this work looks at targeted advertising from an intellectual property and competition law perspective. The chosen prism is the Facebook / WhatsApp concentration. The chapter aims to evaluate whether the decision of the Commission authorising the concentration would be different today, in light of the change to WhatsApp’s privacy policy allowing the use by Facebook of certain data of WhatsApp’s users. More generally, it is assessed whether targeted advertising can be prevented or somehow regulated through the unfair commercial practices regime. It is concluded with a pragmatic proposal which aims to empower the users, yet to strike a balance between their interests and rights and those of the businesses (ad networks, publishers, advertisers, etc.), i.e. the “Cooperative Charter on Online Behavioural Advertising.” In general, the idea is that one should recognise that the opt-in regime required by some regulators is not implemented by the companies using targeted advertising; cumbersome regimes such as the notice and consent provided by the ePrivacy Directive have been a failure. Therefore, one should impose on businesses a more reasonable opt-out mechanism, providing that the right to dissent is actually enforced (as opposed to the current practice of circumventing adblockers and kindred tools) and that the information is clear, brief, and provided in an interactive and gamified way. The user has to be at the centre of the system, but it is debatable that data protection rules are the best means to ensure a user-centric system.

As to the methodology, alongside a review of legislations, regulations, self-regulations, legals, and literature in Europe (with a particular, albeit non-exclusive, focus on the UK and Italy), some experiments have been carried out with the aim of understanding: 1) How and how much are we tracked and, therefore, served with targeted advertising; 2) How effective are the technical tools a user can put in place to stop being the target of such advertising; 3) Whether users are aware they are tracked and whether they know what “targeted advertising” means”. The sometimes-surprising results are presented below.

**2. The European regulation of targeted advertising**

Data are commonly seen from the perspective of the data subject’s rights to privacy and data protection, which have undoubtedly reached the status of fundamental human rights. However, phenomena such as targeted advertising 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. Therefore, a balance has to be struck between competing interests.

Perhaps understandingly, the European regulators have favoured privacy and data protection over the other perspectives. The first – and currently most important – (quasi) regulation is the Article 29 Working Party’s opinion on “online behavioural advertising” (OBA).[[48]](#footnote-48)

Though the focus will be on the said opinion, some quick historical remarks are in order.

The relevant brief history might date back to 1993, when the Council of Europe's European Convention on Transfrontier Television[[49]](#footnote-49) entered into force. However, at that time, given the development of the relevant technologies, targeted advertising was understood as advertising directed to audiences based in a single country. Indeed, under Article 16(1), in order to avoid distortions in competition and endangering the television system of a party to the Convention, “advertising and tele-shopping which are specifically and with some frequency directed to audiences in a single Party other than the transmitting Party shall not circumvent the television advertising and tele-shopping rules in that particular Party”.

Two years later an amendment was proposed to Council Directive 89/552/EEC on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the pursuit of television broadcasting activities (Television Broadcasting Directive).[[50]](#footnote-50) The Commission underlined that, in order to enable the broadcasting organisations and the national regulatory authorities to organise their activities efficiently, the Directive and the Convention should be as compatible as possible. It is noteworthy that as an example of fundamental difference between the two instruments reference is made to Article 16 of the Convention on targeted advertising that “has no equivalent in the Directive (given that it would be fundamentally incompatible with Article 59 of the Treaty)”.[[51]](#footnote-51) The reference seems to the Treaty of the European Economic Area that provided that “restrictions on the free supply of services within the Community shall be progressively abolished”.[[52]](#footnote-52)

A number of amendments have been introduced over the years and, ultimately, the Audiovisual Media Services Directive repealed the Television Broadcasting Directive.[[53]](#footnote-53) One can infer from recitals 41 and 42 of the former that targeted advertising (understood as advertising directed to an audience in a country) is consistent with the EU law. Therefore, one has to believe that the Convention’s rule on targeted advertising is no longer applicable in the countries which are parties both of the Council of Europe and of the European Union.[[54]](#footnote-54) Indeed, Article 27(1) of the Convention states that in their relations with each other the Parties that are Members of the European Union will apply the latter's rules, and will apply the rules of the Convention only insofar as there is no EU measure relating to the particular subject in question.

Given that today one can watch television via the Internet (accessing it through multiple devices) and given the developments of smart TVs, as a policy recommendation one should wish that the Audiovisual Media Services Directive would soon be amended to take into account the possibility to serve advertisements targeted not only to an audience, but to a specific user. A new legislative proposal amending the said Directive was adopted by the European Commission on 25 May 2016, in the context of the Digital Single Market Strategy.[[55]](#footnote-55) This proposal does not take into consideration our suggestion, which is surprising if one considers that television has the highest share of advertising revenue across all media,[[56]](#footnote-56) therefore there is a significant interest in increasing targeted advertising through this channel.

A by far more up-to-date vision has been expressed by the Commission with regard to online platforms, even though the reference to targeted advertising is arguably limited to the search engine platforms. It is noted, indeed, that some search engines use disaggregated data about users' online behaviour to provide targeted advertising.[[57]](#footnote-57) The Commission points out that cookies should only be placed on a user's device after consent has been given. Taking a balanced (if not holistic) view, the Institution observes that “users encounter a dilemma in the face of a trade-off between ex-ante information benefits and ex-post risks”.[[58]](#footnote-58)

Coming to the cited opinion, according to the Article 29 Working Party, the first piece of legal framework one should take into consideration is the ePrivacy Directive. Under its Article 5(3),

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

Therefore, advertising network providers are allowed to place cookies or similar devices on users' terminal equipment or obtain information through such devices only with the informed consent of the users.

In order to review the ePrivacy Directive, the European Commission has launched a public consultation,[[59]](#footnote-59) whose preliminary findings were published in August 2016.[[60]](#footnote-60) There are two points that are particularly relevant for targeted advertising.

The first concerns cookies. According to 77% of citizens and civil society and 70% of public authorities, information service providers ought not to have the right to prevent access to their services if users refuse to have identifiers, such as cookies, stored in their terminal equipment. Three quarters of industry on the other hand disagree with this statement. As confirmed by the Google use case below, this is a hot issue. For instance, once one disables the cookies, one is no longer able to log in to Facebook. The social network platform does not explain why, but they say that cookies are necessary to access Facebook.[[61]](#footnote-61) Twitter is somewhat clearer. It prevents users who disable cookies from accessing it, though it explains that Twitter and its partners use cookies for statistics, personalisation and advertising. To make a long story short, it seems that these tools the users theoretically have to prevent cookies and advertisements are more formal than substantial.

Another relevant issue in the preliminary report is the choice between opt-in and opt-out. Even though the question concerned marketing calls, the concept is the same, since targeted advertising 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 consultation has partly informed the draft ePrivacy Regulation[[62]](#footnote-62) that will change some relevant rules, such as the (no longer compulsory) cookies notice. In the version adopted by the Council in September 2017,[[63]](#footnote-63) it presents a threefold strategy. Firstly, browser settings shall replace the cookie notice. Secondly, the exceptions to consent are clarified and expanded. Positively, the Presidency of the Council of the EU added a paragraph stating that the browser “shall provide in a clear manner easy ways for end-users to change the privacy setting consented to […] at any time during the use.”[[64]](#footnote-64) 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[[65]](#footnote-65). 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”[[66]](#footnote-66).

The Article 29 Working Party stresses that opt-out mechanisms do not in principle deliver data subjects' consent. Only in very specific, individual cases could implied consent be argued.[[67]](#footnote-67) Therefore, the European data protection authority asks 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. Even though, to meet the requirements of Article 5(3) of the ePrivacy Directive, it is not necessary to request consent for each reading of the cookie, to keep data subjects aware of the monitoring, ad network providers should:

1. limit in time the scope of the consent;
2. offer the possibility to revoke it easily; and
3. create visible tools to be displayed where the monitoring takes place.

It does not seem that these principles have been adopted by the main actors of the Web.

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 is also applicable”.[[68]](#footnote-68) 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.[[69]](#footnote-69) 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.[[70]](#footnote-70) Therefore, as a policy recommendation, one should go back to the version of Article 5(3) prior to the 2009 amendment[[71]](#footnote-71) of 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 profiles and explicit profiles. The formeris created by observing individual and collective user behaviour over time, the latterfrom 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.[[72]](#footnote-72) Consequently, one must remain particularly vigilant. In the second one, an anti-paternalistic approach should 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 the users are given the possibility to delete the account and/or the data any time and as long as the ‘legals’ are readable.[[73]](#footnote-73) It is worth noting that the High Court of England and Wales in *Spreadex v Cochrane[[74]](#footnote-74)* has clarified that the clauses of such never-ending legals are not binding for noncompliance with the unfair terms regime.[[75]](#footnote-75)

The opinion of the Article 29 Working Party 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, ifit has obtained the user's consent to store or access information on the user’s terminal equipment, after having provided the information requested.

The Article 29 Working Party goes on to reason that, based on the definition and requirements for valid consent exArticle 2(h) of Directive 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”. Article 4(11) of the GDPR 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”. Arguably, methods such as that adopted by LinkedIn and Facebook, which equal using the site to agreeing to the cookie policy, are not compliant with the law.

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,[[76]](#footnote-76) 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”.[[77]](#footnote-77)

Finally, consent by browser setting to receive cookies in bulk is invalid, because it implies that users will accept future processing, possibly 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, calling on the European Commission to ensure that Article 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”.[[78]](#footnote-78) The statement criticises the European Commission for commending the EASA-IAB[[79]](#footnote-79) Best Practice Recommendation[[80]](#footnote-80) and Framework on behavioural advertising[[81]](#footnote-81) and a US-driven ‘do-not-track’ initiative,[[82]](#footnote-82) because they do not adopt the consent rule. This cast doubts (which then proved on this point baseless) on the position of the European Commission on this subject. The chapter, however, moves on to analyse the European and International self-regulation initiatives,[[83]](#footnote-83) since they can affect businesses’ and users’ behaviour even more than regulations and hard law initiatives.[[84]](#footnote-84)

**3. European and international self-regulation of targeted advertising**

In Europe, the public debate on OBA started as a 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.[[85]](#footnote-85) 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”.[[86]](#footnote-86) Therefore, one has to take into account the effects of the regulation on industry and its practicality, and “to consider the long-term health of digital environments”.[[87]](#footnote-87) Hence, she called for a self-regulatory solution, with the caveat that “it will need to be one clearly based on the applicable EU legislation”. The below assessment shows that the opt-out approach taken by the industry does not entirely comply with the European legal framework, even though some good steps have been taken.

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 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 that are 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.[[88]](#footnote-88)

The second principle regards the 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).[[89]](#footnote-89) 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).

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).[[90]](#footnote-90) Secondly, they should refer to the YourOnlineChoice.eu website (also “OBA User Choice Site”).

On 19 August 2016 at 10:43 GMT, this author visited the site and went to the “Your Ad Choice” section, where a message popped up: “Your Chrome browser blocks cookies used for behavioural advertising purposes. To successfully switch off behavioural advertising these cookies need to be enabled”. Therefore, strangely enough, one has to enable OBA cookies to disable targeted advertising. The system double-checked this author’s status with regard to 119 companies. In this occasion, it was found that three companies this author had never heard of before (Delta Projects, Captify, Atlas Solution) were delivering him targeted advertisements, even though he had always blocked third-party cookies and he had installed AdBlock Plus. Moreover, no company displayed the icon indicating that the “company is not delivering advertisements customised to your interests”.[[91]](#footnote-91)

It is commendable that the site adopts a user-friendly icon that contains a hyperlink to the OBA User Choice Site or to the third party notice.  It can be used to turn off OBA by some or all companies.



Fig. 1 Online behavioural advertising icon.

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.[[92]](#footnote-92) Moreover, it is not easy to assess the reliability of the tool. The experiment was repeated on 20 August 2016 at 10:28 GTM and results regarding only 8 companies (as opposed to 49) were displayed. This time the only company that was targeting this author was Accordant Media, 4 companies were experiencing technical issues and 3 companies had not set up a cookie, but might in the future deliver advertisements customised to his interests. Finally, the experiment was repeated a third time on the same day at 10:45 GTM and the results were again different. This time, this author was offered targeted advertising by ADEX, results regarding 18 companies were displayed, 3 companies had not set up a cookie, but might in the future deliver advertisements customised to his interests and 14 were experiencing technical issues. Accordant Media was one of the companies encountering technical issues, and thus not able to retrieve the relevant status.

The IAB’s framework, based on an opt-out mechanism with minor exceptions, is complemented by the EASA Best Practice Recommendation on OBA (hereinafter “the Recommendation”). EASA is a non-profit organisation dealing with advertising self-regulation issues and bringing together 34 national advertising self-regulatory organisations and 16 organisations representing the advertising industry.

The Recommendation provides “a pan-European, industry-wide self-regulatory standard for OBA, which empowers consumers across Europe”.[[93]](#footnote-93)

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.

The Recommendation draws its principles from those 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”.[[94]](#footnote-94)

Probably the most interesting part of the Recommendation regards enforcement: “[a] consumer could be making his feedback/complaint 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 (ADR) body (e.g. a consumers association). These would form different routes which could all transit a one stop shop for compliance. This would consist of a web page where the transfer of feedback/complaints would be passed to the relevant process and organisations.”[[95]](#footnote-95) 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.

The procedure in the second scenario is as follows. The scenario regards the use of a user’s sexual orientation data for OBA purposes without that user’s explicit consent. On 20 August 2016 at 12:30, this author conducted an experiment to assess whether sensitive data about sexual orientation were exploited to serve targeted advertisements or not. Therefore, he googled “gay.com”, “gay dates”, and “Grindr” (a popular gay dating mobile app). He then refreshed his Facebook feed and nothing gay-related appeared for some time. At 14:45 GTM, Facebook suggested him to subscribe to a group for “Sicilian gay bears”. However, this cannot be considered advertising, because the group was not selling products or services. At the same time, scrolling down the page this author noticed the sponsored page “Meetic.it”, which showed pictures of women. One might infer, hence, that Google and Facebook are not (directly) exploiting sensitive data on sexual orientation, but they might deduce from search terms that the user is looking for dates and the like. The experiment should be repeated and the results observed for a longer period, in order to present a more reliable outcome. For instance, it may not necessarily be a coincidence that, on the same day at 21:22 GMT, when this author was accessing Facebook via his smartphone, he was shown the advertisement of “Mrb&b”, an app (and service) for people looking for temporary gay-friendly accommodations. Likewise, the day after, at 00:02, he was shown an advertisement of the Western Fertility Institute, which provides surrogacy services to same-sex couples.

If one were convinced that Facebook[[96]](#footnote-96) was exploiting data on their sexual orientation without one’s explicit consent (or for other non-technical reasons), one should proceed as follows. One should turn to one’s national self-regulation authority or organisation, for instance the Istituto di Autodisciplina Pubblicitaria (IAP) in Italy.[[97]](#footnote-97) The IAP would assess whether it is competent in the matter or needs to transfer the complaint to the competent self-regulation authority following the EASA Cross-Border Complaint rules[[98]](#footnote-98) (for instance, it could transfer it to the Deutsche Datenschutzrat Online-Werbungor to the Advertising Standards Authority in the UK).[[99]](#footnote-99) If it is competent, the IAP will then decide whether the complaint is of substance.[[100]](#footnote-100) In particular, if the complaint does not raise any issue under the IAB Recommendation, it will inform the user that their complaint cannot be handled. If it deems that the complaint should be pursued, the IAP will contact the company concerned (in this case, Facebook) or refer the complainant to the latter. At this point, Facebook would be given the opportunity to resolve the issue informally, with or without mediation by the IAP, which should be informed of the outcome. If Facebook refused to resolve the complaint, did not resolve it satisfactorily or did not react to the enquiries, the IAP would launch a formal investigation. The IAP may consult experts in order to decide whether the company has breached the rules. The IAP’s jury (the Comitato di Controllo, which may refer to the Giurì),[[101]](#footnote-101) subsequently, would adjudicate the complaint. The ruling would be communicated to the parties (the main decision being the *ingiunzione di desistenza* to make the company desist) and then published on the website of the IAP and its database, with the names of the parties listed. If Facebook did not comply with the ruling, the jury would reiterate the *ingiunzione di desistenza* and would have it published in the newspaper, with the costs covered by Facebook itself. Should it continue to breach the rules on a persistent and deliberate basis, the IAP would apply other sanctions such as industry or relevant statutory referral.[[102]](#footnote-102)

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 Advertising and Marketing Communication Practice.[[103]](#footnote-103) It is interesting that, when commenting on the most significant changes to the Code, the first example given 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 that of IAB and EASA. Limiting the focus to 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”.[[104]](#footnote-104) 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”.[[105]](#footnote-105) 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”.[[106]](#footnote-106) Two provisions of the Code deserve a particular mention. First 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 fit the intricate supply chain of advertising (with responsibilities mainly shared between ad networks, advertisers, and publishers). Second, “[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”.[[107]](#footnote-107)

The international and European self-regulation systems are based on an opt-out mechanism which does not seem consistent with the law, in particular with the ePrivacy Directive[[108]](#footnote-108) 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”.[[109]](#footnote-109) Moreover, the opt-out tools can be and are sometimes ineffective. For instance, as one can read in the last report[[110]](#footnote-110) on cross-border complaints,[[111]](#footnote-111) in all the cases regarding OBA, the users complained about the opt-out mechanism because “they had continually been unable to opt out of OBA data collection and use”[[112]](#footnote-112) or “[d]espite selecting the ‘Off’ mode, the website kept on reverting to ‘On’ mode”.[[113]](#footnote-113) As already said, even if the right to consent is critical, one should start by ensuring the right to dissent, because in its present unenforced form it has no real effect. Furthermore, even though there seems to be an increasing percentage of users clicking on the OBA icon,[[114]](#footnote-114) there is no evidence that users actually know and understand what OBA is. On the contrary, this author has conducted a small-scale poll on Facebook. Its outcome is that 46 users did not know what targeted advertising was, whereas 10 users knew (one of which was an advertiser herself) and one was undecided. Notwithstanding the scale of the observation, a percentage of 17.5% has to be considered worryingly low, especially considering that the target users were young and highly educated.[[115]](#footnote-115)

**4. Profiling, direct marketing and algorithmic decision-making in the General Data Protection Regulation**

In 2013, a Member of the European Parliament asked the Commission if, in connection with targeted advertising, they could explain “why Facebook says it does not search for data, via keywords for example, in private and not public emails, but appears to be doing so anyway”.[[116]](#footnote-116) This is a common practice. For instance, on 20 August 2016 at 11:50 GTM this author accessed his Gmail account and he was shown an advertisement on the “MIT Big Data Course”. After clicking to learn more details, he was informed that he had been targeted due to the content of his emails and on the basis of the information of his Google account.

The Commission replied that the then proposal for a GDPR “clarifies and strengthens the rights of data subjects in the context of online activities, such as social networking: providers must take account of the principle of ‘data protection by default’”.[[117]](#footnote-117) It further pointed out that “[c]ompanies will be obliged to inform individuals as clearly, understandably and transparently as possible about how their personal data will be used, so that they are in the best position to decide what data they share”.[[118]](#footnote-118)

Strictly speaking, this reply did not really address the issues related to targeted advertising. Therefore, it can be useful to have a closer look at the Regulation to assess whether the problem has been taken into specific consideration.

The review process of the Data Protection Directive started in 2009[[119]](#footnote-119) and the first driver determining the environment in which the review process took place was technological development. Indeed, “[t]echnological phenomena like cloud computing, behavioural advertising, social networks, road toll collecting and geo-location devices profoundly changed the way in which data are processed and pose enormous challenges for data protection”.[[120]](#footnote-120) Therefore, the European Data Protection Supervisor suggested the insertion of a “specific provision protecting children against behavioural advertising”.[[121]](#footnote-121) Even at that time it was clear that the problem was not merely about the provisions themselves, but mostly about their enforcement. When stressing that there were areas where “full compliance needs to be monitored and enforced”,[[122]](#footnote-122) the Supervisor referred specifically to the proceeding of the Commission against the UK for alleged breach of various data protection provisions, including the requirement of confidentiality of electronic communications in respect of behavioural advertising.[[123]](#footnote-123)

This position has its roots in an opinion of 2010, when the Supervisor clarified the importance of privacy by default browser settings to guarantee informed consent to receive advertisements. It was noted, indeed, that “in practice very few people exercise the opt-out option, not because they have made an informed decision to accept behavioural advertisement, but rather because they do not realise that by not using the opt out, they are in fact accepting”.[[124]](#footnote-124) The interpretation of the existing rules was not deemed to be sufficient. Mandatory privacy by default settings are indicated as the solution whereby the users will have to change the browser settings if they are willing to receive targeted advertisements. In particular, it was held that the browsers should be set to reject third party cookies by default and new legislation should “require users to go through a privacy wizard when they first install or update the browser”.[[125]](#footnote-125)

After much debate, the European Commission published its proposal for a GDPR,[[126]](#footnote-126) which differed from the versions of the Parliament[[127]](#footnote-127) and the Council,[[128]](#footnote-128) and all the more from the final instrument, adopted on 27 April 2016, which will apply from 25 May 2018.

It is noteworthy that the Economic and Social Committee, in opining on the Commission’s proposal, stressed that one of the things to be included in the scope of the regulation should have been search engines, “the majority of whose revenue comes from targeted advertising thanks to their collection of personal data concerning the visitors to their sites, or indeed the profiling of those visitors”.[[129]](#footnote-129)

Now, 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”. Given that targeted advertising is usually based on predictive 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 (targeted advertising may be considered as different from, albeit intrinsically connected with, direct marketing) and because thanks to its generic reference to automated decisions affecting (not necessarily from a pecuniary point of view) the user, it fits targeted advertising scenarios well.

Nothing in this provision expressly mentions 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. Nonetheless, one has to appreciate that at least the GDPR mentions online advertising. Its recital 58 stresses 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 that 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[[130]](#footnote-130) 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 most 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 defences whereby controllers assert 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 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 very peculiar provision. Indeed, if the data subject has the right to object to the processing of his or her data for direct marketing purposes, it is in the very nature of thingsthat further processing for marketing purposes would be illegal. Therefore, the provision has two possible interpretations: 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 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”.[[131]](#footnote-131) 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”[[132]](#footnote-132), a sort of objection by design (e.g. through adblockers). Even though that “may” weakens the provision, it may still 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 becoming a classic case of overload of information. For instance, should every website present the user with, say, separate notices for cookies and direct marketing? It shall be seen if the revision of the ePrivacy directive takes account of these issues.[[133]](#footnote-133)

Furthermore, it is questionable whether the new provision on automated individual decision-making constitutes a step forward. 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, as compared with the previous wording. However, two innovations are to be commended. Firstly, in principle automated decisions 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 or her point of view and to contest the decision”. This is a victory for those who think that human decision-making can still be better than its automated counterpart.

A target of specific interest for the European legislature 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)). It is hardly imaginable that a 15-year-old guy would call his parents and ask for their authorisation every time Facebook or Google are processing his data. However, what strikes is not this rather ludicrous provision. It is that, under art. 8(2), 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.[[134]](#footnote-134) The remedy risks being worse than the disease.

As observed by the European Commission, what matters is not (necessarily) the right to consent, but the right to dissent. Indeed, the last new provision that deserves to be stressed is that now direct marketing is a ‘legitimate interest’ to process the users’ personal data without their consent (recital 47).[[135]](#footnote-135) This may be interpreted as the result of a balance between data protection and freedom of enterprise. Indeed, competitiveness may be hampered if an undertaking is required to obtain the users’ consent prior to any processing for targeted advertising and direct marketing.

More generally, there are provisions which do not directly focus on direct marketing, but will affect it nonetheless.[[136]](#footnote-136) For instance, the GDPR, unlike the Directive, will apply to the processing carried out even 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.[[137]](#footnote-137)

Overall, then the GDPR constitutes increased protection of the data subject, with some flaws. Alongside what is said above, for instance, it is submitted that referring to targeted advertising instead of direct marketing would have been preferable. For instance, it seems rather unfair that citizens can prevent companies from selling them products, but cannot avoid targeted advertising aimed to influence their voting preferences. Much will depend on how the courts will interpret the GDPR.

**5. “It’s a Google market”: Adsense, a recent change to the Google privacy policy and related details**

Advertising “is a Google market”[[138]](#footnote-138) and Google-controlled cookies are present on 97 of the top 100 sites.[[139]](#footnote-139) In 2015, Google's ad revenue amounted to more than USD 67 billion, thus accounting for the majority of the online company's total revenues.[[140]](#footnote-140) Its position in the advertising market is growing steadily.[[141]](#footnote-141)

Many users have been surprised to find out that Google records and stores their voice and that they can listen to it.[[142]](#footnote-142) Google tracks and profiles users across all their devices (which is worrying in an Internet of Things environment),[[143]](#footnote-143) using the data collected by its services (e.g. Search, YouTube, Maps) and storing all their searches, browsing history, and locations, thus enabling Google and its partners to have the full picture of who a user is and what he desires.

The search engine service plays a critical role in enabling Google to take the leading position in the targeted advertising market. Indeed, as called to mind by the Commission in the working document accompanying its recent communication on online platforms,[[144]](#footnote-144) Google is the most frequently used search engine in most EU countries, where it handles about 90% of search queries. It is unlikely, moreover, that the situation will change, due to the fact that significant costs are involved in creating a web index, developing a search algorithm and building computing centres.[[145]](#footnote-145) Therefore, cost-related economies of scope and scale allow search engine providers (primarily Google) to extract precious information from the large amounts of historical data from search queries submitted by users as well as other types of activity conducted by the users of the platform (email, use of maps, video, operating systems, internet browsers) and “[t]his argument is applicable for targeted advertising as well”.[[146]](#footnote-146) One needs only remember that the Court of Justice was able to condemn Google in the *Google Spain* case only because it found that advertising and search were “inextricably linked since the activities relating to the advertising space constitute the means of rendering the search engine at issue economically profitable and that engine is, at the same time, the means enabling those activities to be performed”.[[147]](#footnote-147)

Google shows ads based on:

1. The types of website that the user visits and the mobile apps that they have on their devices;
2. Cookies on the user’s browser and the settings in the Google account;
3. Websites and apps that the user has visited that belong to businesses that advertise with Google;
4. The user’s activity on another device;
5. The previous interactions with Google’s ads or advertising services;
6. The user’s Google account activity and information.[[148]](#footnote-148)

From the ad settings page,[[149]](#footnote-149) one may get the impression that the system is an opt-in one. Indeed, Google informs you about targeted advertising and it gives you the option to agree or not. Looking closer, however, one reads that “the Ads Personalisation setting *currently allows* Google to use data in your account to tailor ads that appear in Google products [and] on websites and apps that partner with Google” (emphasis added). This means that even if you do not express any consent, you will be served with bespoken advertisements. The legality of an opt-out mechanism for targeted advertising is indeed debatable.[[150]](#footnote-150)

The users are offered some tools to delete the personal information regarding them and, sometimes, to prevent its collection.[[151]](#footnote-151) However, these means are not always user-friendly and, what is more important, they can be circumvented, as the *Vidal-Hall v Google* case has shown. Alongside deleting personal information, the user has an interest in not receiving intrusive advertisements. There are several browser extensions (e.g. Adblock plus) and products (e.g. eBlocker) for this purpose. However, one cannot access many websites once the extension is installed (unless one puts the site on a whitelist or subscribes to it). The reason is made clear, for instance, by the ToS of the online version of the magazine Forbes, under section 1.5, whereby “Free access to the content made available to you on the Website is possible due to the paid advertising that appears on the Website. Without this advertising, we would not be able to provide you with this content for free. In exchange for your free access to this content, you agree that *you will not, and will not permit any third party to, remove, obstruct, modify or otherwise interfere with the delivery or display of advertisements* on the Website”.[[152]](#footnote-152)

The importance of the issue has been (I suggest to delete given that the book will be published in 2018) confirmed by the battle between Facebook and Adblock Plus. On 9 August 2016, Facebook has released an ad block bypass, offering ad targeting opt-outs. In just two days, Adblock Plus has launched a workaround called FB-reblock. On the same day, the popular social network platform has reacted by rolling out the code update to disable Adblock Plus’ workaround.[[153]](#footnote-153) We are just at the beginning of a war and legislators and regulators intervene as usual too late to regulate the process.[[154]](#footnote-154)

Google uses the DoubleClick cookie on publisher websites displaying AdSense[[155]](#footnote-155) for content ads.[[156]](#footnote-156) In theory, “DoubleClick cookies contain no personally identifiable information”.[[157]](#footnote-157) However, as said above, by recombining the information of the multiple devices of a user and the data relevant to the use of the services provided by Google and its partners, it is easy for the non-personal information to become personal and, hence, subject to data protection laws. The consent to these policies can hardly be considered meaningful, since the user is rarely aware of the data collection. Indeed, when the server delivers the ad content, it also sends a cookie. However, “a page doesn't have to show DoubleClick ads for this to happen; it just needs to include DoubleClick ad tags, which might load a click tracker or impression pixel instead”.[[158]](#footnote-158) One could object that all publishers must clearly display a privacy policy notifying visitors about the site's use of cookies. Nonetheless, it is common experience that it is customary the take it or leave it approach: either you accept the cookies policy by keep on surfing the site, or you can leave it. For instance, on 12 August 2016, this author first blocked all cookies and then tried to access the search setting preferences on Google Chrome, which sent him the following automatic message.

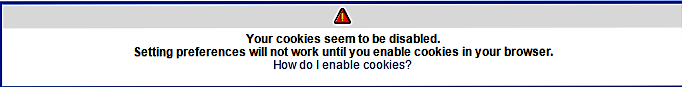


Fig. 2

Similar consequences occur for other Google services (e.g. Gmail),[[159]](#footnote-159) but also on other websites, as seen above when discussing the review process of the ePrivacy Directive.

Furthermore, there is a risky obsession with consent in the public discourse on privacy. The truth is that there are several justifications for data controlling.[[160]](#footnote-160) Consent is just one of them and requiring it for each and every kind of processing is cumbersome and hinders transparency and users’ awareness. For instance, one of the several documents the user should be aware of is Google’s EU user consent policy.[[161]](#footnote-161) This requires the European user to express consent for each and every collection, sharing and use of data on every site or app. Provisions like this look more like privacy white-washing, rather than a serious commitment to privacy.

One should note, however, that Google requests that the publishers should not use AdSense “to facilitate the merging of personally identifiable information with information previously collected as non-personally identifiable information without robust notice of, and the user's prior affirmative (i.e. opt-in) consent to, that merger”.[[162]](#footnote-162) This invitation is commendable, but there is no evidence as to its implementation and, what is more important, the big data controlled by Google still enable the company to recombine personal and non-personal data to single out users. More generally, computer scientists and engineers have stressed that, even if many tools empower users to control whether and when they are tracked for targeted advertising,[[163]](#footnote-163) “whether users can effectively control tracking and OBA using these tools is unclear”.[[164]](#footnote-164)

To add to the complexity, alongside the AdSense programme policies, there are additional policies for specific products, for instance AdMob, used for mobile applications. Its “Behavioural policies” deserve some attention. AdMob requires **test ads in order to avoid invalid clicks and impressions. Accounts are disabled if** Google finds such an invalid activity. The company analyses all clicks and impressions to determine whether they fit a pattern of use that might artificially drive up an advertiser's costs or a publisher's earnings. This approach is commendable; however, developments in artificial intelligence (e.g. machine learning) will render it more and more difficult to distinguish between machine/robot and human behaviour. Lastly, the policy states that “Google may use the advertising ID from the device on which the ad is being served to generate interests and demographics (for example, 'sports enthusiasts')”. It further clarifies that “interests, demographics, and other data may be used to serve better targeted ads to the user”. It is not clear which data these “other data” are. It probably refers to the targeting options, i.e. the parameters that make it possible to narrow down a mobile ad campaign to a specific audience.  Unsurprisingly, AdMob is at the top of the list and it is the service with the highest number of targeting options, that is: country, region, carrier, connection type, mobile platform, OS version, device, audience (user profile data).

The AdSense programme policies and the product-specific policies, together with the Terms of Service (ToS),[[165]](#footnote-165) form the agreement between the publisher and Google. As to privacy, the ToS refer to the general Google Privacy Policy,[[166]](#footnote-166) which applies to all services provided by the company, unless otherwise stated.[[167]](#footnote-167) The latter ensures that “[w]hen showing you tailored ads, we will not associate an identifier from cookies or similar technologies with sensitive categories, such as those based on race, religion, sexual orientation or health”.[[168]](#footnote-168) However, it is very easy to infer these data, for instance through an analysis of the searches on Google Search. For instance, if one searches for information about pills for a kidney disease, one will soon be shown relevant ads on one’s social networking page.[[169]](#footnote-169) Moreover, there is the issue of data recombination, as touched on above. Indeed, “your activity on other sites and apps may be associated with your personal information in order to improve Google’s services and the ads delivered by Google”.[[170]](#footnote-170) Therefore, even if the ad is not supposed to collect personal information about the user, the personal information controlled by Google can be used for targeted advertising purposes. Google requires “opt-in consent for the sharing of any sensitive personal information”,[[171]](#footnote-171) in contrast with the Article 29 Working Party’s opinion requiring opt-in mechanisms for all personal data (not only sensitive ones).

Furthermore, Google is not an island. It is part of a very intricate corporate structure and it partners with several companies. This can jeopardise privacy, as can be inferred by another passage of the privacy policy. Indeed, “Our Privacy Policy does not cover the information practices of other companies and organisations that advertise our services and that may use cookies, pixel tags and other technologies to serve and offer relevant ads.”

Google is the strongest actor of the behavioural advertising world because it can monitor the users across several devices and services. The system feeds itself. In other words, if most of the advertisers, publishers, etc. use Google’s services for advertising, at the same time they are providing Google with further data. Every time the user browses a website that does not belong to Google, but, for instance, uses AdSense, the +1 button of Google+, or Google Analytics, “your web browser automatically sends certain information to Google”.[[172]](#footnote-172) The same happens when using the apps that partner with Google.

On 13 September 2016, Google informed its users that there were some new features in their accounts. The declared purpose of the introduction was to give the user “more control over the data Google collects and how it’s used, while allowing Google to show you more relevant ads”.[[173]](#footnote-173)

The first news is that more data will be available in the Google account. This includes all the data related to things the users search for, videos they watch on YouTube, and browsing data from Chrome,[[174]](#footnote-174) as well as activity from sites and apps that partner with Google,[[175]](#footnote-175) including those that show ads from Google. On the one hand, this is a lot of information, also because the new settings apply across all of the signed-in devices and across all Google services.[[176]](#footnote-176) On the other hand, Google was already able to recombine the data produced by the use of all its different services. The news is that users now have a single place to review and control it. Moreover, Google is transparent as to the use they want to make of these data (and therefore, implicitly, of the *raison d’* *être* of the policy update): to serve more tailored advertisements.

Google also wants to increase its market power. Therefore, whereas now it can “only” use the data in “My Account” to tailor ads that appear in Google products, with the policy update the company will be allowed to leverage these big data also for targeted advertisements “on websites and apps that partner with Google”.

Again, it is a huge amount of data. However, Google provides the users with the power to control and review its activity through “Web & App Activity” and “Ads Personalisation”.

If the reader of the update wants to “Learn more”, they will discover the real revolution behind the update: Google is sending cookies into retirement. Indeed, instead of serving ads based on a cookie ID for each device (which became quite useless in an Internet of Things era), “this change makes it possible to use a single identifier associated with your account that gets used in Google products and across the web”.

Finally, it is commendable that there was no pre-ticked box (unlike the last WhatsApp policy update). One was able to choose between “I agree” and “Other options”, which looked very straightforward (see screenshot below).

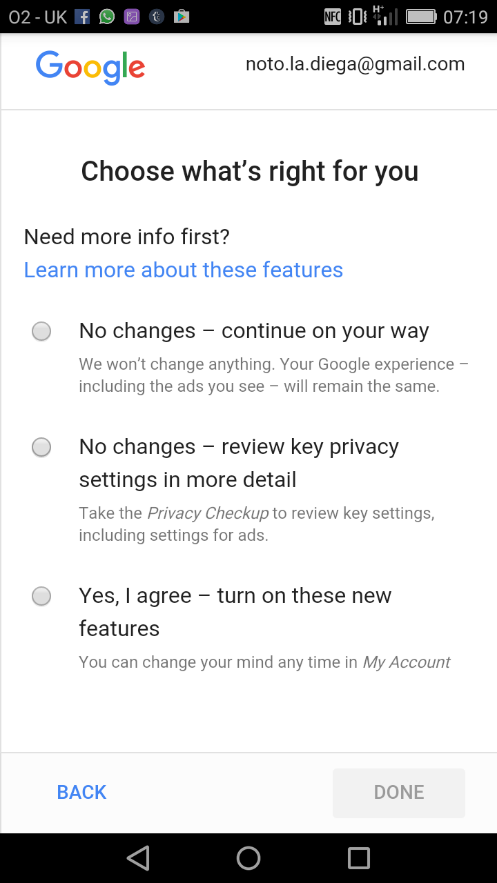


Fig. 3

**6. The use of digital assets to hinder competition. Facebook and WhatsApp: from the concentration to the transfer of the latter’s user data to the former’s IP portfolio**

Companies (advertising networks, publishers, advertisers) can leverage the data in their IP portfolio to carry out unfair commercial practices and, more generally, to jeopardise competition.[[177]](#footnote-177)

It is easily imaginable, for instance, that exploiting the users’ data without their consent (or even awareness) or, more generally, using the users’ data illegally does not merely damage consumers, but can also harm competitors. Also price discrimination and dynamic pricing based on profiling activities (e.g. offering a different price if one accesses a website from an old desktop than from an iPhone) might seem an unfair practice, but the Commission has clarified that under the Unfair Commercial Practices Directive[[178]](#footnote-178) “traders are free to determine their prices if they duly inform consumers about the prices or how they are calculated”.[[179]](#footnote-179) However, some provisions of the said Directive do not really fit the reality of targeted advertising. For instance, under Art. 5(3), “[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 current tracking and profiling techniques, it is unrealistic to allow for the possibility that a company might not be able to 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, should be changed accordingly. One solution might be a presumption of vulnerability when it comes to targeted advertising, in consideration of the intrinsic characteristics of this kind of advertising.[[180]](#footnote-180)

Another issue is the persistency of unwanted targeted advertisements. It is believed that 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’).[[181]](#footnote-181) Lastly, it has been suggested that “an undue increase in the use of personal data may very well be compared to excessive prices”,[[182]](#footnote-182) thus amounting, potentially, to a practice constituting abuse of dominant position.

As recently reaffirmed by the General Court in the first case of pay-for-delay in the pharmaceutical industry,[[183]](#footnote-183) competition law can be used as a tool to prevent some of the IPRs holders’ abuses. The below passages will assess if this could be the case in a recent event regarding the transfer of WhatsApp’s users data to Facebook.

Harnessing the big data controlled by Facebook (directly and through its subsidiaries), the popular social networking platform can be considered one of the strongest actors in the targeted advertising world, especially considering its share of collected data across the web.[[184]](#footnote-184) Indeed, in 2015, Facebook's advertising revenue was USD 17.08 billion.[[185]](#footnote-185)Many approaches may be followed in choosing Facebook as a case study on targeted advertising. Here the focus will be on a mostly overlooked perspective, i.e. competition. There are many aspects of the Commission’s decision[[186]](#footnote-186) on the Facebook / WhatsApp concentration that offer a sample of the relevance of targeted advertising[[187]](#footnote-187) from a competition law perspective. This decision, by the by, should be read again today in light of the use Facebook in August 2016 commenced making of WhatsApp users’ data for targeted advertising purposes.[[188]](#footnote-188)

To briefly recap the facts, in the summer of 2014, the European Commission received notification of a proposed concentration pursuant to Article 4 of the Merger Regulation, and following a referral pursuant to Article 4(5) of the Merger Regulation, by which Facebook, Inc. acquired within the meaning of Article 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.

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 already had its own instant messaging app, Messenger. In assessing the closeness to competition, however, the Commission explains that Messenger is a stand-alone app that was 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”.[[189]](#footnote-189) This is no longer the case after the update to the “legals” of WhatsApp occurred on 25 August 2015.[[190]](#footnote-190) 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 (see the screenshot below[[191]](#footnote-191)). ii. The opt-out procedure is not straightforward.[[192]](#footnote-192) 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.

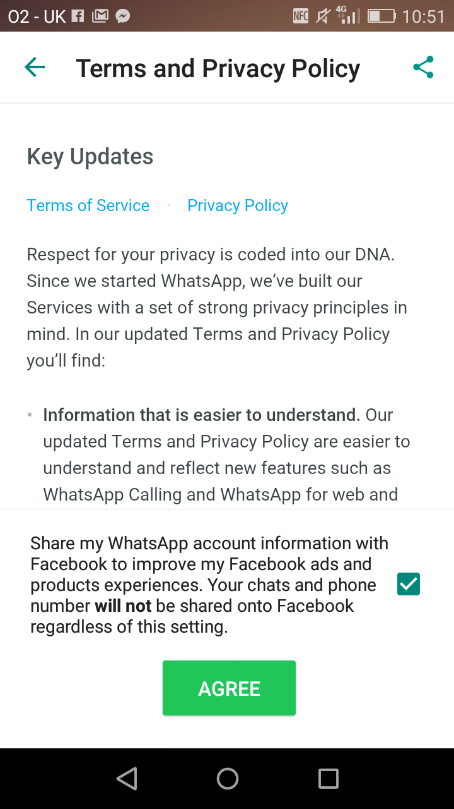


Fig. 4

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, the new ToS state:

*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 the assessment of whether Facebook and WhatsApp were direct competitors, the Commission found that they were not and therefore authorised the concentration. It can be argued that, if the Commission was notified today of the said transaction, the conclusion would be different. Indeed, at that time the Commission considered Facebook as in direct competition with Twitter or Google Hangouts, but not with WhatsApp, which was in turn closer to Viber.[[193]](#footnote-193) 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 by using advertising, in-app purchases, and stickers, “Messenger is not currently monetised: it is funded by the monetisation of Facebook's networking platform through advertising”.[[194]](#footnote-194) Therefore, it is to be believed 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 by chance that, as seen above, this has been the subject of a written question to the Commission.[[195]](#footnote-195)

In the concentration, there are three relevant markets: consumer communications services, social network platforms, and online advertising. The latter is of main interest here.

Facebook's activities in the advertising sector consist in the provision of online (non-search) advertising services on Facebook's core social networking platform and on Instagram[[196]](#footnote-196) (which is its subsidiary as well), both on computers and on mobile devices. As noted above in the case of Facebook and Mrb&b, Facebook collects its users’ data (also through its subsidiaries[[197]](#footnote-197)) and analyses them in order to 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,[[198]](#footnote-198) 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 ads as non-substitutable, since they serve different purposes (search advertisements mainly generate direct user traffic to the merchant's website, while non-search advertisements mainly build brand awareness).[[199]](#footnote-199)

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”.[[200]](#footnote-200) Nonetheless, the Commission decides 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[[201]](#footnote-201) such narrower product market definition”.[[202]](#footnote-202)

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.[[203]](#footnote-203) Therefore, In line with the *Google / DoubleClick* and *Microsoft / Yahoo! Search Business* decisions, the Commission concluded that the online advertising market and its possible sub-segments should be defined as national in scope or alongside linguistic borders within the EEA.[[204]](#footnote-204)

The Commission exposed itself to criticism by taking a rather formalistic approach,[[205]](#footnote-205) rigidly distinguishing between a competition law approach and a privacy law approach, whereas a holistic one would have been appropriate. The Commission seems to imply that there may be privacy concerns emerging from the merger, but this is not a matter for 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 whether there is an overlap. This seemed to be the case in 2014 and is all the more true now, after the terms update of 25 August 2016. It has, indeed, become clear that one of the main ways Facebook is profiting from the authorised merger is in its access to the gigantic amount of data once controlled by WhatsApp. At any rate, even if the Commission continued to adopt the said formalistic approach, if the Commission had to decide on this case 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”.[[206]](#footnote-206)

However, the Commission also assessed the possibility that, in the future, Facebook would start 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";[[207]](#footnote-207) ii. "Facebook has publicly made it clear that it has no current plans to modify WhatsApp’s collection and use of user data";[[208]](#footnote-208) 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”;[[209]](#footnote-209) iv. Facebook pointed out, debatably, that it was technically nearly impossible "to match each user's WhatsApp profile with her/his Facebook profile";[[210]](#footnote-210) v. There was no incentive to use the WhatsApp users’ data, because this would lead them to abandon the famous app in favour of more privacy-friendly competitors such as Telegram. It can be said that some or all of these assertions were wrong. For instance, the last statement ignores some basic concepts such as lock-in and network effect. However, what is decisive is that, given the leading position of Google (also) in the online advertising market, the only merger that would probably not be authorised is the Google / Facebook one.

As a brief note on the aftermath: in September 2016 the European Commissioner for Competition Margrethe Vestager declared that she has asked some follow-up questions to Facebook, in relation to the change of WhatsApp’s 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”.[[211]](#footnote-211) We do not know yet how the story will end, nor does the Commissioner, who leaves the social network and us in the dark by saying that “[w]hat we’re going to do with the answers we get is still an open question”.[[212]](#footnote-212)

1. **Conclusions. A more balanced approach to data as digital assets and the “Cooperative Charter on Online Behavioural Advertising”**

Targeted advertising can be a positive phenomenon, inasmuch as it helps the user experience to be less disrupted by irrelevant advertisements. On the other hand, there can be several problems for the consumer, for instance in terms of price discrimination, influence on voting preferences, distress at having the (well-grounded) feeling that one cannot really escape the advertising net. The principles at stake are of the highest importance; they include autonomy[[213]](#footnote-213) and self-determination.[[214]](#footnote-214) The best consumers are the most predictable ones, and it is understandable why companies are doing their best to influence our present and future behaviour in subtler and subtler ways, especially through subliminal messages[[215]](#footnote-215) and machine learning algorithms to which users do not have access. At the same time, however, it is not possible to ban targeted advertising by saying that it conflicts with data protection, privacy, and consumer protection. As mentioned above, if the targeted advertising is effective, data protection laws will apply, because the clear purpose of the former is to single out a consumer. Banning targeted advertising altogether would be contrary to the principles of competition and freedom of enterprise and it would jeopardise one of the biggest assets in the IP portfolio of a great many companies.

The approach being taken to data in Europe is far from holistic. Leaving aside the rhetoric of fundamental and human rights, it is apparent that most regulators take account of data only from a perspective of privacy and data protection, thus showing their failure to understand the role of data as digital assets.[[216]](#footnote-216) Probably, if citizens were aware of the economic value of their data, and if data were treated as their intellectual property,[[217]](#footnote-217) then they would care more about the information they share.[[218]](#footnote-218) The legal tools introduced over the years by lawmakers and regulators under the data protection umbrella have proven to be quite easily circumventable by online intermediaries, public bodies, and hackers. The developments concerning targeted advertising confirm this insight. Therefore, to empower the citizens in their online dimension, as well as in the offline one, this chapter calls on lawmakers, regulators, judges, and academics to embrace a shift of paradigm. Too many times compliance with the data protection rules has proven to be impossible or fictitious (the ePrivacy Directive with its mechanism on cookies provides robust evidence of this). Data protection laws should be simplified and informed by a holistic interplay of data protection, intellectual property, consumer protection, and competition. There are at least two reasons to do this. Firstly, in a world where the economy is global and space is virtual, it is not possible for all the national systems to demand compliance with their own (sometimes radically different) rules.[[219]](#footnote-219) Secondly, like it or not, data have become the crucial commodity for countless markets and companies.

Opt-in mechanisms would provide a stronger protection for users, but the international and European self-regulatory frameworks have made clear that there is no chance that companies will voluntarily adopt the opt-in mechanism. At the same time, the ePrivacy Directive shows how useless certain legal burdens based on pure consent can be. Hence, one may take a pragmatic approach and try to make the former method work.

Therefore, it is proposed the following “Cooperative Charter on Online Behavioural Advertising”

**Article 1**

Users have the right to opt out from online[[220]](#footnote-220) advertising altogether, as well as from its single types.[[221]](#footnote-221) 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[[222]](#footnote-222), 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 gamified*[[223]](#footnote-223)* 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’ intellectual property portfolios. Users can issue data licenses, which can be terminated at any time. Personal data cannot be assigned and the relevant remedies cannot be excluded by means of a contract.

**Article 5**

Companies responsible for online behavioural advertising (primarily, advertising networks, publishers, advertisers) act in good faith.[[224]](#footnote-224) 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*[[225]](#footnote-225)*.

**Article 7**

Companies make available optional*[[226]](#footnote-226)* online dispute resolutions, and refrain from mandatory binding arbitration.

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

There are some technical as well as legal tools that can enhance privacy in an environment of ubiquitous surveillance, like the one necessary for targeted advertising to thrive. Some of these means can be easily circumvented (see the AdBlock Plus v Facebook war) or are more apparent than real (see the experiment on the consequences of blocking all cookies).[[227]](#footnote-227) Tracking and profiling, however, are not all bad. For some time, this author used DuckDuckGo, the search engine famous for not tracking users. The problem was that the results of the searches were utterly useless. To receive suggestions of music we can enjoy on YouTube, to be shown news we are interested in or search results that answer our questions precisely, badly formulated though 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.[[228]](#footnote-228) Even targeted advertising, if freely and actively chosen, with the possibility to withdraw one’s consent any time, can reduce our search costs, thus making our life easier. Letting users understand that their data are a critical digital asset of their IP portfolio is a good way to raise awareness and increase the quality of data flows and the overall satisfaction of all the actors of the market. The awareness of the pros and cons of this practice should be kept in mind by courts and regulators that are called upon to protect users’ privacy, but also to strike a balance between that privacy and intellectual property, free competition, and consumer protection.

The GDPR constitutes a step forward as compared with the Data Protection Directive, but much will depend on the revision of the ePrivacy Directive and on the adoption of the Cooperative Charter on Online Behavioural Advertising. Hopefully, algorithmic accountability and transparency, the right to dissent, gamified interactions and the right to disconnect will be the North Star that the online sailors follow.[[229]](#footnote-229)

**Afterword. Of chocolate chips and lavender buds.**

I recently came across a story that deserves to be shared, because it reminds us to avoid any kind of simplism and invites us to adopt more nuanced approaches when it comes to our online lives.

Amy and her husband had long tried to conceive, unfortunately without success. Therefore, when the magenta plus sign materialised on the stick, they were overwhelmingly happy. On the day of the positive pregnancy test, Amy logged into her period tracker to share the good news. The tracker suggested a pregnancy app that Amy downloaded. It was very entertaining and sweet, it showed the evolutions of the baby, who initially was the size of a lavender bud. Alas, when the baby had reached the stage of the chocolate chip, Amy miscarried. Once home from the clinic, Amy terminated her virtual pregnancy with the touch of a button. The app responded with a soothing email and cleared her data. Harsh times followed, understandably, when one day a parcel arrived. Seven months after the miscarriage, Amy received a box of baby formula bearing the note: “We may all do it differently, but the joy of parenthood is something we all share.” A product she had never intended to use from people she had never told she was pregnant at a company she had never heard of. The period tracker had shared, that is to say sold, her data to providers of products for mothers. One’s instinct, in reading this story, could be to react with a sense of repulsion and by condemning tracking, profiling, and direct marketing altogether. However, if tracking, profiling, and direct marketing had worked properly, this unfortunate event would not have happened. If the reader is wondering how the story ends, it is with a bitter laugh. When Amy received the box, she laughed. Indeed, on the one hand, she “liked the idea that a data-hungry entity like the internet, which is so intimately involved in every trivial aspect of our lives, had completely missed the most important news of all”.[[230]](#footnote-230) On the other hand and more importantly,  she realised that her “little chocolate chip, long since deleted, is indeed out there somewhere, drifting around in cyberspace, endlessly trolling the internet”.[[231]](#footnote-231)

**Reference list**

Article 29 Working Party (2011), Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising, adopted on 8 December 2011, 02005/11/EN WP 188, European Commission

Article 29 Working Party (2010), Opinion 2/2010 on online behavioural advertising, adopted on 22 June 2010, 00909/10/EN WP 171, European Commission

Article 29 Working Party and Working Party on Police and Justice (2009), The Future of Privacy. Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, adopted on 1 December 2009, 02356/09/EN WP 168, European Commission

Ask Your Target Market (2011), Targeted Advertising Survey: Many Worried About Privacy Violations, Aytm.com of 20 December 2011, available at: <https://aytm.com/blog/daily-survey-results/targeted-advertising-survey/#sthash.3rEVQvsg.dpbs>

Bakshy, E. / Messing, S. / Adamic, L. (2015), Exposure to ideologically diverse news and opinion on Facebook, in: SciencExpress of 7 May 2015, available at: <http://cn.cnstudiodev.com/uploads/document_attachment/attachment/681/science_facebook_filter_bubble_may2015.pdf>

Bauer, C. / Eickmeier, F. (2016), GDPR: What’s Relevant for the Use of Cookies & Identifiers in Online Marketing, ExchangeWire of 24 May 2016, available at: <https://www.exchangewire.com/blog/2016/05/24/gdpr-whats-relevant-for-the-use-of-cookies-identifiers-in-online-marketing/>

Bauer, C. / Breuer, M. / Diebold, D. / Eickmeier, F. / Klekamp, J. / Maucher, S.-A. / Neuber, N. / Rackwitz, G. / Wegmann, T. (2015), Browsercookies und alternative Tracking-Technologien: technische und datenschutzrechtliche Aspekte, BVDW Whitepaper of September 2015, available at: <http://www.bvdw.org/medien/browsercookies-und-alternative-tracking-technologien-technischeund-datenschutzrechtliche-aspekte?media=7007>

Bernal, P. (2012), Phorm – A chapter closes?, Blog post of 28 January 2012, available at: <https://paulbernal.wordpress.com/2012/01/28/phorm-a-chapter-closes/>

Bray, O. / Griffiths, S. (2008), Information Commissioner's Office opinion on Phorm's targeted advertising technology,World Data Protection Report 2008, 8(6), 24-26

Caddy, B. (2015), Google tracks everything you do: here's how to delete it, Wired of 15 October 2015, available at: <http://www.wired.co.uk/article/google-history-search-tracking-data-how-to-delete>

Calabrese, C. / McInnis, K.L. / Hans, G.S. / Norcie, G. (2015), 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, available at: <https://cdt.org/files/2015/10/10.16.15-CDT-Cross-Device-Comments.pdf>

Chamberlain, P. (2015), Misuse of private information: Google Inc v Vidall-Hall & Ors [2015] EWCA Civ 311, 20(3) Communications Law 93

Commission of the European Communities (1995), Report on application of Directive 89/552/EEC and Proposal for a European Parliament and Council Directive 89/552/EEC on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the pursuit of television broadcasting activities, COM(95)86 final 95/0074 (COD)

Constine, J. (2016), Facebook rolls out code to nullify Adblock Plus’ workaround, TechCrunch of 12 August 2016, available at: <https://techcrunch.com/2016/08/11/friendblock/>

Coutts, S. (2016), Anti-Choice Groups Use Smartphone Surveillance to Target ‘Abortion-Minded Women’ During Clinic Visits, Rewire of 25 May 2016, available at: <https://rewire.news/article/2016/05/25/anti-choice-groups-deploy-smartphone-surveillance-target-abortion-minded-women-clinic-visits/>

Cranor, L.F. (2012), Can Users Control Online Behavioral Advertising Effectively?, 2 IEEE Security & Privacy, 2012, 93

Cufoglu, A. (2014), User Profiling - A Short Review, International Journal of Computer Application 2014, 3, 1-9, Foundation of Computer Science

De Hert, P. / Papakonstantinou, V. (2016), The new General Data Protection Regulation: Still a sound system for the protection of individuals?, 32(2) Computer Law & Security Review 179.

Dempsey, M.A. / Mitchell, A.A. (2010), The Influence of Implicit Attitudes on Choice When Consumers Are Confronted with Conflicting Attribute Information, Journal of Consumer Research 2010, 37, 4, 614-625

Department of Business Innovation & Skills (2014), Misleading and Aggressive Commercial Practices – New Private Rights for Consumers. Guidance on the Consumer Protection (Amendment) Regulations 2014, August 2014, available at: <https://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>

Díaz-Morales, R. (2015), Cross-Device Tracking: Matching Devices and Cookies, 2015 IEEE International Conference on Data Mining Workshop (ICDMW), 2015, 1699-1704

Dogtiev, A. (2016), Top Mobile Ad Networks 2016, MobyAffiliates of 27 June 2016, available at: <http://www.mobyaffiliates.com/blog/top-mobile-ad-networks-2016/>

Drexl, J. / Hilty, R. / Desaunettes, L. / Greiner, F. / Kim, D. / Richter, H. / Surblytė, G. / Wiedemann, K. (2016), Data Ownership and Access to Data - Position Statement of the Max Planck Institute for Innovation and Competition of 16 August 2016 on the Current European Debate. Max Planck Institute for Innovation & Competition Research Paper No. 16-10, available at: <https://ssrn.com/abstract=2833165>

Eggers, W. / Hamill, R. / Ali, A. (2013), Data as the new currency: Government’s role in facilitating the exchange, Deloitte Review 2013, 13, 19-29

European Advertising Standards Alliance (2015a), Cross-Border Complaints Quarterly Report no. 68 April – June, available at: <http://www.easa-alliance.org/sites/default/files/2015%20EASA%20Cross-Border%20Complaints%20Report%20No.%2068.pdf>

European Advertising Standards Alliance (2015b), Cross-Border Complaints Quarterly Report no. 67 January – March, available at: <http://www.easa-alliance.org/sites/default/files/2015%20EASA%20Cross-Border%20Complaints%20Report%20No.%2067.pdf>

European Advertising Standards Alliance (2014), Cross Border Complaints Report, available at: <http://www.easa-alliance.org/sites/default/files/2014%20EASA%20Annual%20Cross-Border%20Complaints%20Report.pdf>

European Advertising Standards Alliance (2011), Best Practice Recommendation on Online Behavioural Advertising, 13 April 2011, available at: <http://www.edaa.eu/wp-content/uploads/2012/10/EASA_BPR_OBA_12_APRIL_2011_CLEAN.pdf>

European Interactive Digital Advertising Alliance and TRUSTe (2015), European Advertising Consumer Research Report 2015. Consumer Awareness & Impact of European Self-Regulatory Programme for OBA, available at: <https://www.dropbox.com/s/2wueligxquyn5mm/EDAA-TRUSTe_2015%20Consumer%20Research%20Report.pdf?dl=0>

European Commission (2016a), Summary report on the public consultation on the Evaluation and Review of the ePrivacy Directive, 4 August 2016, available at: <https://ec.europa.eu/digital-single-market/en/news/summary-report-public-consultation-evaluation-and-review-eprivacy-directive>

European Commission (2016b), Commission Staff Working Document on Online Platforms, Accompanying the document Communication on Online Platforms and the Digital Single Market {COM(2016) 288 final}, SWD(2016) 172 final

European Commission (2016c), Commission Staff Working Document “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 {COM(2016) 320}”, SWD(2016) 163 final

European Commission (2016d), Commission Staff Working Document “Impact Assessment on the modernisation of EU copyright rules”. Accompanying the document “Proposal for a Directive of the European Parliament and of the Council on copyright in the Digital Single Market” and “Proposal for a Regulation of the European Parliament and of the Council laying down rules on the exercise of copyright and related rights applicable to certain online transmissions of broadcasting organisations and retransmissions of television and radio programmes” {COM(2016) 593} {COM(2016) 594} {SWD(2016) 301}, SWD(2016) 302 final

European Data Protection Supervisor (2011a), EDPS calls on the European Commission to ensure that safeguards for online behavioural advertising are respected, Press release of 11 July 2011, available at: <https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/PressNews/Press/2011/EDPS-2011-08_Behavioural%20advertising_EN.pdf>

European Data Protection Supervisor (2011b), Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions — ‘A comprehensive approach on personal data protection in the European Union’, 2011/C 181/01, Official Journal of the European Union of 22 June 2011 C 181/1

European Data Protection Supervisor (2010), Opinion of the European Data Protection Supervisor on Promoting Trust in the Information Society by Fostering Data Protection and Privacy, 2010/C 280/01, Official Journal of the European Union of 16 October 2010 C 280/1

Evans, K. (2015), Vidal-Hall and Risk Management for Privacy Breaches, 13(5) IEEE Security & Privacy 80

Fan, Y.C. / Chen, Y.C. / Tung, K.C. / Wu, K.C. / Chen, A.L.P. (2016), A Framework for Enabling User Preference Profiling through Wi-Fi Logs, IEEE Transactions on Knowledge and Data Engineering, 3, 592-603, IEEE

Federal Trade Commission (2009), Self-Regulatory Principles for Online Behavioral Advertising, FTC Staff Report of February 2009, available at: <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf>

Flint, D. (2016), Computers and Internet: what is the value of personal data? 37(1) Business Law Review (UK) 38

Gebicka, A. / Heinemann, A. (2014), Social Media & Competition Law, 37(2) World Competition 149

Gibbs, S. (2016), Facebook will delete your backed-up photos if you don’t install Moments app, The Guardian of 13 June 2016, available at: <https://www.theguardian.com/technology/2016/jun/13/facebook-delete-photos-moments-app>

Graham, N. / Anderson, H. (2008), Phorm: the legality of targeted advertising, 10(4) E-Commerce Law & Policy 1

Groom, S. (2014), Spam judgment against John Lewis highlights limits of soft opt-in and ICO Guidance, but questions remain, Osborne Clarke Marketing Law of 18 June 2014, available at: <http://marketinglaw.osborneclarke.com/data-and-privacy/spam-judgment-against-john-lewis-highlights-limits-of-soft-opt-in-and-ico-guidance-but-questions-remain/>

Hoofnagle, C.J. / Soltani, A. / Good, N. / Wambach, D.J. / Ayenson, M.D. (2012), Behavioral Advertising: The Offer You Cannot Refuse, 6 Harvard Law & Policy Review 273

Hustinx, P. (2011), Do not track or right on track? – The privacy implications of online behavioural advertising, Speech of 7 July 2011, available at: <https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Speeches/2011/11-07-07_Speech_Edinburgh_EN.pdf>

 Information Commissioner’s Office (2016), Overview of the General Data Protection Regulation (GDPR), 7 July 2016

Information Commissioner’s Office (2011), Personal Information Online Code of Conduct, v.2.0

Intellectual Property Office (2016), Intellectual Property Awareness Survey 2015, available at: <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/500211/IP_awareness_survey_2015.pdf>

Interactive Advertising Bureau (2011), Europe EU Framework for Online Behavioural Advertising, April 2011, available at: <http://www.edaa.eu/wp-content/uploads/2012/10/2013-11-11-IAB-Europe-OBA-Framework_.pdf>

International Chamber of Commerce (2011), Advertising and Marketing Communication Practice Consolidated ICC Code, Document No. 240-46/660 of August 2011, available at: <http://www.codescentre.com/media/2083/660%20consolidated%20icc%20code_2011_final%20with%20covers.pdf>

Istituto di Autodisciplina Pubblicitaria (2015), Regolamento sulla Pubblicità Comportamentale Online – OBA, November 2015

Iveson, K. (2016), How Pokemon Go will make money from you, The Sydney Morning Herald of 3 August 2016, available at: <http://www.smh.com.au/comment/how-pokemon-go-will-make-money-from-you-20160802-gqj457.html>

Joung, Y.-J. / Yen, C. / Huang, C.-T. / Huang, Y.-J. (2005), On personal data license design and negotiation, 29th Annual International Computer Software and Applications Conference, 2005. COMPSAC 2005, IEEE

Kanoje, S. / Girase, S. / Mukhopadhyay, D. (2014), User Profiling Trends, Techniques and Applications, International Journal of Advance Foundation and Research in Computer 2014, 1, 1-6, IJAFRC

Kerr, I.R. / Bornfreund, M. (2005), Buddy Bots: How Turing's Fast Friends Are Undermining Consumer Privacy, Presence 2005, 6, 647-655, MIT Press

Kilian, W. (2012), Personal Data: The impact of Emerging Trends in the Information Society. How the marketability of personal data should affect the concept of data protection law, 13(6) Computer und Recht International (Cri) 169

Klein, W.E.J. (2016), Can We Trust For-Profit Corporations to Protect Our Privacy?, September, IEEE Technology and Society Magazine 17

Kopstein, J. (2016), Brands Want To Predict Your Behavior By Mining Your Face From YouTube Videos, Motherboard of 24 May 2016, available at: <http://motherboard.vice.com/read/facial-recognition-brands-mattersight>

Kroes, N. (2010), Towards more confidence and more value for European Digital Citizens**,** European Roundtable on the Benefits of Online Advertising for Consumers, Speech of 17 September 2010, available at: <http://europa.eu/rapid/press-release_SPEECH-10-452_en.htm>

Liem, C. / Petropoulos, G. (2016), The economic value of personal data for online platforms, firms and consumers, Blog post of 14 January 2016, available at: <http://bruegel.org/2016/01/the-economic-value-of-personal-data-for-online-platforms-firms-and-consumers>

Linkomies, L. (2008), BERR approves of Phorm's targeted-advertising techniques, Privacy Laws & Business United Kingdom Newsletter 2008, 38(Oct), 12

Lomas, N. (2016), WhatsApp to share user data with Facebook for ad targeting — here’s how to opt out, TechCrunch of 25 August 2016, available at: <https://techcrunch.com/2016/08/25/whatsapp-to-share-user-data-with-facebook-for-ad-targeting-heres-how-to-opt-out/>

Marshall, J. (2014), Do Consumers Really Want Targeted Ads?, The Wall Street Journal Blog of 27 April 2014, available at: <http://blogs.wsj.com/cmo/2014/04/17/do-consumers-really-want-targeted-ads/>

Martens, B. (2016), An economic policy perspective on online platforms, JRC/IPTS Digital Economy Working Paper 2016-05, available at: <https://ec.europa.eu/jrc/sites/default/files/JRC101501.pdf>

Merikle, P.M. (2000), Subliminal perception, 17, 497, in: E. Kazdin (Ed.), Encyclopedia of Psychology, Oxford University Press

Michael, M.G. (2016), The Paradox of the Uberveillance Equation, IEEE Technology and Society Magazine 2016, September 2016, 14, IEEE

Mik, E. (2016), A Contractual Perspective on Consent and Notification Requirements in Privacy Legislation, Paper presented at the Society of Legal Scholars Conference of 6-9 September 2016, Oxford

Neelam, S. / Sood, S. / Mehmi, S. / Dogra, S. (2015), Artificial intelligence for designing user profiling system for cloud computing security: Experiment, 2015 International Conference on Advances in Computer Engineering and Applications (ICACEA) 2015, 51-58, IEEE

Network Advertising Initiative (2015a), Code of Conduct, May 2015, available at: <https://www.networkadvertising.org/sites/default/files/NAI_Code15encr.pdf>

Network Advertising Initiative (2015b), Guidance for NAI Members: Use of Non-Cookie Technologies for Interest-Based Advertising Consistent with the NAI principles and Code of Conduct, 18 May 2015, available at: <http://www.networkadvertising.org/sites/default/files/NAI_BeyondCookies_NL.pdf>

Noto La Diega, G. (2016a), Uber law and awareness by design. An empirical study on online platforms and dehumanised negotiations, 2015/2 European Journal of Consumer Law 383

Noto La Diega, G. (2016b), In light of the ends. Copyright hysteresis and private copy exception after the British Academy of Songwriters, Composers and Authors (BASCA) and others v Secretary of State for Business, Innovation and Skills case, in: C. Franchini (Ed.), Studi giuridici europei 2014, 39-60, Giappichelli

Pandey, K. / Mittal, A. (2016), User profiling on Tumblr through blog posts, 2016 International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT), 85-89, IEEE

Pang, Y. / Wang, B. / Wu, F. / Chen, G. / Sheng, B. (2015), PROTA: A Privacy-pReserving prOtocol for real-time Targeted Advertising, 2015 IEEE 34th International Performance Computing and Communications Conference (IPCCC) 1-8, IEEE

Pariser, E. (2011), The Filter Bubble: What the Internet Is Hiding from You, Penguin Press

Pittman, A. (2016), The Internet Thinks I’m Still Pregnant, The New York Time of 2 September 2016, available at: <http://www.nytimes.com/2016/09/04/fashion/modern-love-pregnancy-miscarriage-app-technology.html>

PwC (2015), Global entertainment and media outlook,PricewaterhouseCoopers

Purcell, K. / Brenner, J. / Rainie, L. (2012), Search engine survey 2012, Pew Research Centre Survey of 9 March 2012, available at: <http://www.pewinternet.org/2012/03/09/search-engine-use-2012/>

Reding, V. (2013), Answer given to the question for written answer E-000850/13 by Mrs Reding on behalf of the Commission, 8 April 2013, European Commission

Reed, C. / Kennedy, E. / Nogueira Silva, S. (2016), Responsibility, Autonomy and Accountability: legal liability for machine learning, Paper presented at the 3rd Annual Symposium of the Microsoft Cloud Computing Research Centre, 8-9 September 2016, Cambridge

Reed, C. (2016), Why Judges Need Jurisprudence in Cyberspace, Paper presented at the Society of Legal Scholars Conference 2016 of 6-9 September 2016

Rottondi, C. / Verticale, G. (2017), A Privacy-Friendly Gaming Framework in Smart Electricity and Water Grids, IEEE Access, 5, 14221-14233.

Rowinski, D. (2011), Mobile Advertising Explosion: Nexage Hits 8 Billion Impressions Per Month, in ReadWrite of 20 August 2011, available at: <http://readwrite.com/2011/08/10/mobile-advertising-explosion-n/>

Sattler, A. (2017), From Personality to Property? Revisiting the Fundamentals of the Protection of Personal Data, in: This book

Soltani, A. / Canty, S. / Mayo, Q. / Thomas, L. / Hoofnagle, C.J. (2009), Flash Cookies and Privacy, 10 August 2009, available at: <http://ssrn.com/abstract=1446862>

Sunstein, C.R. (2007), Republic.com 2.0, Princeton University Press

Surblytė, G. (2015), Competition Law at the Crossroads in the Digital Economy: Is it All About Google? 4 EuCML 170.

Tarabella, M. (2013), Question for written answer E-000850/13 to the Commission, Marc Tarabella (S&D), 28 January 2013, European Commission

Turow, J. / King, J. / Hoofnagle, C.J. / Bleakley, A. / Hennessy, M. (2009), Americans Reject Tailored Advertising and Three Activities that Enable It, Paper of 9 September 2009, available at: <http://ssrn.com/abstract=1478214>

White, A. / Levring, P. (2016), Facebook Grilled by EU’s Vestager Over WhatsApp Merger U-Turn, Bloomberg of 9 September 2016, available at: <http://www.bloomberg.com/news/articles/2016-09-09/facebook-grilled-by-eu-s-vestager-over-whatsapp-merger-u-turn>

Woodward, J.D. (2000), Is Biometrics an Age Verification Technology?, Santa Monica, RAND

Yan , J. / Shen, D. / Mah, T. / Liu, N. / Chen, Z. / Li, Y. (2011), Behavioral targeted online advertising, in: X.-S. Hua, T. Mei, A. Hanjalic (Eds.), Online multimedia advertising, 213-232, Information Science Reference

Zuiderveen Borgesius, F.J. (2016), Singling out people without knowing their names – Behavioural targeting, pseudonymous data, and the new Data Protection Regulation, Computer Law & Security Review 2016, 2, 256, Elsevier

1. \* Guido Noto La Diega is Lecturer in Law at the Northumbria University; President of ‘Ital-IoT’ Centre of Multidisciplinary Research on the Internet of Things; Fellow of the Nexa Center for Internet and Society; Convenor of NINSO The Northumbria Internet & Society Research Interest Group. Thanks to Eliza Mik for the valuable input and to Gintare Surblyte, Allison Felmy and Stella Wasielak for the thorough review. Responsibility for this chapter and the errors therein rests solely with the author.

   G. Noto La Diega

   Northumbria University School of Law, Newcastle upon Tyne, United Kingdom

   E-Mail [guido.notoladiega@northumbria.ac.uk](mailto:guido.notoladiega@northumbria.ac.uk) [↑](#footnote-ref-1)
2. Cf. European Commission, Case No. M.7217 – Facebook/ WhatsApp, 3 October 2014, para. 47, according to which the “vast majority of social networking services are provided free of monetary charges. They can however be monetised through other means, such as advertising or charges for premium services”. [↑](#footnote-ref-2)
3. Spotify is perhaps the most famous example of the “freemium” model. Amazon, LinkedIn, and Badoo are other noteworthy examples. [↑](#footnote-ref-3)
4. European Commission (2016d), part 1/3, para. 5.2.1. This part refers to user-generated content on online platforms, but the idea applies to several (I would say most) online “free” services. [↑](#footnote-ref-4)
5. On the use of high-frequency sounds to covertly track across a range of devices see Calabrese et al. (2015). For a solution based on semi-supervised machine learning methods see Díaz-Morales (2015). Cookie technologies may not be available in mobile applications. 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 ads 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 which, if one clicks on it (perhaps inadvertently), launches a web page in the mobile browser. Finally, one should keep an eye 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 (Soltani et al. (2009), 1-8). See also Bauer et al. (2015). [↑](#footnote-ref-5)
6. See Pandey / Mittal (2016), Fan et al. (2016), Kanoje et al. (2014) and Cufoglu (2014). [↑](#footnote-ref-6)
7. Targeted advertising is sometimes referred to as behavioural advertising, but, strictly speaking, the terms are not synonyms. Indeed, the former can be considered as the genus and the latter as a species. There are several ways a prospective customer can be targeted: for instance, by analysing previous behaviour (behavioural advertising), the page or the content the user is displaying (contextual advertising) or known characteristics of the data subject (age, sex, location, etc.), or the information provided by the data subject at the registration stage (segmented advertising). Even though behavioural advertising can be more intrusive and can lead to the collection of more personal data, the issues arising from the different types of targeted advertising are similar. Hence, the paper will refer mainly to the concept of targeted advertising. Recently, it is becoming fashionable to call the phenomenon “interest-based advertising”, but the change of names has practical consequences. [↑](#footnote-ref-7)
8. There are countless ways to provide targeted advertisements, but for brevity’s sake this chapter will not go into details. A good read is Yan et al. (2011), 213. [↑](#footnote-ref-8)
9. In re Facebook biometric - Information privacy litigation, Case 3:15-cv-03747-JD. [↑](#footnote-ref-9)
10. In Italy, the *Garante della protezione dei dati personali* has authorised, subject to an explicit consent of the data subjects, the collection of biometric data for profiling purposes, following a request of a bank which wanted to profile its clients to prevent fraud. See *Garante per la protezione dei dati personali*, *Verifica preliminare. Trattamento di dati personali e biometrici basato sull'analisi comportamentale dei clienti di una banca in occasione della loro navigazione nell'area privata del sito web*, 9 June 2016 n. 256. [↑](#footnote-ref-10)
11. Cf. Gibbs (2016). For the use of faces for advertising purposes see, for instance, Kopstein (2016). [↑](#footnote-ref-11)
12. Facebook Data Policy, available at: <https://www.facebook.com/policy.php>. Facebook’s strategy is quite clear. It is believed there is a common design behind 1) the new WhatsApp privacy policy allowing Facebook’s access to WhatsApp’s user data; 2) The separation of “Moments” and “Messenger” from the mother app; 3) The introduction of the “Live” function of Facebook; 4) The introduction of “Your Story” on Instagram; and 5) Instagram videos now recordable for up to 60 seconds (against the initial 15). Such functions incentivise users to produce more data and harness them (mainly) for advertising purposes. [↑](#footnote-ref-12)
13. It is not straightforward how to find this information, which is available at: <https://www.facebook.com/ads/preferences/>. [↑](#footnote-ref-13)
14. The second group (which includes, for instance, The Guardian) will not be analysed, because it less worrying, since one is likely to expect to be tracked by websites and apps with which one has interacted. [↑](#footnote-ref-14)
15. <https://www.facebook.com/about/basics/facebook-and-advertising/on-facebook/>. [↑](#footnote-ref-15)
16. See Coutts (2016). [↑](#footnote-ref-16)
17. <https://www.facebook.com/ads/preferences/>. [↑](#footnote-ref-17)
18. Facebook declares that this author has liked a page which was connected to the Italian Social Movement, but it does not let him see the page he has supposedly liked. [↑](#footnote-ref-18)
19. There is also an ex-post mechanism. When the user views an ad, they can select “Why am I seeing this?” and they can choose to hide all ads from that advertiser. However, it is an opt-out mechanism, and the users should have right to prevent the ads from being shown, because viewing them can in itself create distress. [↑](#footnote-ref-19)
20. <https://www.facebook.com/settings/?tab=ads>. [↑](#footnote-ref-20)
21. Side note. The experiment was conducted on 11 September 2016. The day after disabling all interest-based advertising this author accessed again <https://www.facebook.com/ads/preferences/> and found that whereas the five “[a]dvertisers whose website or app you've used” had disappeared, the 11 advertisers with his contact information were still there. It is not clear on which basis they were still serving him with advertisements, if not on the basis of his supposed interests (or audiences). [↑](#footnote-ref-21)
22. As pointed out by the European Commission (2016b), para. 3.5.5.1, with reference to Liem / Petropoulos (2016), “targeted Internet advertising in theory serves a useful informational role for consumers because they are able to see the ads that are related to their potentially unique interests [ as] online platforms reduce the 'noise' of irrelevant advertising by enabling interest-based advertising that is based on users’ personal data and demographic characteristics”. [↑](#footnote-ref-22)
23. See, e.g., Turow et al. (2009), 1-27; Marshall (2014). [↑](#footnote-ref-23)
24. Ask Your Target Market (2011). [↑](#footnote-ref-24)
25. Purcell et al. (2012), 1-42. [↑](#footnote-ref-25)
26. Ibid. [↑](#footnote-ref-26)
27. Iveson (2016), who further observes “[t]his data could potentially be sold to third parties with an interest in targeted advertising”. The Pokémon Go Privacy Policy, last updated on 1 July 2016, available at: <https://www.nianticlabs.com/privacy/pokemongo/en/>, is not clear about targeted advertising. It merely reads that “[s]ome third party services providers that we engage (including third party advertisers) may also place their own Cookies on your hard drive”. Moreover, “we may use Web Beacons to deliver or communicate with Cookies, to track and measure the performance of our Services, to monitor how many visitors view our Services, and to monitor the effectiveness of our advertising”. Clearer on this point is the Pokémon Privacy Policy, last updated on 19 April 2016, available at: <http://www.pokemon.com/uk/privacy-policy/>: “[w]e may collect and store your device's source IP address which may disclose the location of your device at the time you access the Services. Advertisements and certain content could be directed to you as a result of this data. In addition, in some cases the Services can deliver content based on your current location if you choose to enable that feature”. It is also clarified that location data will be used to “[p]ersonalize the advertising you receive, including advertising based on your activity on our Sites or activity on third party sites and applications”. It should be noted that Niantic, the owner of Pokémon Go, and Nintendo, the owner of Pokémon, developed the former in partnership. It is not clear whether the two companies may share the users’ data. Moreover, Niantic spun out of Google in 2015, but it would be unsurprising if the former was indirectly controlled or at least influenced by the latter, given the generous financial support provided by Google and given that Niantic was born as a start-up within Google. [↑](#footnote-ref-27)
28. Information Commissioner’s Office (2011). The ICO distinguishes between non-targeted advertising, contextual advertising, and behavioural advertising. Even though contextual advertising could be considered to some extent, targeted, behavioural advertising will be the main focus of this paper. [↑](#footnote-ref-28)
29. Cross-device tracking is crucial in an Internet of Things world. Consider, for instance, the use of high-frequency sounds to covertly track across a range of devices. Below, the chapter will give account of a Google privacy policy update that enables users to be tracked across devices (and services) via “My Account”. In the field of advertising (especially mobile advertising), companies such as Rocket Fuel are developing solutions of cross-device optimisation (“Moment Scoring”). [↑](#footnote-ref-29)
30. Cf. Zuiderveen Borgesius (2016), 256. [↑](#footnote-ref-30)
31. The relevance of targeted advertising for intellectual property is multifaceted. For instance, alongside the data themselves as assets (which can be transferred from the data subjects to the data controllers and to third parties), the algorithms used to analyse the users’ behaviour are usually covered by trade secrets or related tools. On the problem of accountability in machine learning algorithmic decisions see Reed, Kennedy, and Nogueira Silva (2016). [↑](#footnote-ref-31)
32. **Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions “A Digital Single Market Strategy for Europe”,** COM/2015/192 final. [↑](#footnote-ref-32)
33. **Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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), OJ [2016] L 119/1.** [↑](#footnote-ref-33)
34. **GDPR, Article 20 (1).** [↑](#footnote-ref-34)
35. **GDPR, Article 20(1).** [↑](#footnote-ref-35)
36. **Regulation (EU) 2017/1128 of the European Parliament and of the Council of 14 June 2017 on cross-border portability of online content services in the internal market, OJ [2017] L 168/1.** [↑](#footnote-ref-36)
37. **Regulation (EU) 2017/1128 of the European Parliament and of the Council of 14 June 2017 on cross-border portability of online content services in the internal market, OJ [2017] L 168/1, Article** 8(2). [↑](#footnote-ref-37)
38. **On data licensing, cf. Kilian (2012), 169 and Joung et al. (2005). One should recognise, however, that “as any violation of data subject’s personality rights are very context-sensitive, there remains a Damoclean threat to the validity of such contracts on data (‘data licences’) thus turning them into an imperilled high-risk transaction.” (Sattler (forthcoming)).** [↑](#footnote-ref-38)
39. **Proposal for a Regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union, COM/2017/0495 final - 2017/0228 (COD).** [↑](#footnote-ref-39)
40. **Proposal for a Regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union**, recital 2. [↑](#footnote-ref-40)
41. European Commission (2016b), para. 3.4.4. [↑](#footnote-ref-41)
42. Article 29 Working Party (2010). The Article 29 Working Party has been replaced by the European Data Protection Board (Article 68 of the General Data Protection Regulation). [↑](#footnote-ref-42)
43. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ [1995] L 281/31. [↑](#footnote-ref-43)
44. See, e.g., John Lewis v. Roddy Mansfield, unpublished, analysed by Groom (2014). [↑](#footnote-ref-44)
45. Vidal-Hall & Ors v. Google Inc [2014] EWHC 13 (QB) (2014); Google Inc v. Vidal-Hall & Ors [2015] EWCA Civ 311 (2015). On 30 June 2016, Google withdrew its appeal from the Supreme Court. See, for instance, Evans (2015) 80; Chamberlain (2015) 93; Flint (2016) 38. [↑](#footnote-ref-45)
46. Automated decisions do not always work. For instance, on 29 August 2016, Facebook blocked the accounts of many LGBT advocates because their posts had been judged … homophobic. [↑](#footnote-ref-46)
47. **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), OJ [2002] L 201/37. [↑](#footnote-ref-47)
48. Article 29 Working Party (2010). [↑](#footnote-ref-48)
49. The text is available at: <https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/090000168007b0d8>. [↑](#footnote-ref-49)
50. See Commission of the European Communities (1995). [↑](#footnote-ref-50)
51. Ibid., para. 3.1. [↑](#footnote-ref-51)
52. The original text of 1957 is available at: <http://www.ab.gov.tr/files/ardb/evt/1_avrupa_birligi/1_3_antlasmalar/1_3_1_kurucu_antlasmalar/1957_treaty_establishing_eec.pdf>. [↑](#footnote-ref-52)
53. **Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive), OJ [2010] L95.** [↑](#footnote-ref-53)
54. For instance, Germany, Italy, and the UK. See the full list of signatories available at: <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/132/signatures?p_auth=DyuOx8C9>. [↑](#footnote-ref-54)
55. **Proposal for a Directive of the European Parliament and of the Council amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services in view of changing market realities,** COM/2016/0287 final - 2016/0151 (COD). [↑](#footnote-ref-55)
56. PwC (2015), as cited by the European Commission (2016d), para. 56. [↑](#footnote-ref-56)
57. European Commission (2016b), para. 3.3.4.7 refers to Eggers / Hamill / Ali (2013), 19. [↑](#footnote-ref-57)
58. Ibid., with reference to Martens (2016).   [↑](#footnote-ref-58)
59. On 6 May 2015, the Commission adopted the Digital Single Market (DSM) Strategy, which announced that, following the adoption of the General Data Protection Regulation, the ePrivacy rules would also be reviewed. Therefore, on 11 April 2016, the European Commission 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 closed on 5 July 2016. [↑](#footnote-ref-59)
60. European Commission (2016a). The full report can be found at <https://ec.europa.eu/digital-single-market/en/news/full-report-public-consultation-eprivacy-directive>. [↑](#footnote-ref-60)
61. Consequently, this author could not access all the services he had registered with through the Facebook login, such as Spotify and Academia.edu. [↑](#footnote-ref-61)
62. 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 - 2017/03 (COD), 10 January 2017 (hereinafter draft ePrivacy Regulation). [↑](#footnote-ref-62)
63. Presidency of the Council of the European Union, note n. 11995/17, 2017/0003 (COD), 8 September 2017. [↑](#footnote-ref-63)
64. Ibid., Art. 10(2a). [↑](#footnote-ref-64)
65. 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. [↑](#footnote-ref-65)
66. European Parliament (n 15) para. I (see also ibid para 20). [↑](#footnote-ref-66)
67. Different rules apply to sensitive data, e.g. health and sex data. Indeed, the only available legal ground

    for processing the data is explicit, separate prior opt-in consent (no opt-out, no browser settings). [↑](#footnote-ref-67)
68. 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. [↑](#footnote-ref-68)
69. 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. [↑](#footnote-ref-69)
70. Cf. Hoofnagle et al. (2012), 273. [↑](#footnote-ref-70)
71. 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, OJ [2009] L 337/11. [↑](#footnote-ref-71)
72. Cf. Neelam et al. (2015), 51; Kerr et al. (2005), 647. [↑](#footnote-ref-72)
73. Noto La Diega (2016a) suggests a practical tool to overcome the opaqueness of the legals: the “awareness by design” app. [↑](#footnote-ref-73)
74. 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 clause, “let alone appreciated its purport or implications, and it would have been quite irrational for the claimant to assume that he had" (Judgment at para. 19). [↑](#footnote-ref-74)
75. The Court applied the Unfair Terms in Consumer Contracts Regulations 1999, which has now been substituted by the Consumer Rights Act 2015. [↑](#footnote-ref-75)
76. See Ayenson et al. (2011), 1. [↑](#footnote-ref-76)
77. Ibid, 14. HTML5 may be used as well to enhance privacy. [↑](#footnote-ref-77)
78. European Data Protection Supervisor (2011a). For the full speech, see Hustinx (2011). [↑](#footnote-ref-78)
79. European Advertising Standards Alliance and Interactive Advertising Bureau. [↑](#footnote-ref-79)
80. European Advertising Standards Alliance (2011). [↑](#footnote-ref-80)
81. Interactive Advertising Bureau (2011). [↑](#footnote-ref-81)
82. The reference is to the Network Advertising Initiative’s (NAI) self-regulatory framework. In 2013, the NAI substituted the framework with a code of conduct update by NAI (2015a). Cf. also NAI (2015b) and Federal Trade Commission (2009). 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 (§II.C.1 of NAI (2015a)), 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. [↑](#footnote-ref-82)
83. The national implementations of the said regulations will not be analysed. See, for example, Istituto di Autodisciplina Pubblicitaria (IAP) (2015), for the Italian regulation. Complaints can be filed online with the Comitato di Controllo IAP, which double-checks compliance with the EASA/IAB self-regulations. If necessary, the IAP applies the EASA Cross Border Complaints system. [↑](#footnote-ref-83)
84. Given that the Internet operates outside a precise physical location it is hard to enforce the laws and it is often unclear which national or regional institution should govern and regulate the relevant activities. Therefore, self-regulatory initiative, by being independent from geographical boundaries and by virtue of peer-pressure mechanisms, can be more effective. [↑](#footnote-ref-84)
85. It should be noted that EASA interprets Kroes’s pillars differently, referring to them as “transparency, choice and control” (available at: <http://www.easa-alliance.org/issues/oba>). [↑](#footnote-ref-85)
86. Kroes (2010). [↑](#footnote-ref-86)
87. Ibid. [↑](#footnote-ref-87)
88. The regulation of the content of online advertisements and the advertisement delivery are out of the scope of the Framework. [↑](#footnote-ref-88)
89. 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”. [↑](#footnote-ref-89)
90. 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 of 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 statement that the company adheres to these principles; and (f) A link to [www.youronlinechoices.eu](http://www.youronlinechoices.eu), a consumer-focussed website and education portal. [↑](#footnote-ref-90)
91. 28 companies were “experiencing technical issues, and […] cannot retrieve your status” (Google and Facebook were among them), and 18 companies had “not set-up a cookie, but may deliver in the future advertisements that are customised to your interests”. No results were displayed for the remaining 60 companies. [↑](#footnote-ref-91)
92. This author tried to retrieve his status with regards to Google until 16:43 GMT of the same day. [↑](#footnote-ref-92)
93. http://www.easa-alliance.org/issues/oba. [↑](#footnote-ref-93)
94. European Advertising Standards Alliance (2011), Principle II.A. [↑](#footnote-ref-94)
95. Ibid., 27. [↑](#footnote-ref-95)
96. Practically, if this author represented as legal counsel a customer wanting to file a complaint in this case, pragmatically he would file it against both Facebook Ireland Limited and SFO84, Inc. (the owner of Mrb&b). However, it is plausible that the real defendant be the former, since it has the control over its users’ data. If one reads European Commission, Case No. M.7217 – Facebook/ WhatsApp, 3 October 2014, para 70, on the Facebook – WhatsApp merger, they will notice that, for the purpose of its online advertising activities, “Facebook collects data regarding the users of its social networking platform and analyses them in order to serve advertisements on behalf of advertisers, which are as much as possible "targeted" at each particular user of its social networking platform. However, Facebook does neither sell any of the user data it collects nor provides data analytics services to advertisers or other third parties as a stand-alone product separate from the advertising space itself”. This means that SFO84, Inc. does not have access to Facebook users’ data and, therefore, it could not be considered liable for any illegal use of them. [↑](#footnote-ref-96)
97. The form to fill in is available at: <http://www.iap.it/le-attivita/per-i-cittadini/pubblicita-comportamentale-online/>. [↑](#footnote-ref-97)
98. Reviewing European Advertising Standards Alliance (2015a), one can notice that 100% of the reported complaints falling under the category “privacy and data protection” are about OBA. The other categories are misleading advertising, social responsibility, taste and decency. Of the 26 total complaints, six were about “privacy and data protection”, and hence about OBA. Therefore, OBA complaints amount to more than 23% of the total. [↑](#footnote-ref-98)
99. One has to look at the country where the medium carrying the advertisement is based; in the case of direct mail and digital marketing communications, the country where the advertiser is based; and in the case of OBA, the country where the principal decision-maker is established. See European Advertising Standards Alliance (2014), II. [↑](#footnote-ref-99)
100. The self-regulation authorities and organisations (and this is the case with the IAP) usually invite the user to contact directly the interested company before filing a complaint. [↑](#footnote-ref-100)
101. The Comitato di Controllo can refer to the Giurì cases of noncompliance with the Codice di Autodisciplina della Comunicazione Commerciale (Advertising Self-Regulation Code, updated on 22 March 2016). It can exert moral suasion, by inviting the advertising companies to edit the advertisement or the accompanying information. It can also issue injunctions to oblige the company to desist and to comply with the Codice (ingiunzione di desistenza). Injunctions can be issued by the Giurì as well, should the Comitato refer to it or should an *istanza* be filed. The user can complain informally to the Comitato (*segnalazione*) and formally to the Giurì (*istanza*). [↑](#footnote-ref-101)
102. Industry referral would lead to other sanctions, such as loss of the right to use the B2B seal. [↑](#footnote-ref-102)
103. International Chamber of Commerce (2011). [↑](#footnote-ref-103)
104. Art. D7.1 of the ICC Code of Conduct. [↑](#footnote-ref-104)
105. Ibid., italics added. [↑](#footnote-ref-105)
106. Art. D7.2 of the ICC Code of Conduct. [↑](#footnote-ref-106)
107. Art. D7 of the ICC Code of Conduct. [↑](#footnote-ref-107)
108. This is the main conclusion of Article 29 Working Party (2011). [↑](#footnote-ref-108)
109. Ibid. [↑](#footnote-ref-109)
110. In the previous report, European Advertising Standards Alliance (2015b), 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. [↑](#footnote-ref-110)
111. European Advertising Standards Alliance (2015a). [↑](#footnote-ref-111)
112. 2914-5 Rubicon Project; 2916-7 AudienceScience; 2922-3 Xaxis, 2920-1 Infectious Media, 2918-9 Captify. The Advertising Standards Authority upheld the complaints. [↑](#footnote-ref-112)
113. 2969 Eyeota Ltd. The Deutsche Datenschutzrat Online-Werbung decided that the problem lay with the complainant: their technical device, privacy setting or Internet connection. [↑](#footnote-ref-113)
114. 1 in 4 surveyed users in European Interactive Digital Advertising Alliance and TRUSTe (2015) have engaged with the OBA icon. [↑](#footnote-ref-114)
115. A one-day survey of some of this author’s Facebook friends was conducted on 21 August 2016. Their age range was 18-40 with a majority of people in their early thirties. Apart from the 18-year-old user and a user who did not attend any university, the rest of them had (at least) a master’s degree (20 of which with a law background), whilst 7 users had completed a Ph.D. (two of them were professors). [↑](#footnote-ref-115)
116. Tarabella (2013). [↑](#footnote-ref-116)
117. Reding (2013). [↑](#footnote-ref-117)
118. Ibid. [↑](#footnote-ref-118)
119. For a history of the law-making process see de Hert / Papakonstantinou (2016), 181. [↑](#footnote-ref-119)
120. European Data Protection Supervisor (2011b), para 14. This opinion elaborated on Article 29 Working Party and Working Party on Police and Justice (2009), a milestone in the review process that led to the adoption of the General Data Protection Regulation. However, the contribution was limited to the observation that, “in specific cases, specific legislative measures embedding the concept of ‘privacy by design’” (para 56) should be adopted. This was deemed to be the case with RFID technology, social networks, and behavioural advertising. It was also said that, given that the duty to inform the data subject is not always properly put into practice, a new legal framework should provide alternative solutions, in order to enhance transparency. For instance, “new ways to inform data subjects could be developed in relation to behavioural advertising” (para 63). [↑](#footnote-ref-120)
121. Ibid., para 94. [↑](#footnote-ref-121)
122. Ibid., para 162. [↑](#footnote-ref-122)
123. The reference is to the “Phorm” case. The Commission launched legal action against the UK on 14 April 2009; the case entered its second phase on 29 October 2009. On 30 September 2010, the European Commission decided to refer the UK to the Court of Justice, but the former decided to close the case after the UK amended its national legislation so as not to allow interception of users' electronic communications without their explicit consent, and established an additional sanction and supervisory mechanism to deal with breaches of confidentiality in electronic communications. In particular, the Regulation of Investigatory Powers Act 2000 (RIPA) was amended to remove references to implied consent and to establish a new sanction against unlawful interception, which previously fell outside the scope of RIPA. On the Phorm case see Bernal (2012); Bray / Griffiths (2008), 24; Linkomies (2008), 12; Graham / Anderson (2008), 10. [↑](#footnote-ref-123)
124. European Data Protection Supervisor (2010), para 96. [↑](#footnote-ref-124)
125. Ibid., § 116(c). [↑](#footnote-ref-125)
126. Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM(2012) 11 final — 2012/011 (COD). [↑](#footnote-ref-126)
127. European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 - C7-0025/2012 - 2012/0011(COD)). [↑](#footnote-ref-127)
128. Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) - Preparation of a general approach, 9565/15. [↑](#footnote-ref-128)
129. **Opinion of the European Economic and Social Committee on the ‘Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)’ COM (2012) 11 final — 2012/011 (COD),** § 1.10. [↑](#footnote-ref-129)
130. However, national lawmakers, regulators and judges may clarify this aspect. For instance, Information Commissioner’s Office (2016), 23, points out that “You must deal with an objection to processing for direct marketing at any time and free of charge”. [↑](#footnote-ref-130)
131. See art. 6(4) GDPR on the scenarios where processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent. [↑](#footnote-ref-131)
132. GDPR, Article 21(5). [↑](#footnote-ref-132)
133. According to European Commission (2016b), 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”. [↑](#footnote-ref-133)
134. See, for instance, BioPay biometric payments system to verify the age of customers of retail shops. According to Woodward (2000), however, “there are no age verification biometrics”. [↑](#footnote-ref-134)
135. The “legitimate interest” justification for processing cannot be used, however, to violate the data subject’s fundamental rights, including data protection and privacy. Indeed, the legitimate interest goes with the proviso that “the interests or the fundamental rights and freedoms of the data subject are not overriding” (recital 47, see also art. 6(1)f). On data protection and privacy as fundamental rights see, for instance, arts. 7-8 of the Charter of Fundamental Rights of the European Union, Article 16(1) TFEU, art. 8 ECHR, art. 1(2) GDPR, art. 1(1) Data Protection Directive. In the case law, ECJ, Case C‑553/07, *College van burgemeester en wethouders van Rotterdam v M. E. E. Rijkeboer*, 7 May 2009, ECLI:EU:C:2009:293, para. 47; ECJ, Case C-293/12 and C-594/12, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Ireland and the Attorney General, and Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and Others,* 8 April 2014, ECLI:EU:C:2014:238, para. 53. As reminded, for instance, in ECJ, Case C-362/14, *Maximillian Schrems v Data Protection Commissioner,* 6 October 2015, ECLI:EU:C:2015:650 para. 38 “the provisions of Directive 95/46, inasmuch as they govern the processing of personal data liable to infringe fundamental freedoms, in particular the right to respect for private life, must necessarily be interpreted in the light of the fundamental rights guaranteed by the Charter”. [↑](#footnote-ref-135)
136. On some other aspects see Bauer / **Eickmeier (2016).** [↑](#footnote-ref-136)
137. European Commission (2016c), 148-149. [↑](#footnote-ref-137)
138. This was the statement of Ernie Cormier, then president and CEO of Nexage, to Rowinski (2011). In the meantime, Nexage has been acquired by Millennial Media for USD 108 million. Millennial Media has recently been bought by AOL for USD 238 million. [↑](#footnote-ref-138)
139. Ayenson et al. (2011), 1. [↑](#footnote-ref-139)
140. See the summary of the relevant statistics, available at: <http://www.statista.com/statistics/266249/advertising-revenue-of-google/>. [↑](#footnote-ref-140)
141. Comparing 2015 and 2016, there has been an increase of 18% (<https://abc.xyz/investor/news/earnings/2016/Q3_alphabet_earnings/>). [↑](#footnote-ref-141)
142. This author has listened to his own recorded voice by visiting <https://myactivity.google.com/myactivity?restrict=vaa&utm_source=help> and it is noteworthy that Google recorded his voice several times without him having actually uttered the words “OK Google”. [↑](#footnote-ref-142)
143. On the one hand, the interaction between the devices creates highly valuable and potentially personal big data; on the other hand, the devices are increasingly equipped with sensors capable of collecting new types of data. This is confirmed by Google’s Advertising page (https://www.google.it/intl/en-GB/policies/technologies/ads/): “[w]e may also select advertising based on information about your computer or device, such as your device model, browser type or sensors in your device like the accelerometer”. [↑](#footnote-ref-143)
144. European Commission (2016b). [↑](#footnote-ref-144)
145. In 2014, for instance, Google spent approximately USD 11 billion on real estate purchases, production equipment, and data centre construction and USD 10.5 billion on R&D. [↑](#footnote-ref-145)
146. European Commission (2016b), § 3.3.3.1. [↑](#footnote-ref-146)
147. ECJ, Case C-131/12*, Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, date of the judgment, ECLI:EU:C:2014:317, para. 56. [↑](#footnote-ref-147)
148. About Google Ads, available at: <https://support.google.com/adsense/troubleshooter/1631343>. [↑](#footnote-ref-148)
149. <https://www.google.com/settings/u/0/ads/authenticated>. [↑](#footnote-ref-149)
150. This cannot be inferred from the ads setting page, but it can be from the bottom of the DoubleClick cookies page. More transparency would be preferable. [↑](#footnote-ref-150)
151. Caddy (2015). [↑](#footnote-ref-151)
152. FORBES® Website Terms of Service, Revised and posted as of 5 November 2015, emphasis added, available at: <http://www.forbes.com/terms>. [↑](#footnote-ref-152)
153. This is what a source close to Facebook told Constine (2016). [↑](#footnote-ref-153)
154. This phenomenon can be called ‘legal hysteresis’ (Noto La Diega (2016b)). [↑](#footnote-ref-154)
155. # AdSense is an advertising placement service whereby website publishers earn money by displaying targeted Google ads on their websites. In turn, a business can advertise itself by using AdWords. The present analysis will focus on AdSense. However, one should be aware that Google also provides AdWords, Google Analytics and a range of DoubleClick-branded services.

     [↑](#footnote-ref-155)
156. # AdSense programme policies, last updated on 21 June 2016, available at: <https://support.google.com/adsense/answer/48182?utm_source=aso&utm_medium=link&utm_campaign=ww-ww-et-asfe_&hl=en-GB>.

     [↑](#footnote-ref-156)
157. DoubleClick cookies, available at: <https://support.google.com/adsense/answer/2839090>. [↑](#footnote-ref-157)
158. Ibid. [↑](#footnote-ref-158)
159. On 12 August 2016, this author tried to access his Gmail account and was redirected to the page where cookies can be turned on (<https://support.google.com/accounts/answer/61416?hl=en>). [↑](#footnote-ref-159)
160. As seen above, there are some actions for which informed consent is required (e.g. under Article 5(3) of the ePrivacy Directive). [↑](#footnote-ref-160)
161. <https://www.google.com/about/company/user-consent-policy.html>. [↑](#footnote-ref-161)
162. AdSense programme policies, which refer to a separate document named ‘Best practices to avoid sending Personally Identifiable Information’. It is intended to provide guidance for complying with the Identifying Users Policy. See <https://support.google.com/adsense/answer/6156630?ref_topic=6162392&rd=1>. [↑](#footnote-ref-162)
163. For a privacy-preserving tool see Pang et al. (2015), 1-8. [↑](#footnote-ref-163)
164. Cranor (2012), 93. [↑](#footnote-ref-164)
165. Google AdSense Online Terms of Service, available at: <https://www.google.com/adsense/localized-terms?hl=en_GB>. The contract between Google and the publishers is composed of (at least) three documents: the Google AdSense Online Terms of Service, the AdSense Programme Policies, and theGoogle Branding Guidelines. The AdSense programme policies are complemented by the EU consent policy, Deductions from Earnings FAQs, the Webmaster quality guidelines, the Ad implementation policies, the Content policies, the Product-specific policies and the Guidance for complying with the Identifying User Policy. Some of these policies are further fragmented. For instance, the Product-specific policies are divided into Behavioural policies, AdSense for video and games policies and AdSense for Search (AFS) policies. See also the Custom Search Engine Terms of Service. [↑](#footnote-ref-165)
166. Privacy Policy, last updated on 26 June 2016, available at: <https://www.google.it/intl/en-GB/policies/privacy/>. [↑](#footnote-ref-166)
167. There are specific privacy policies concerning Chrome and Chrome OS, Play Books, Payments, Fiber, Project Fi, and Google Apps Education Edition. [↑](#footnote-ref-167)
168. Google privacy policy, last updated on 29 August 2016, available at: <https://www.google.com/policies/privacy/>. [↑](#footnote-ref-168)
169. On 12 August 2016, this author googled ‘kidney disease’ and Adblock Plus blocked two relevant advertisements. Generally speaking, however, the protection afforded to sensitive personal data is high. See the experiment presented above in section 3. [↑](#footnote-ref-169)
170. Google privacy policy. [↑](#footnote-ref-170)
171. Ibid. [↑](#footnote-ref-171)
172. How Google uses data when you use our partners' sites or apps, available at: <https://www.google.it/intl/en-GB/policies/privacy/partners/>. [↑](#footnote-ref-172)
173. The notice is still available at: <https://accounts.google.com/signin/newfeatures?cbstate=1&cbflow=promo-2-EN>. [↑](#footnote-ref-173)
174. It is interesting that, with regard to the change concerning Chrome, Google points out that “[i]f you don't want to personalize your Google products, you can still use Google's cloud to store and sync your Chrome data without letting Google read any of your data. To add an additional layer of encryption, set up a sync passphrase” (<https://support.google.com/chrome/answer/165139?p=personalization&visit_id=1-636098212979690973-579754209&rd=1#personalization>). [↑](#footnote-ref-174)
175. For instance, if a third-party app uses one of Google’s services, say, Analytics, the app will send Google information about the user’s behaviour, including “the name of the app and an identifier that helps us to determine which ads we've served to other apps on your device”. [↑](#footnote-ref-175)
176. Using “My Account” Google is actually overcoming the fragmentation of the Internet of Things by easily recombining data from multiple devices to identify a single user regardless of the point of access. [↑](#footnote-ref-176)
177. The European regulation of competition in the field of advertising still defines targeted advertising as advertising targeted to a specific Member State, not the kind that singles out a user usually based on his or her behaviour. For instance, the ECJ stated that social, linguistic and cultural features specific to a given Member State, may cause consumers in that Member State to have a different interpretation of a product description used in commercial practice (ECJ, Case C-220/98, *Estée Lauder Cosmetics GmbH & Co. OHG v. Lancaster Group GmbH*, 13 January 2000, ECLI:EU:C:2000:8, para. 29). On 25 May 2016, the Commission adopted an updated version of the 2009 Guidance on the application of the Unfair Commercial Practices Directive. This seems to allow an extension to the new definition of 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” (European Commission (2016c), 45). [↑](#footnote-ref-177)
178. Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council (‘Unfair Commercial Practices Directive’), OJ [2005] L 149. The Unfair Commercial Practices Directive is complemented, as regards business-to-business relations, by the Misleading and Comparative Advertising Directive. [↑](#footnote-ref-178)
179. European Commission (2016c), 148. [↑](#footnote-ref-179)
180. For a clear explanation of the functioning of the system with regard to the average consumer in the UK, see Department of Business Innovation & Skills (2014), para. 26 ff. [↑](#footnote-ref-180)
181. The two main categories of unfair commercial practices are misleading practices and aggressive practices. 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”. [↑](#footnote-ref-181)
182. Gebicka / Heinemann (2014), 165. However, as correctly pointed out by Surblytė (2015), 174, “although data could be considered the ‘currency’ of the Digital Economy in very general terms, it cannot precisely be equalled to the concept of a ‘price”. [↑](#footnote-ref-182)
183. General Court, H. Lundbeck A/S and Lundbeck Ltd v. European Commission, T-472/13, ECLI:EU:T:2016:449. 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 were "a restriction of competition by object". The examples of use of competition law to limit IPRs are myriad, but the classic example is exhaustion. [↑](#footnote-ref-183)
184. As noted by Surblytė (2015), 174, the quantity of data can become quality insofar as “the volume of data counts when it comes to the quality of search results, which may improve based on the economies of scale”. [↑](#footnote-ref-184)
185. See the summary of the relevant statistics at: <http://www.statista.com/statistics/234056/facebooks-average-advertising-revenue-per-user/>. [↑](#footnote-ref-185)
186. European Commission, Case M.7217 – Facebook/ WhatsApp, 3 October 2014. [↑](#footnote-ref-186)
187. The decision refers mainly to ‘online advertising’ in general, but given that the company involved carries out mainly targeted advertising, the author believes that the Commission’s 2014 decision constitute a good prism through which to observe the competition implications of targeted advertising. [↑](#footnote-ref-187)
188. <https://www.whatsapp.com/legal/#key-updates>. [↑](#footnote-ref-188)
189. European Commission, Case M.7217 – Facebook/ WhatsApp, 3 October 2014, para. 102. [↑](#footnote-ref-189)
190. <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 former version of the terms, no reference was made to advertising (be it that of Facebook or of WhatsApp). In the previous privacy notice, in turn, it was stated: “[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 advertisements into the product, but if we ever do, we will update this section”. [↑](#footnote-ref-190)
191. This pre-ticked box appeared on the screen of this author’s phone on 26 August 2016 at 8:51 GMT. [↑](#footnote-ref-191)
192. Cf. Lomas (2016). [↑](#footnote-ref-192)
193. European Commission, Case M.7217 – Facebook/ WhatsApp, 3 October 2014, paras 106-107. [↑](#footnote-ref-193)
194. Ibid., fn 42. [↑](#footnote-ref-194)
195. Tarabella (2013). [↑](#footnote-ref-195)
196. See the section on “Rights”, § 2 of Instagram Terms of Use, effective as of 19 January 2013, available at: https://help.instagram.com/478745558852511: “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”. [↑](#footnote-ref-196)
197. Facebooks owns Instagram, WhatsApp, PrivateCore, and Oculus VR. [↑](#footnote-ref-197)
198. European Commission, Case M.5727 – Microsoft / Yahoo! Search Business, 18 February 2010, para. 61; European Commission, Case M. 4731 – Google / DoubleClick, 11 March 2008, paras 45-46; 56. [↑](#footnote-ref-198)
199. European Commission, Case M.7217 – Facebook/ WhatsApp, 3 October 2014, para. 76. [↑](#footnote-ref-199)
200. Ibid., para. 77. [↑](#footnote-ref-200)
201. Another question which has been left open regards a possible distinction between online advertising on different platforms (essentially on computers or on mobile devices). [↑](#footnote-ref-201)
202. European Commission, Case M.7217 – Facebook/ WhatsApp,3 October 2014, para. 79. [↑](#footnote-ref-202)
203. 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. [↑](#footnote-ref-203)
204. European Commission, Case M.7217 – Facebook/ WhatsApp, 3 October 2014, para. 83. [↑](#footnote-ref-204)
205. “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” (European Commission, Case M.7217 – Facebook/ WhatsApp, 3 October 2014, para. 164). [↑](#footnote-ref-205)
206. Ibid., para. 166. [↑](#footnote-ref-206)
207. Ibid., para. 181. [↑](#footnote-ref-207)
208. Ibid., para. 182. [↑](#footnote-ref-208)
209. http://blog.whatsapp.com/529/Setting-the-record-straight. [↑](#footnote-ref-209)
210. European Commission, Case M.7217 – Facebook/ WhatsApp, 3 October 2014, para. 185. [↑](#footnote-ref-210)
211. White / Levring (2016). [↑](#footnote-ref-211)
212. Ibid. [↑](#footnote-ref-212)
213. Especially when we try to ignore the ads, the effects of 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, regardless of its intrinsic characteristics. According to Dempsey / Mitchell (2010), 622, this “can occur even when consumers have both the motivation and the opportunity to retrieve product attribute information from memory”. [↑](#footnote-ref-213)
214. The problem is not limited to targeted advertising, but 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 Michael (2016), 20, “We are losing our ability to make decisions for ourselves, to make a choice based on our preferences, not imposed by computer systems.”. [↑](#footnote-ref-214)
215. Cf. Merikle (2000), 497. [↑](#footnote-ref-215)
216. With regard to other topics, a similar conclusion is proposed by Mik (2016). [↑](#footnote-ref-216)
217. One may object to this proposal becaure data do not fall easily under the traditional IP categories (copyright, designs, patents, trademarks). However, many developments show how the IP paradigm is evolving, becoming simpler and more comprehensive. For instance, in the UK, trade secrets are protected through the breach-of-confidence rule, usually in combination with contract law. The *Vidal-Hall v Google* case is a reminder of how hard it is to draw a clear line between data protection, breach of confidence, and misuse of private information (the first and the last are torts, while with the second it is not entirely clear whether it has its roots in contract, property, tort, or equity, or is a *sui generis* action). Moreover, the Intellectual Property Office (2016) 18 has shown that the most popular means to protect immaterial assets in the UK is the confidentiality agreement, which does not really fit in any traditional IP category. [↑](#footnote-ref-217)
218. Nonetheless, see the concerns expressed by Drexl et al. (2016) as to creation of new exclusive rights in data “which could even hamper the functioning of the data-driven economy”. The authors’ concerns, however, are mainly due to the fact that intellectual property of data is seen only from the perspective of those who commercially exploit the users’ data. This chapter’s stance takes the viewpoint of users and it would like to entrust them with the ownership of data. It is believed that data are already de facto treated as digital assets: the main aim of the proposal is to broaden the audience of data owners to include their subjects. [↑](#footnote-ref-218)
219. Cf. Reed (2016) and his proposal of a new concept of legitimacy. [↑](#footnote-ref-219)
220. The characteristics of online advertising make the “change the channel” remedy often unviable. [↑](#footnote-ref-220)
221. Users should be made aware, for instance, that the opt out from interest-based advertising might still allow some form of OBA. [↑](#footnote-ref-221)
222. Including, for instance, when and where they have consented, which data were used to serve it, etc. [↑](#footnote-ref-222)
223. Gamifying privacy seems pivotal to making users take privacy seriously. Indeed, given the tendency not to read the privacy policies, gamification can lead to increased interactivity and thus alertness. See, for instance, Centre for Democracy and Technology ‘The Gamification of Privacy’ (2011), <https://cdt.org/blog/the-gamification-of-privacy/>. Some authors distinguish between serious games and gamified interactions (Rottondi and Verticale (2017), 14221). The former refers to games designed for purposes others than entertainment, the latter to “the use of game design elements in non-game contexts”. In this paper, it is believed that using game design elements in the drafting and presentation of privacv policies can be a good way to increase the users’ awareness thus making it more likely that they will have privacy-preserving behaviours. Unlike Rottondi and Verticale (2017), 14221, this chapter is more concerned with the use of games to protect privacy, rather than with the privacy risks of online gaming. [↑](#footnote-ref-223)
224. 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. See the recently amended Article L. 111-7(II) of the *Code de la consommation*,which provides that “Tout opérateur de plateforme en ligne est tenu de délivrer au consommateur une information loyale, claire et transparente,” [↑](#footnote-ref-224)
225. 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. The concept of “awareness by design” was introduced in Noto La Diega (2016a), 24, where it is defined broadly as “the use of technologies (especially design) to empower the user and make them aware of risks, rights, and obligations”. [↑](#footnote-ref-225)
226. 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. [↑](#footnote-ref-226)
227. More generally, as observed by Hoofnagle et al. (2012), 273, “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”. [↑](#footnote-ref-227)
228. There is a number of cons. One of them is social network homophily, that is, the fact that we listen and speak only to the like-minded while online, with the risks of “excessive confidence, extremism, contempt for others, and sometimes even violence” (Sunstein (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 appears (Pariser (2011)). Bakshy et al. (2015), 1-4, have presented evidence that people are exposed to a substantial amount of content from friends with opposing viewpoints. [↑](#footnote-ref-228)
229. This solution empowers the user, whereas most solutions focus on the role of the public institutions and on regulation. Along those lines, for instance, see Klein (2016), 19, according to whom, given that corporations have no 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”. The premise is acceptable, less so the top-down solution. [↑](#footnote-ref-229)
230. Pittman (2016). [↑](#footnote-ref-230)
231. Ibid. [↑](#footnote-ref-231)