



[Global Advertising Lawyers Alliance](#)

2013 ANA Advertising Law & Public Policy Conference

The exciting potential of R(eal) T(ime) M(arke)ting and other new tools that use computer algorithms: just don't forget about some legal implications.

By Keri S. Bruceⁱ and Felix Hoferⁱⁱ

Recently we found ourselves debating the explosive attention marketers and related businesses have dedicated, over the last twelve months, to new techniques to target more efficiently their existing or prospective customers. Every day numerous articles discuss the rapid expansion of the use of Real Time Bidding (RTB), Real Time Marketing (RTM) or some other programmatic buying system. There are even new magazines specifically dedicated to the topic. Increasingly, similar words are coined at impressive speed according to the perspective chosen for approaching the topic.

In the end, however, all these terms and acronyms simply stand for the concept of "*delivering the right commercial communication, to the right person, at the right moment (or place) through the right device*". Nothing exactly revolutionary or new, as many advertisers have been using advertising that employs online behavioral advertising (OBA) for some time.

The key to RTB is its algorithms. These algorithms, like those that are used in financial high frequency trading, are subsets of computer programs that make calculations and process and analyze data in real time. In the context of RTB, these algorithms enable marketers to buy media automatically in real time, aggregate the results of a buy, and build on those results over time to

ⁱ Keri S. Bruce is a Senior Associate in the Advertising, Technology and Media group at Reed Smith LLP. Keri is the author of the comments on the U.S. approach and may be reached through the following contact details: Phone: 212-549-0220 and email kbruce@reedsmith.com.

ⁱⁱ Felix Hofer is a named and founding partner of the Italian law firm Studio Legale Hofer Lösch Torricelli, in Firenze (50132), via Giambologna 2/rosso; he may be reached through the following contact details: Phone +39.055.5535166 , Fax +39.055.578230 – e-mail: fhofer@hltlaw.it (personal) or info@hltlaw.it (firm e-mail). Felix has authored the comments on the European perspective.

identify connections, gain knowledge and optimize marketing plans. It is becoming a game changer for marketers. The technical progress in using very large, diverse data (often referred to as “Big Data”) to deliver commercial communication provides not just advantages, but also challenges for advertisers and media- and advertising agencies as well as search engines and Big Data companies.

On one hand, traditional media, such as radio, television, press, outdoor, and sponsored links, face tough competition from new devices (and their applications) such as smart phones and tablets, and new media platforms, such as social media. It has been reported that RTB will grow at a rate of 53% per year in the U.S. between 2011 and 2016¹ and that in 2012 RTB accounted for nearly 13 percent of all U.S. display advertising spending². According to recent studies, at the end of 2013 mobile search clicks are likely to attract approximately 20-25% of the total amount of search clicks. Not such an impressive number by itself, but up by a double digit number compared to the past year (and deemed to increase at similar speed in near future), which is very impressive!

On the other hand, new technology always goes hand-in-hand with an increased level of sophistication and a need for refined strategies: “predicting” search terms or content will soon be increasingly more important for efficient marketing in an on-line environment. Exciting times are definitely ahead for the advertising industry. But, not all that shines is necessarily made of gold.

The legal implications raised by these more advanced technologies are continuing to get lots of attention from regulators and law makers around the world. Advertisers, agencies, exchanges, publishers, search engines and the like that are taking advantage of RTB should understand the current legal landscape and properly minimize risk before diving in.

I. The United States approach

While there are a myriad of legal issues that can arise when using RTB, regulators, consumers groups and class action lawyers in the U.S. continue to be highly focused on privacy and data protection in online and mobile environments. The focus on this area is driven by many factors, including, the general anxiety consumers have about being “tracked” and wanting to ensure their personally identifiable information (“PII”) and personal and private data is kept safe and that it is not shared or used in ways that were not intended or disclosed. While anonymization and aggregation of data has provided some comfort in the past to data sharing, it’s not perfect. There are real-life examples of where anonymization of data has failed thereby allowing such information to be re-identified.³ Further, with the rapid advancement of technology, there is the possibility that re-identifying data may become easier.

While privacy and the protection of PII is already subject to a variety of U.S. laws and regulations, such as the Graham-Leach-Bliley Act (governs personal information collected by financial institutions), the Health Insurance Portability and Accountability Act (which regulates medical and health information) and numerous state laws, such as the California Online Privacy Protection Act, the online and mobile industries continue to be targeted for new legislation and regulations. In February 2013, U.S. Senator Jay Rockefeller introduced a law coined the “Do-Not-Track Online Act of 2013” which would require all web browsers, online companies, and app makers to give users a choice of opting out of being tracked online.⁴ In addition to laws and regulations directly relating to data protection in certain industries, other Federal laws come into play and have been the basis of litigation and regulatory investigations, including:

- Electronic Communications Privacy Act (ECPA), which prevents tracking and access to user behavior without consent⁵;
- Federal Wiretap Act⁶, part of the ECPA which provides for statutory damages if the contents of electronic communications are intentionally intercepted using a device;
- Stored Electronic Communications Act⁷, which provides penalties for anyone who "intentionally accesses without authorization a facility through which an electronic communication service is provided or... intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorize access to a wire or electronic communication while it is in electronic storage in such system";
- Computer Fraud and Abuse Act⁸, which is an anti-computer hacking law that prevents tracking of user behavior if it causes economic damage of \$5,000 or more;
- Section 5 of the FTC Act⁹, which prohibits deceptive acts and practices; and
- Children's Online Privacy Protection Act¹⁰, which was updated in December of 2012 to expand privacy protections for children.

In addition to data and privacy issues, anti-competition concerns can come into play. We've already seen one major investigation by the FTC into whether of a search engine's search algorithms and restrictions on use of certain data by advertisers across competitive platforms resulted in anticompetitive practices.¹¹ While anti-competitive practices in the area of RTB may not necessarily pose direct liability for advertisers and agencies, the practices can nevertheless cause harm (and frustration) to advertisers and agencies.

So, what should advertisers and agencies do to manage risk as they delve into RTB?

Disclose and Abide By Privacy Policies

Companies should ensure that they are disclosing their privacy practices and abide by them. Seems simple, but many companies haven't reviewed or updated their privacy policies since they first launched their websites years ago. It's highly likely that the technology used to collect data and their data sharing practices have evolved since that time. The Federal Trade Commission (FTC) views a company's website terms of use and privacy policy as an express representation to consumers as to how their information and data will be collected, stored and (if applicable) shared. Failure to disclose and abide by a privacy policy can expose a company to an action for unfair and deceptive acts or practices under Section 5 of the FTC Act and similar state laws and breach of contract claims. For example, in December of 2012, the FTC entered into a consent order against a large advertising network that used "history sniffing" technology to track data, including sensitive financial and medical information, about consumers on websites outside of the website's own network.¹² This practice was deceptive because the ad network's privacy policy disclosed only that it would collect information about consumers' visits to websites in its own network. Under the terms of the settlement, the ad network must cease "history sniffing" practices and delete and destroy all data collected using it. Also in December 2012, the California Attorney General sued an airline for violating the California Online Privacy Protection Act (OPPA) and the state's Unfair Competition Law by failing to conspicuously post a privacy policy on its app and failing to comply with its own website privacy policy.¹³ These cases are just two of many cases where a company's failure to abide by the terms of its privacy policy had legal implications.

Privacy policies should be robust and cover all potential data uses and transfers now and in the future so as to reduce the need to revise the policy. Policies should have an effective date or "last

revised” date, so that users can identify if and when the policy was changed. Before implementing a revision to a privacy policy, special attention should be paid to whether the change is material and whether it will have an effect on previously collected data. If, for instance, the change will increase the ways in which PII previously collected from users will be used, then express consent to the new change will likely be required before historical data can be used in the new ways. Companies should carefully consider the most effective manner of disclosing a change. For instance, the need for express consent may alter how a change is communicated to users, such as via email, on the website, during check out, etc. Perhaps more importantly, before implementing a change, companies should consider the potential consumer reactions to the change. It’s not uncommon for companies to receive backlash from consumers to proposed privacy policy revisions.¹⁴

Finally, regulators and industry organizations are also currently focusing heavily on the manner in which privacy disclosures are made, in particular in the mobile space. For instance, California recently released its “Privacy On the Go: Recommendations for the Mobile EcoSystem” paper which, among other items, suggests that mobile provider privacy policies be in an easy-to-understand format, such as a layered privacy notice, or a “nutrition label for privacy.”¹⁵ Companies should be prepared for the method and manner of disclosure of privacy policies to potentially evolve in the near future.

Adhere to the DAA’s Self-Regulatory Principles

In addition to ensuring their privacy policies are up to date and followed, companies that own or operate websites where data is collected by third parties for OBA purposes or companies that use OBA data to deliver ads should adopt and comply with the Digital Advertising Alliance’s (DAA)¹⁶ self-regulatory principles.¹⁷ These principles set standards for consumer-friendly OBA practices and include use of an “Advertising Option Icon” (“Icon”) on advertisements using OBA. The Icon links to disclosures and provides the ability for consumers to opt-out of being tracked. Compliance with the principles is monitored by the industry as well. Adoption and compliance with this self-regulatory effort is critical if the advertising industry wants to continue to keep regulators and legislators at bay.

Research Providers Thoroughly and Ensure Agreements with Providers have Adequate Protections

Companies should research their RTB service providers thoroughly before entering into an agreement to use their services. Providers that will be tracking and providing tools to analyze multi-site data should have appropriate privacy policies that disclose in detail their privacy practices and the technologies used. Agreements should require that provider’s comply with the DAA’s principles, where applicable. Furthermore, companies should ask for assurances that providers have appropriate data security practices in place.

Licensing and ownership is important as well. Thoroughly understanding who will own and have access to the data collected and how can it be used is essential. For instance, does the technology allow aggregated data to be used across a variety of platforms, including competitive platforms? And, if so, does the provider have application protocol interfaces (API) that will allow one to access data and develop separate programs to manage the data? The answers to these questions could end up having a major impact on how useful the technology is over time.

Finally, companies should ensure that the contracts with providers have appropriate defense,

indemnity and insurance clauses to protect against potential data security breaches and breaches of privacy practices. With class actions continuing to be filed en masse, there is the increased potential for advertisers and the agencies that use ad networks to be named in the actions.

While the legal issues associated with RTB are not new, they are heightened due to the ever increasing scrutiny by regulators and law makers on data and privacy practices. Moreover, the increasing number of class actions that are filed relating to data and privacy practices increases the need for companies to ensure they are participating in RTB activities with adequate protections and compliance programs in place. While the White House recently commended the DAA's significant progress in implementing a strong privacy protection program for consumers,¹⁸ it does not mean that the issues of privacy are going to be left to self-regulation. Companies should stay on top of new laws and industry efforts to improve self-regulation.

II. The European perspective

Personal data are the raw material and their profiling and monitoring the common denominator for using the new tools, such as RTB, and the sophisticated marketing strategies made possible by them. But, in the end it all boils down to processing of personal data, a highly critical process in Europe. Within the territory of the European Union such practice is governed by two basic laws: the General Privacy Directive¹⁹ and the ePrivacy Directive²⁰, both currently under review and to be replaced soon by a new Regulation²¹.

In addition, researching and classifying of on-line behavior almost always implies the use of cookies, a practice that falls under the provisions of a separate Directive²² (known as the “Cookie Directive”), which clearly holds that *“Terminal equipment of users of electronic communications networks and any information stored on such equipment are part of the private sphere of the users requiring protection under the European Convention for the Protection of Human Rights and Fundamental Freedoms”* and therefore sets a range of limits to legitimate use of cookies.

Marketers will therefore have to carefully consider how these laws will impact on techniques and practices used for behavioral targeting. Furthermore it's advisable to achieve at least a broad idea on how European Data Protection Authorities usually approach compliance with the principles and requirements set by the EU's privacy provisions. Knowing that will help bring understanding as to how authorities are likely to enforce the principles against offenders.

To that purpose, there are some key aspects marketers should bear in mind.

- According to the General Data Protection Directive²³ all data processing may be performed exclusively for “*specified, explicit and legitimate purposes*” and all further handling has to be coherent with such purposes. In addition, the processing shall be adequate, relevant and not excessive in relation to the purposes for which data had been collected. Marketers performing any form of behavioral targeting will presumably perceive as the most disturbing requirement the one imposing that all collected data are to be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected.
- If we consider that the Directive also sets²⁴ – as a general criterion – that “*... personal data may be processed only if: (a) the data subject has unambiguously given his consent*” a strictly opt-in system results in nothing else than a true nightmare to the advertising industry. Neither

will marketers be happy about the provisions allowing data transfer exclusively to third countries (i.e. countries not member to the European Union) “ensuring an adequate level of protection”²⁵ or “on condition that: (a) the data subject has given his consent unambiguously to the proposed transfer...”²⁶.

- This initial legal framework was “refined” by the ePrivacy Directive²⁷ which, while referring to the general principles on processing of personal data to their handling in the context of electronic communication, has also introduced some important additional considerations. The Directive makes clear that all “*terminal equipment of users of electronic communications networks and any information stored on such equipment are part of the private sphere of the users requiring protection under the European Convention for the Protection of Human Rights and Fundamental Freedoms*” and therefore holds that “so-called spyware, web bugs, hidden identifiers and other similar devices can enter the user's terminal without their knowledge in order to gain access to information, to store hidden information or to trace the activities of the user and may seriously intrude upon the privacy of these users. The use of such devices should be allowed only for legitimate purposes, with the knowledge of the users concerned”²⁸.
- Therefore, any “intrusive device” “... for instance so-called 'cookies', can be a legitimate and useful tool, for example, in analyzing the effectiveness of website design and advertising, and in verifying the identity of users engaged in on-line transactions”, but “... their use should be allowed on condition that users are provided with clear and precise information ... about the purposes of cookies or similar devices so as to ensure that users are made aware of information being placed on the terminal equipment they are using” and “users should have the opportunity to refuse to have a cookie or similar device stored on their terminal equipment”, while “...the methods for giving information, offering a right to refuse or requesting consent should be made as user-friendly as possible. Access to specific website content may still be made conditional on the well-informed acceptance of a cookie or similar device, if it is used for a legitimate purpose”²⁹.
- Accordingly, practices essential to marketers, such as surfers' profiling or analyzing their on-line conduct through behavioral-, contextual- or location targeting, become extremely difficult, if not impossible, to perform legally as in the end only “... 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” is allowed³⁰ without users' proper in-advance information and consent.
- Basically, under these provisions the use of cookies is legitimate, provided: (a) targeted subjects are offered an easy to understand in-advance indication, both about the fact that cookies are to be installed on user's terminal as well as about their function and purposes, (b) users' consent for placing cookies is achieved, and (c) they're informed about their possibility to refuse cookies' placement on their terminals and about the browser settings apt to exercise such blocking right.

While marketers clearly were not exactly excited about all these requirements, a somehow viable solution to adopt a “notice and choice” system; in other words, usually “cookies” were placed and then users were informed about the placement and the possibility of having them removed. But such “notice and choice” practice had to be reviewed after the so-called “Cookie Directive”³¹ came into force.

According to the Directive's introductory declarations on inspiring key principles and scopes pursued:

- “Software that surreptitiously monitors the actions of the user or subverts the operation of the user’s terminal equipment to the benefit of a third party (spyware) poses a serious threat to the privacy of users, as do viruses. A high and equal level of protection of the private sphere of users needs to be ensured, regardless of whether unwanted spying programmes or viruses are inadvertently downloaded via electronic communications networks or are delivered and installed in software distributed on other external data storage media ”³²
- “Third parties may wish to store information on the equipment of a user, or gain access to information already stored, for a number of purposes, ranging from the legitimate (such as certain types of cookies) to those involving unwarranted intrusion into the private sphere (such as spyware or viruses). It is therefore of paramount importance that users be provided with clear and comprehensive information when engaging in any activity which could result in such storage or gaining of access. The methods of providing information and offering the right to refuse should be as user-friendly as possible. Exceptions to the obligation to provide information and offer the right to refuse should be limited to those situations where the technical storage or access is strictly necessary for the legitimate purpose of enabling the use of a specific service explicitly requested by the subscriber or user. Where it is technically possible and effective, in accordance with the relevant provisions of Directive 95/46/EC, the user’s consent to processing may be expressed by using the appropriate settings of a browser or other application. The enforcement of these requirements should be made more effective by way of enhanced powers granted to the relevant national authorities”³³.

Applying such principles under the Directive requires the following:

- Impose adequate notice to customers about their rights concerning information contained in subscriber directories (and about the purposes of such directories) as well as suitable organizational and technical protection measures apt to safeguard all personal information of (fixed and mobile) end users stored in databases.
- Take the opportunity of stressing again that “traffic data” controlled by providers of security technologies and services are subject to privacy requirements set both, by the General Privacy Directive as well as by the ePrivacy Directive.
- Provide that any new application based on devices for data collection and identification must result in uses “acceptable” to the targeted individuals and has to grant individual’s fundamental rights (and among them that to privacy and data protection).
- Flag concerns about the risks involved by the use of “software surreptitiously monitoring actions of the user or subverting the operation of the user’s terminal equipment to the benefit of a third party (spyware)”.
- Inform whoever intends “... to store information on the equipment of a user, or to gain access to information already stored, for a number of purposes, ranging from the legitimate (such as certain types of cookies) to those involving unwarranted intrusion into the private sphere (such as spyware or viruses)” that in such case users must receive “.. clear and comprehensive information when engaging in any activity which could result in such storage or gaining of access”.
- Clarify that “safeguards provided for subscribers against intrusion into their privacy by unsolicited communications for direct marketing purposes by means of electronic mail should also be applicable to SMS, MMS and other kinds of similar applications”.

The most worrying aspect for marketers relates to a strict “opt-in” mechanism deriving from the new wording of Section 5/3 of the ePrivacy Directive no. 58 of 2002. According to the amended text, cookie placement without seeking targeted subject's in-advance consent will be possible and legitimate in only the following two cases:

1. When essential for performing a communication's transmission over an electronic communications network; or
2. When necessary for providing an information society service specifically requested by the subscriber or user.

Thus, since 2011 providers, businesses and companies that need to process personal information in performing their activities face a serious struggle coping with these new requirements. This is made even more complicated as the amended new text of Section 5/3 of the ePrivacy Directive expressly refers to “information” about users, which is clearly something different – and has a much broader meaning - than what's defined by the term of “personal data”.

What can marketers expect from European Data Protection Authorities in terms of investigation and enforcement?

EU provisions such as those set by the General Data Protection Directive of 1995 and the ePrivacy Directive of 2002 require implementation on a national level, a fact that frequently leads to a certain level of differences in the application of the rules between one country and another. The current reform efforts of both Directives are aimed at preventing such differing interpretations through the approval of a Regulation, which is immediately binding for all Member States and does not allow flexibility in national implementation³⁴.

It is therefore all but easy – if not impossible - to achieve a 'harmonized' perspective about how privacy regulations are applied throughout the European Union.

The best way for addressing this problem is to monitor - on an ongoing basis - the working papers released by the Article 29 Working Party³⁵, an independent Advisory Body assisting the EU Commission with expert opinion on privacy issues.

Over the last few years, Internet companies (e.g., providers, search engines and on-line platform owners) frequently took the position that, because their business headquarters were located outside of Europe and the processing of the personal data was handled overseas, there was no reason to be concerned about the EU's privacy laws. Today, such approach could definitely result in a rather risky position for a number of reasons.

Over the years the Article 29 Working Party had expressed the view that:

- An individual's search history, IP addresses and cookies had to be considered ³⁶ as “*data relating to an identifiable person*” any time identification is possible by relying on reasonable means likely to be used.
- All the principles and key aspects dealt with by the provisions of the General Data Protection Directive did “*apply to the processing of personal data by search engine providers in many cases, even when their headquarters are outside the EEA*”³⁷ and that multinational search engine providers were subject to the national laws governing the

handling of personal information (aside from the case where they had an “establishment” in a country member to the EU), when a “*company makes use of equipment, automated or otherwise on the territory of that Member State, for the purposes of processing personal data (for example, the use of a cookie)*”.

- It was “*beyond doubt that the processing of traffic data falls within the scope of the Data Protection Directive*”,³⁸ and that unless a service provider “*is in a position to distinguish with absolute certainty that the data correspond to users that cannot be identified ... all IP information*”, will have to be treated “*as personal data, to be on the safe side*”,
- “*...the technological developments have strengthened the risks for individuals' privacy and data protection and to counterbalance these risks, the principle of “Privacy by Design” should be introduced in the new framework: privacy and data protection should be integrated into the design of Information and Communication Technologies*”³⁹ and mechanisms safeguarding an individual's privacy should “*become embedded in ICT*”⁴⁰.
- Social networks also have to comply with privacy requirements and obligations⁴¹ deriving from the key principles of the Directives, with a specific reminder about the fact that while direct marketing is certainly to be recognized as “*an essential part of the SNS business model*”, the respective practices are also required to “*comply with relevant provisions of both Data Protection and ePrivacy Directive*”⁴².
- The multiple advantages and economic benefits offered by “*on-line behavioral advertising*”⁴³ in an Internet focused economy being out of question, marketers nevertheless should not ignore “*individual's rights to privacy and protection of personal data*” and the requirements to be fulfilled for correct compliance with the respective provisions (among them: achievement of user's “*informed consent*” for placement of tracking devices such as cookies, availability of adequate browser settings and “*affirmatively activated*” opt-in systems granting users' actual willingness to be subject to the monitoring of surfing behavior for the purpose of receiving tailored advertising, possibility of limiting in time the scope of user's consent and of revoking easily such consent in the aftermath, presence of visible alerts about monitoring being performed and tracking devices being in place)⁴⁴.

In recent years the Working Party has also looked into other privacy aspects related to technical development and new devices.

A specific Opinion⁴⁵ deals with geolocation services on smart mobile devices. Believing that “*the value of information*” (e. g. financial data, health data and other consumer behavioral data) “*increases when it is connected to location*”, the Working Party has considered necessary clarifying the legal requirements of such new services under the Data Protection Directive⁴⁶, especially when providers of geolocation based services are capable of gaining a very intimate overview on a mobile device owner's habits and patterns as well as of building extremely detailed and comprehensive user profiles. With respect to smart mobile devices such scrutiny and profiling potential is increased by the fact that these devices are generally equipped with a number of “*unique identifiers*” (e.g. the MAC address, the operating system identifying number, etc.) and therefore allow “*singling out*” an individual even without knowing the device owner's real name. Systems with more or less identical capacities are in place with respect to WiFi access points. Relying on elements such as signal strength or SSID, it's easy to trace and determine the exact location of an access point. From there, the path to discovering an individual's name isn't difficult. There is no surprise that these technical implications have convinced the Working Party of unconditional applicability of the Directive no. 46 of 1995 to these practices, as its provisions define “*personal data*” as “*any information relating to an identified or identifiable natural person ('data subject')*”⁴⁷.

On the basis of such premise the Opinion identifies “*three different functionalities ... with different responsibilities...*” i. e. “*the controller of a geolocation infrastructure, the provider of a specific geolocation application and the developer of an operating system of a smart phone device*”. All will have to comply –in different ways – with privacy requirements.

In December 2011, the Working Party delivered its views on the EASA/IAB Best Practice Recommendation on Online Behavioral Advertising, as a token a rather than a critical stand⁴⁸. While the economic benefits potentially deriving from behavioral advertising were openly acknowledged, the Working Party clearly voiced its opposition against such practices being “*carried out at the expense of individuals' rights to privacy and data protection*”. The opinion exposes the conclusion that “*adherence to the EASA/IAB Code on online Behavioral advertising and participation in the website www.youronlinechoices.eu does not result in compliance with the current e-Privacy Directive*” and that “*moreover the Code and the website create the wrong presumption that it is possible to choose not to be tracked while surfing the Web.*”⁴⁹

In its reasoning the Working Party argues its position by affirming that:

- The use of cookies in the context of behavioral advertising and the collection of unique identifiers with tracking capacity implied by such use will easily bring such practice under the applicability of the provisions of the ePrivacy Directive.
- That users' consent for the placement of cookies will be necessary in many cases, but may also be obtained in user friendly ways (such as an information banner at the top of a website, a splash screen) and once correctly achieved, is suitable to cover both, “*a cookie serving the same purpose and originating from the same provider*” as well as the access to other websites “*that share the same OBA network*”.
- An issue of concern consists in the fact that the proposed Code fails to offer provisions and detailed indications as to the ways of collection, the amount of data achieved, the period of storage and the purposes of processing.

A few months later, the Working Party issued additional guidance on the use of cookies, provided through Opinion no. 4/2012⁵⁰. Specifically, the working paper addressed the problem of correct interpretation of Article 5/3 of the ePrivacy Directive in its amended wording (introduced by Directive no. 136 of 2009⁵¹) on the possible uses of cookies without users' consent and provides the following requirements:

- A cookie use may be held as “strictly necessary” for communication transmission purposes only when it allows to: (a) route the information over the network, (b) exchange data items in their intended order, and (c) detect transmission errors or losses⁵², and
- A cookie use for meeting a subscribers or users specific service request will have to meet a double requirement: (a) it has to be necessary for fulfilling a specific (exactly identified) service request originating from a subscriber/user who performed a “positive action” in order to solicit the service, (b) the cookie is absolutely instrumental for providing the requested service which would not work at all in absence of the cookie (reference is clearly to a “functionality” criterion).

The Working Party also explained that in its view, “third party cookies” and “multipurpose cookies” will have difficulty meeting these exemption criteria and additionally warned that cookies compliant with the requirements and legitimately placed without seeking consent (e.g. a cookie necessary for accessing a certain functionality via a “log in” mechanism) may not be used for other secondary purposes such as behavioral monitoring or advertising⁵³. Finally, it stressed that the

duration of a cookie use is a crucial aspect to consider and closes with the recommendation: “*in case of doubt, seek user's consent in a simple and unobtrusive way*”.

To round off this *excursus*, a few lines from another recent Opinion⁵⁴ that focused on facial recognition in on line and mobile services is worth mentioning.

On the premise that “*facial recognition contains sufficient details to allow an individual to be uniquely identified*”, the Working Party held that “digital images” allowing an individual's identification are to be considered as “personal data” and easily as “biometric data” (when “*they relate to biological properties, behavioural aspects, physiological characteristics, living traits or repeatable actions where those features and/or action are both, unique to that individual and measurable*”). Therefore, facial recognition results in an “*automated form of processing of personal data, including biometric data*”. Subsequently, all key principles and criteria laid down in the General Data Protection Directive no. 46 of 1995 will apply to face recognition practices, a fact that web site owners, on-line service providers and mobile application operators should keep in mind as all requirements and obligations set by the Directive will apply to them⁵⁵. This conclusion may also be extended to companies running on-line social networks as in the Working party's view “*SNS providers are data controllers*” in the Directive's meaning.

This may sound odd in times when social networks enjoy extreme popularity and offer immense potential to marketers; but ignoring these views and recommendations will easily expose an infringer to fines (sometimes of significant amount) and sometimes also to criminal prosecution⁵⁶.

Self-Regulation in the EU

Interested industry sectors have tried – and are trying hard – to prevent further regulatory intervention by pushing the adoption of self-regulation systems.

Aside from the mentioned joint initiative of EASA and IAB⁵⁷, the International Chamber of Commerce – ICC in December 2012 published a Resource Guide⁵⁸ for self-regulation of online behavioral advertising with the intent to offer the advertising sector some “*fundamental principles that any market in the world can use when setting up OBA self-regulation*”. The Guide provides a check list of things to do and of aspects to properly consider before engaging in OBA. This check list extends from contacting (or cooperating with) interested stakeholders to developing adequate program architecture and operational structure as well as to considering the use of trust marks or special icons and adherence to self-certification systems and finally to consumer education and on-going dialogue in order to ensure regulatory alignment and support.

On a national level we have also seen:

- The Federation of the German Advertising Industry setting up (in November 2012) a special body, the Privacy Council for Online Advertising (DDOW), which has issued a specific self-regulation code with the key principles to obey with when marketers process personal data in the context of on-line behavioural advertising.
- The Advertising Standards Authority for Ireland extending its digital remit to include marketing communications on advertisers' profile pages and other non-paid-for space on line, under advertisers' control (previously outside of remit)⁵⁹.
- The UK the Advertising Standards Authority (ASA) releasing, earlier this year, new rules⁶⁰ meant to provide the public with notice of, and control over, on line behavioural advertising

(OBA).

What lies ahead in the EU?

The European Union is currently “updating” both the General Data Protection Directive no. 46 of 1995 and the ePrivacy Directive no. 58 of 2002, believing that their provisions need to be brought in line with technical progress and with the challenges of a digital marketplace.

In a recent speech Viviane Reding, Vice-President of the European Commission and EU Justice Commissioner, explained the reasons behind the reform of the current Community Laws governing data processing and has addressed the privacy concerns of EU citizens: “*17 years on, we have to think about whether our data protection rules still work. Many citizens think that they don't. 92% of Europeans are concerned about mobile apps collecting their data without their consent. 89% of people say they want to know when the data on their smartphone is being shared with a third party. They want the option to give or refuse permission.*”⁶¹

On January 25th, 2012, the European Commission released a draft text for a new Regulation meant to replace both existing Directives. The key goals the new Regulation intends to achieve include:

- A single set of rules on data protection, valid across the EU (deemed to remove excessive administrative requirements for companies and allowing them significant cost savings).
- A clear support of a “*one-stop shop*” approach both, for companies doing business on a cross-border basis as well as for consumers intending to file a complaint against a company established in a country other than their own⁶².
- The principle that where data subject's consent is required, it'll have to result in clear and unambiguous form and no “consent-by-mere-implication” mechanisms will be allowed.
- The aim to strengthen data subject's rights as to easy access to and transfer of their personal information from one service provider to another.
- Granting people a “right to be forgotten” in order to achieve a more effective management of risks in on-line environments⁶³.
- Increased enforcement powers assigned to the national DPAs⁶⁴.

The proposed Regulation is currently pending before the European Parliament, which will probably decide on its final approval in 2013.

No doubt foreign marketers doing business in the EU and offering services to its residents have started suffering from serious headaches when faced with the perspective of becoming subject to the EU privacy laws even when personal information of EU citizens are handled abroad. It is also no surprise that all major players active in on-line businesses have deployed all their lobbying potential in order to water down some of the new provisions as much as possible (especially the proposed definitions of “legitimate interest” justifying data use and the “informed and explicit consent” requirement are perceived as highly disturbing and interfering with business). Such efforts are strongly opposed by the Article 29 Working Party which tries to keep the proposed regulation’s text as much as possible coherent with its views on adequate processing and protection of personal data in any context inclusive the on-line environment⁶⁵.

Last Word on the EU

All this may sound strange to those not familiar with the European approach to privacy and the

perception of personal data protection as a fundamental right, pertaining to an individual's most intimate and private sphere.

Nevertheless, foreign marketers relying on behavioural and/or contextual data and intending to perform their business throughout the European Union will need to carefully bear in mind the Old Continent's views on collecting, storing and processing of personal information. When making use of data provided by third parties, they will be well advised to properly address, in their contractual agreements with data sources, issues such as legitimate origin and transfer of data, achievement of informed consent, adoption of adequate safety measures in order to avoid data breaks/losses, etc. Failure to address such potential implications could expose them to (secondary) liability as "joint data controllers".⁶⁶

Considering the increased maximum amounts proposed by the upcoming EU Regulation, fines can badly hurt companies liable of infringement, but it's also crucial to recall that in many European jurisdictions criminal sanctions may easily be served for non-compliance with some requirements set for legitimate data processing (e. g. consent for handling so-called "sensitive" data, illicit publication or diffusion of data, incorrect data transfer abroad, in certain cases, failure to put proper safety measures in place).

(Reference date of this paper: March 2013)

¹ IDC, Real-Time Bidding in the United States and Worldwide, 2011-2016 (Oct. 2011).

² *Real-Time Bidding Poised to Make Up Quarter of All Display Spending*, Emarketer.com Nov. 14, 2012, <http://www.emarketer.com/newsroom/index.php/realtime-bidding-poised-quarter-display-spending/#M0yREeg1tuh1vKc.99> (last visited March 1, 2013).

³ See Sandra Landwehr v. AOL Inc., (E.D. Va.), Case No. 1:11-cv-01014-CMH-TRJ (2006). In 2006, AOL released 20 million search queries to the academic community. AOL attempted to de-identify the data before releasing it by removing IP addresses and usernames to protect the privacy of AOL users. However, researchers were able to link search queries with the individuals who conducted the searches.

⁴ Dara Kerr, *Do Not Track Privacy Bill Reintroduced in Senate*, CNET.com, Feb. 28, 2013, http://news.cnet.com/8301-1023_3-57571958-93/do-not-track-privacy-bill-reintroduced-in-senate/ (last visited, March 1, 2013).

⁵ 18 U.S.C. § 2810.

⁶ *Id.* § 2511.

⁷ *Id.*

⁸ 18 U.S.C. § 1030.

⁹ 15 U.S.C. § 45 et. seq.

¹⁰ 15 U.S.C. § 6501-06; See also John Feldman and Fred Lah, *Right On Time: FTC Announces COPPA Update*, Reed Smith LLP Global Regulatory Enforcement Blog, December 19, 2012, available at, <http://www.globalregulatoryenforcementlawblog.com/2012/12/articles/data-security/right-on-time-ftc-announces-coppa-update/> (last visited February 1, 2013).

¹¹ See *Google Agrees to Change Its Business Practices to Resolve FTC Competition Concerns In the Markets for*

Devices Like Smart Phones, Games and Tablets, and in Online Search, Federal Trade Commission press release, January 3, 2013, available at <http://www.ftc.gov/opa/2013/01/google.shtm> (last visited February 28, 2013).

¹² In the matter of Epic Marketplace and Epic Media Group, LLC, available at <http://ftc.gov/opa/2012/12/epic.shtm> (last visited March 1, 2013).

¹³ People v. Delta Air Lines Inc., Cal. Super. Ct., No. CGC-12-526741, filed Dec. 6, 2012.

¹⁴ See Ian Paul, *Instagram Updates Privacy Policy, Inspiring Backlash*, PC World, Dec. 18, 2012, <http://www.pcworld.com/article/2021285/instagram-updates-privacy-policy-inspiring-backlash.html> (Last visited March 1, 2013).

¹⁵ *Privacy On the Go: Recommendations for the Mobile EcoSystem*, California Department of Justice, Jan, 2013, available at oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf (last visited March 1, 2012)

¹⁶ The DAA is a consortium of the nation's largest media and marketing associations, the American Association of Advertising Agencies (4A's), the Association of National Advertisers (ANA), the American Advertising Federation (AAF), the Direct Marketing Association (DMA), the Interactive Advertising Bureau (IAB) and the Network Advertising Initiative (NAI).

¹⁷ Four years ago, the DAA developed the "Self-Regulatory Principles for Online Behavioral Advertising" which are designed to foster compliance with the Federal Trade Commission's 2009 "Staff Report on Self-Regulatory Principles for Online Behavioral Advertising". In 2010, the DAA introduced the "Advertising Option Icon" which is placed on advertisements and provides consumers with a link to disclosures and options for opting out of tracking. In 2011, the DAA introduced its "Self-Regulatory Principles for Multi-Site Data," which sets forth principles surrounding the collection of online data from a particular computer or device regarding web viewing over time and across non-affiliated websites.

¹⁸ White House, *DOC and FTC Commend DAA's Self-regulatory Program to Protect Consumer Online Privacy*, Feb. 23, 2013, <http://www.prnewswire.com/news-releases/white-house-doc-and-ftc-commend-daa-self-regulatory-program-to-protect-consumer-online-privacy-140170013.html> (last visited February 29, 2013).

¹⁹ Directive no. 95/46/EC of the European Parliament and of the Council of 24 October 1995.

²⁰ Directive no. 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)

²¹ The European Commission has already published (in January 2012) a draft text of such new Regulation, performed a public consultation in order to discuss its key aspects and presented the bill to the EU Parliament for reading and approval; see below point no. (viii.).

²² Directive no. 2009/136/EC of the European Parliament and of the Council of 25 November 2009.

²³ Directive no. 95/46/EC of 1995, applicable to all processing of personal data, irrespective of the technical means used to the purpose.

²⁴ So Section 7 of Directive no. 95/46.

²⁵ So Section 25 of Directive no. 95/46.

²⁶ So Section 26 of Directive no. 95/46.

²⁷ Directive no. 2002/58/EC of 2002.

²⁸ The statements may be found in Recital no. 24 of the Directive's introducing Premise.

²⁹ These indications are contained in Recital no. 25 of the Directive's introducing Premise.

³⁰ See Section 5/3 of the ePrivacy Directive no. 58 of 2002.

³¹ Reference is to 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), which had to be implemented nationally by EU Member States no later than by May 25th, 2011.

³² Statement contained in Recital no. 65 of the Directive's introducing Premise.

³³ Statement contained in Recital no. 66 of the Directive's introducing Premise.

³⁴ See below Point no. (viii.) of this paper.

³⁵ The WP was established by Article 29 of Directive 95/46/EC with the specific task to offer expert opinion from member state level to the EU Commission on questions of data protection, promoting harmonized application of the general principles of the Directives in all Member States through co-operation between data protection supervisory authorities, advising the EU Commission on any Community measures affecting the rights and freedoms of natural persons with regard to the processing of personal data and privacy. All EU Member States have a representative in this body and the national DPA's will always conform their activities to the indications issued by this Advisory Board.

³⁶ So Opinion 4/2007 - WP 136 - of June 20th, 2007 (on the concept of 'personal data').

³⁷ See Opinion 1/2008 – WP 148 - on data protection issues related to search engines adopted on April 4th, 2008.

³⁸ WP 159, issued on February 10th, 2009 with comments relating to the – then - draft text of Directive no. 136/2009.

³⁹ WP 168 of December 1st, 2009, joint contribution - with the Working Party Police and Justice – to the Consultation of the EU Commission on the legal framework for the fundamental right to protection of personal data.

⁴⁰ According to the Opinion "the application of such principle would emphasize the need to implement privacy enhancing technologies (PETS), 'privacy by default' settings and the necessary tools to enable users to better protect their personal data (e.g., access controls, encryption). It should be a crucial requirement for products and services provided to third parties and individual customers (e.g. WiFi-Routers, social networks and search engines). In turn, it would give DPAs more powers to enforce the effective

implementation of such measures" (page 13, point no. 48).

41 Opinion 5/2009 – WP 163 – of June 12th, 2009 on on-line social networking. The Opinion provides guidelines as to: indications about providers' identity, information about purposes and ways of data uses, warnings about privacy risks related to data posting, availability of privacy-friendly default settings, copyright and minors' protection, respect of other data subjects' rights, handling of abandoned accounts, easy-to-use complaint handling procedures and user's possibility of adopting pseudonyms.

42 In Section 3.7. the Opinion addresses contextual, segmented and behavioural marketing.

43 So Opinion no. 2/2010 – WP 171 – of June 22nd, 2010. In the Opinion's introductory section the Working Party defines 'profiling mechanisms' as follows: "*Whereas contextual advertising and segmented advertising use 'snap shots' of what data subjects view or do on a particular web site or known characteristics of the users, behavioural advertising potentially gives advertisers a very detailed picture of a data subject's online life, with many of the websites and specific pages they have viewed, how long they viewed certain articles or items, in which order, etc."*

44 Considering that "*in the context of behavioural advertising users may not know or understand the technology that supports behavioural advertising or even that such types of advertising are being targeted at them*" the Working Party feels that "*it is therefore of paramount importance to ensure that sufficient and effective information is provided in a way that will reach internet users. Only if data subjects are informed, will they be in a position to exercise their choices*", so Opinion no. 2/2010, page 17, Section 4.2.

45 Opinion no. 13/2011 – WP 185 – dated May 16th, 2011.

46 Interestingly the Opinion states that it will not address 'geo-tagging' (through which web users integrate geo-referenced information on social networks) and "*other geo-location technologies that are used to interconnect devices within a relatively small areas (shopping centres, airports, office buildings, etc.) such as Bluetooth, ZigBee, geofencing and WiFi based RFID tags, though many of the conclusions of this opinion with regard to legitimate ground, information and data subjects' rights also apply to these technologies when they are used to geolocate people through their devices*", so Introduction, page 4.

47 So Article 2 of the Directive.

48 Expressed through Opinion no. 16/2011 – WP 188 – of December 8th, 2011, which refers to self-regulatory best practice guidelines for online behavioural advertising, proposed by the European Advertising Standards Alliance (EASA) jointly with the Interactive Advertising Bureau Europe (IAB).

49 See final paragraphs of the Opinion on page 12.

50 The Opinion – WP – 194 – was released on June 7th, 2012 and focuses on "Cookie Consent Exemption".

51 According to the new wording the use of cookies is exempt from the requirement of user's informed consent just in two cases: (a) if it serves the sole purpose of a communication's transmission over an electronic communications network, (b) when it results strictly necessary for providing an information society service requested by a subscriber or user.

52 A cookie simply 'facilitating' a communication's transmission therefore does not fall within the exemption.

53 In Section 4. the Opinion provides also a list of cookies not covered by the consent exemption: social plug-in tracking cookies, third party cookies used for behavioural advertising, first party cookies used for analytics (e. g. audience measuring),

54 Reference is to Opinion no. 2/2012 – WP 192 – released on March 22nd, 2012.

55 That's to say the obligation: to provide in-advance notice about data uses and collection purposes (which have to be relevant, not excessive and performed for legitimate grounds), to keep processing in line with the announced purposes, to use and store collected data only for a strictly necessary period; for biometric data individual's 'informed consent' will have to be sought.

56 Through judgement no. 86611 of a Court of Appeal in Milan (pronounced on December 21st, 2012 and published on February 27th, 2013) a first instance decision was reversed and three executive managers of a major search engine were acquitted on criminal charges of liability for hosting on the company's on-line platform content offensive to a disabled person.

But a few days earlier in the UK the same search engine was reminded by a Court of Appeal (Civil Division) that under certain circumstances it may be considered, in its role of a blog's host, as a 'publisher' and provider of a "*service available on terms of its own choice*", potentially liable for diffusing abusive content and unable to successfully claim immediate exemption "*under section 1 of the 1996 Act*", with the consequence that "*the period during which* company X "*might fall to be treated on that basis as a publisher of the defamatory comments would be a very short one*, but it means that the claim cannot ... be dismissed on the ground that" company X "*was clearly not a publisher of the comments at all*" (the judgement dated February 14th, 2013, may be found on Bailii – ref. [2013] WLR(D) 65, [2013] EWCA Civ 68 - Case No: A2/2012/0691).

57 See comments in point vi. In October 2012 the European Interactive Digital Advertising Alliance (EDAA) was launched to help drive forward this European SR Initiative on OBA.

58 The Guide may be found on the ICC's web site at the URL:

http://www.iccwbo.org/uploadedImages/News_and_Media/Articles/2012/icc-resource-guide_source.png.

59 According to indications on the ASA's web site the extension of remit will be effective from 2nd January 2013. However there will be a three month grace period during which the ASA will investigate complaints, but will not refer them to the independent Complaints Committee for formal adjudication.

60 Effective since February 4th, 2013.

61 Speech delivered in Brussels on December 4th, 2012 at the 3rd Annual European Data Protection and Privacy Conference.

62 An approach that offers significant advantages; companies would need to deal just with a single national data protection authority (that of the EU country where they have their main establishment), consumers will be in a position to file complaints with DPA in their country even in cases when data are processed by companies located outside the EU.

63 This right would imply that data subjects must be enabled to delete their personal information, once no longer legitimate reasons are given for data retention. It's to be seen how such ambitious goal will be achieved and made possible technically.

64 According to the proposed new provisions the national DPAs will be entitled to fine companies infringing the EU data protection rules with penalties of up to Euro 1 million or up to 2% of the global annual turnover of a company.

65 Recently the Working Party contributed, through Opinion no. 8/2012 – WP 199 - of October 5th, 2012, additional input to the discussion on the planned data protection reform.

66 Currently an interesting case is pending in front of the Court of Justice of the European Union (reference is to Case C-131/12, Spain vs. search engine X) involving issues such as: search engine's role (Publisher? Host? Controller?) and applicability of EU law to foreign companies. The case originates from search results leading to a newspaper announcement – published several years earlier – reporting that a certain real estate property was set to auction because of owner's non-payment of social security contributions.