

Chapter 2

On-line Behavioral Tracking: What May Change After the Legal Reform on Personal Data Protection

Georgia Skouma and Laura Léonard

Abstract On-line tracking has gained over the last years a new dimension: it has become an intrinsic part of our Internet-driven society. It touches all levels and types of industries. Consequently, more and more individuals become the target of this trend as routinely users of the internet. On-line tracking techniques are subject to the European personal data protection rules currently in force, insofar as they process information that identifies or may potentially identify a natural person. Nevertheless, the unprecedented threats that such techniques entail to privacy must have been a core motive opening the way towards the revision of the privacy regulations applicable today. New requirements and concepts strengthening the rights of data subjects and the obligations of data controllers or processors are set forth in the current draft of the new Regulation (currently under discussion within the EU institutions). This envisaged legal reform may however prove to be insufficient unless, at the same time, effective measures are adopted to help both on-line users, especially those of young age, and the companies implementing on-line tracking tools in order to change their approach to privacy.

With the exponential growth of “smart” technologies, new forms of tracking individuals’ behavior, habits, and personality have emerged. Amongst those, the tracking of users while they are interacting over the Internet (on-line tracking), has proved its added-value primarily to marketing and advertising companies, but also other industries which increasingly use those smart techniques next to other intelligent “customer relationship management” (CRM) tools.

The opinions expressed in this article reflect the personal views of the authors and do not engage in any way whatsoever the company with whom they are working.

G. Skouma (✉) • L. Léonard

Department of Security and Privacy, Deloitte Bedrijfsrevisoren/Réviseurs d’Entreprises, Diegem, Belgium

e-mail: gskouma@deloitte.com; lauleonard@deloitte.com

The majority of on-line tracking technologies today is based on cookies; by using cookies as the backbone, the designers of on-line tracking tools have developed other smart applications. On-line tracking applications of the latest technology combine users' data through observation tags, analyze them using algorithms, and then compare them with a mass of other data that have been collected by many other users. The purpose of the data analysis and mapping to the "stock" of data already collected is to adduce some conclusions about the interests, marketing and buying habits of the tracked individuals. Other on-line tracking smart solutions dig into the traces website users leave on social networking tools, combine them with data collected off-line, and make up with sometimes (not) so great accuracy the profile of an individual.

All above on-line tracking techniques are already subject to the European personal data protection rules underpinned in the current Data Protection Directive (95/46/EC) insofar as they process information that identifies or may potentially identify a natural person. The basic personal data protection requirements stemming from the principles of purpose limitation, data minimization, proportionality, transparency, data destruction—to mention only some of those—are undoubtedly of great relevance here. Nevertheless, at the time the Directive was enacted, the EU legislator could not predict the massive use of on-line tracking tools we are all subject to nowadays as routine internet users. This is probably one of the reasons why the draft Regulation on personal data protection ("Regulation"), that is ought to replace the aforementioned Directive, reserves in its current wording very specific phrasing around users' monitoring and profiling. First, it seems that the risks associated with online activity have been one of the major incentives to suggest the revision of the existing regulatory framework of personal data protection (Recital 7 of Regulation). Second, a number of requirements set forth in the Regulation strengthen and specify more practically legal rules that are found back in the current legislative framework. This is the case notably with the consent, transparency, and notice requirements. Finally, yet most importantly, a few new concepts formally introduced by the Regulation for the first time, such as the privacy by design principle or the right to be forgotten (or right to erasure) will have a major impact (on condition that they are effectively implemented) on the designers of the on-line tracking solutions, as well as on the companies implementing them.

Yet if the Regulation is adopted with the wording proposed today (or stricter one), will this ensure that the overarching privacy right of the on-line users and the rights resulting from it will be better protected? Undoubtedly this will not be the case if the user's mentality around the "on-line activity" does not change. Users, especially those of young age, many times truly addicted to the network, must constantly reminded of the huge potential that their data represent for marketing companies but also for any other organization wishing to learn about them (headhunters, employers, social networks, press and media, police, law enforcement agencies and so on). Moreover, actions to incentivize on-line users and the implementers of on-line tracking technologies to demand *proven controls* from the designers and vendors of such tools that they adequately safeguard users' privacy may be an addition to ensure better and effective protection. Regulators, standards-setting

bodies, and public interest organizations are some of the categories of market stakeholders who could efficiently drive and monitor users' and implementers' awareness, education, and if needed, meaningful enforcement.

2.1 On-line Behavioral Tracking

2.1.1 Definition and Today's Trends

If on-line behavioral tracking has its roots in the marketing industry,¹ it has gained over the years and due to the emergence of smart technologies, a new dimension: currently, behavioral tracking has become an intrinsic part of our internet-driven society. From a marketing trend (known as on-line *behavioral advertising*), it has rapidly become a general *industry trend* with a deep impact on our everyday activities; it crosses the borders of our privacy. In that sense, the citizen of our Information Society today is tracked constantly on the street (camera surveillance), in car (radars and geo-localization devices), at the workplace (badging, biometrics, monitoring of PC and phone) or during the majority of his other activities (travelling, shopping – RFID –, leisure, and so on).

Amongst all these methods of tracking individuals' behavior, the on-line behavioral tracking represents an important part, as it happens easily and is based on common technological tools an individual is carrying (such as a laptop, a smart-phone, an iPad) and which provide connection to *the Internet*. In other words, on-line tracking consists of recording and collecting data linked to an individual visiting the Internet through such tools over a period of time in order to gain information on this individual.² The information collected forms a source of knowledge linked to the person in question. The knowledge involved in tracking is not empirical or technical. On-line tracking has actually been turning into a real science (part of marketing "intelligence") in which professionals are developing advanced models and patents to optimize the analysis over the data tracked and provide "unique" insights. The on-line behavioral tracking enables the collection of many and diverse data about a person, ranging from merely identification details (such as a user name or a subscriber's name) or the means connecting the person to the internet (IP address), to information which could reveal a lot about an individual's personality, hobbies, interests, shopping habits, favorite activities and so on. Many

¹Matthew S. Kirsch, *Do-Not-Track: Revising the EU's Data Protection Framework to Require Meaningful Consent for Behavioral Advertising*, (XVIII RICH. J.L. TECH. 2) available at <http://jolt.richmond.edu/v18i1/article2.pdf>.

²M. Hildebrandt, *Profiling: from data to knowledge* (DuD: Datenschutz und Datensicherheit 30, 2006 9), 548-549;

P. Eckersley, *What does the "Track" in Do Not Track Mean?* (Electronic Frontier Foundation, 19 February 2011) available at <https://www EFF.org/deeplinks/2011/02/what-does-track-do-not-track-mean>, 548-549.

times, the data tracked through the on-line behavioral techniques explained below are even sensitive data (revealing a person's sexual orientation or philosophical beliefs, for example). If the collection of the data is the first dimension of the on-line behavioral tracking, the second is the "mapping together" or correlation of these data in order to adduce meaningful conclusions about such individual (e.g. about his habits, interests, etc.) or in order to situate him in a particular category (e.g., the type of "buyer" he is). A third dimension is the assembling of data and the comparison of this set of data with other matched data referring to other persons or categories of persons with a view to creating the user's profile.

Examples of online behavioral tracking are broadly discussed in literature and refer to real examples from ordinary web users while surfing on the internet. Imagine yourself visiting an e-commerce website selling clothes. You are specifically searching for shoes. The day after, you visit again the same e-commerce website and the website proposes you a selection of articles you may like. The selection is only composed of pairs of shoes. Even though you did not purchase the product at the end, the site recorded your preferences and adapted the content it to your interests. The majority of the stated examples, as this one, discuss on-line behavioral tracking as used by the marketing and sales industry and, more in particular, in an advertising context.³ Yet, some types of on-line tracking technologies may target citizens for other reasons, such as in order to detect a person's political affiliation and societal activities, work history, social networking activity, religious convictions, and other aspects of his private life and personality. In the same vein, the reasons for performing online behavioral tracking vary from merely lucrative and consumption-driven (advertising) reasons to political motives or reasons related to public and state safety, public security and the like. Thus, targeted advertising online is just a facet of tracking and probably the most widespread one, but not necessarily the only one.

2.1.2 Techniques of Online Tracking

On-line tracking techniques and intelligent "searching" over the internet evolve as fast as "smart" automated technology evolves in general. On the other hand, the research community, with sometimes contributions of industry, have been increasing their efforts to promote technological solutions that enable citizens to better control their data on-line.⁴ Moreover, regulators, public interest stakeholders and the EU

³Advertising can be defined as the activity that consists of attracting potential customers to purchase or use a specific product by using media or other means. Clearly, advertising includes a lucrative purpose. On the contrary, tracking is more general and does not necessarily include a lucrative element.

⁴See in this regard the results of two research projects funded through successive Framework Programs of the European Commission, namely the PRIME and PrimeLife projects (www.primelife.ercim.eu). Both projects had as objectives to show how privacy technologies can enable

legislative bodies seem eager to enhancing users' awareness around the so-called Privacy Enhancing Technologies (PETs).⁵

Which are however the most common "business intelligent" techniques and tools nowadays which collect the human traces on the internet? The predominant technological means used remains the cookie.

The section below discusses the role that cookies could play in on-line tracking, as well as a number of other tools and market trends that systematically or inadvertently can scrutinize individuals and their behavior on-line. The purpose of the section is not to provide an exhaustive list of such techniques but to stress to the reader how tools that represent today "widely accepted" business practices may hide, each one to a less or greater extent, a threat to privacy.

2.1.2.1 On-line Scrutiny Through Cookies: Are They Always a Threat to Privacy?

A cookie is a *"piece of text stored by a user's web browser and transmitted as part of an HTTP request"*.⁶ It contains bits of information and it is set by a web server.

A first distinction that can be made between the different types of cookies used is between "first party" and "third party" cookies. First-party cookies are

citizens to execute their legal rights to control personal information in on-line transactions. The main objective of these projects was to bring sustainable privacy and identity management to future networks and services. It is noteworthy that well-known software vendors were members of the research consortium having conducted this project. Some more information about the PETs and their added-value for business, see: Privacy-enhancing technologies for the Internet. Ian Goldberg, David Wagner, Eric Brewer.

<http://www.cs.berkeley.edu/~daw/papers/privacy-compcon97-www/privacy-html.html>; Study on the economic benefits of privacy-enhancing technologies (PETs), Final Report to The European Commission DG Justice, Freedom and Security, Prepared by London Economics, July 2010 at http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_pets_16_07_10_en.pdf (the article contains relevant examples of PETs and a business survey regarding the use of PETs; Privacy Enhancing Technology. Privacy Enhancing Technology. Guidelines and Testing Methodology, W3C/QA Position Paper, Tara M. Swaminatha at <http://www.w3.org/2001/01/qa-ws/pp/tara-swaminatha-cigital.html>. The article gives an introduction on the fact that the market has seen an increasing flood of privacy enhancing products.

⁵The European Commission seems to accept the definition of PETs as provided in the EC-funded PISA project, being "a coherent system of ICT measures that protects privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data, all without losing the functionality of the information system", see Communication from the Commission to the European Parliament and the Council on promoting data protection by privacy-enhancing technologies. COM(2007) 228 final. According to the same Communication, examples of PETs include encryption tools preventing tracking of the data transferred; cookie-cutters blocking cookies placed on user's PC; the platform for Privacy Preferences (P3P) allowing users to analyse privacy policies and compare them to their preferences.

⁶ENISA, *Privacy considerations of online behavioural tracking*, (October 2012) available at <http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-considerations-of-online-behavioural-tracking>, 6.

implemented by companies on their own websites enabling such companies to interact directly with the users who visit their sites. On the contrary, when a company enables other third parties to track the users visiting its website, for example, by placing advertisements of third party vendors, then we talk about “third party” cookies.⁷ Companies implementing first party cookies can control better the types of information that is stored on the cookies and decide on their own how to use the information collected through their own cookies. On the contrary, the companies accepting cookies of other vendors on their websites often waive any responsibility relating to how the companies having placed the cookies will treat the information collected through such cookies. It is obvious that third party cookies represent a greater risk to privacy compared to first party cookies since in the first case it becomes more complicated for users to keep an effective control over their data.

A second notable differentiator amongst the cookies used on vendors’ websites is the time of tracking. It is generally accepted that session cookies are less offensive to individual’s privacy as they capture information on the website instantly and they are automatically deleted when closing the browser. Accordingly, the session cookies store information when the user is interacting with the website. The information stored on session cookies are typically navigation choices and preferences of the users. The law and market practices tend to consider session cookies as useful for a good navigation along a website.⁸

Contrary to session cookies, the persistent cookies remain when closing the browser and need to be deleted by the user or with a planned cleaning set up in the browser settings. The persistent cookies aim in general to collect identifying information, interests of the users navigating on a website, preferences and authentication information. They allow the connection between pragmatic information and a specific user, and they are reactivated *by design* when the user comes back to the website.

For these reasons, persistent cookies raise serious concerns from a privacy point of view. The knowledge accumulated within the cookies resulting from the users’ navigation and clicking on the URL of different webpages, targets users with personalized advertisements, tailored to the purported preferences and pattern of the behavior the user expressed on-line.

⁷ENISA, *Privacy considerations of online behavioural tracking*, (October 2012) available at <http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-considerations-of-online-behavioural-tracking>, 3.

⁸The e-Privacy Directive states that the obligation of confidentiality of the communications “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” (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, as amended by Directive 2009/136, art. 5 point 3).

To be noted that, in most cases, the way in which the company defines the parameters of information collection through cookies is a decisive factor for qualifying the cookie as really “privacy intrusive” or not. An example could help us illustrate this observation. Let us imagine a company using session cookies that instantly capture very basic details identifying an individual (e.g. the user name and password the user has used for registration on the website). Concurrently, the said company has foreseen that the data will be stored on such cookies in an encrypted form. On the opposite to that, another company displays on its website third party cookies that collect not only basic identifying information about a user but also more sensitive information, such as the number of the user’s credit card or the product purchases he effected on the site. In both cases, the same technology is used (cookies), but the way in which cookies are designed to capture information is different.

2.1.2.2 Javascript

When navigating on the Internet, many Javascript files are downloaded. These files can be used for first-party tracking and the information collected will be sent back to the servers.⁹ In terms of level of threat to privacy, Javascript files are comparable to first-party cookies. In addition, users can take action in order to block the storage of data collected by Javascript files.

2.1.2.3 Stateless Tracking

Without using cookies or other tracking technologies, web browser identification can be used as a tracking method.¹⁰ Indeed, web browsers provide information such as fonts, screen resolution, equipment used and the like, that may allow the recognition of a web browser amongst others. This tracking method, also called Browser Fingerprinting, is more difficult to block as it is particularly difficult to detect.¹¹

⁹ENISA, *Privacy considerations of online behavioural tracking*, (October 2012) available at <http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-considerations-of-online-behavioural-tracking>, 6.

¹⁰P. Eckersley, *How unique is your web browser?* (Privacy Enhancing Technologies, Springer Berlin Heidelberg, 2010) in *Consumer Privacy Law 2: Data Collection, Profiling and Targeting* (July 16, 2009, Law And The Internet, L. Edwards & C. Waelde, eds., Hart Publishing, 2009) available at <https://panopticklick.eff.org/browser-uniqueness.pdf>.

¹¹P. Eckersley, *How unique is your web browser?* (Privacy Enhancing Technologies, Springer Berlin Heidelberg, 2010) in *Consumer Privacy Law 2: Data Collection, Profiling and Targeting* (July 16, 2009, Law And The Internet, L. Edwards & C. Waelde, eds., Hart Publishing, 2009) available at <https://panopticklick.eff.org/browser-uniqueness.pdf>.

2.1.2.4 Supercookies and Evercookies

Over the years, users have taken into consideration the threats associated to their privacy by tracking techniques when navigating on a website. They have also been offered new applications that are designed to block cookies and delete them on a regular basis. Therefore, new means of tracking have emerged. Amongst these, new types of cookies have appeared: supercookies and evercookies.^{12,13,14}

Supercookies, also called Flash cookies are robust tracking mechanisms placed on a user's computer.¹⁵ Flash cookies are often linked and placed by Adobe Flash plug-in on websites. These cookies collect personal or technical information. As in other types of cookies, when supercookies are installed no specific notification is provided to users and they do not expire. What makes supercookies more "privacy-evasive" than the aforementioned other types of cookies is that, as they are located outside the browser's control, it makes it more difficult for the user to delete and control them.¹⁶

Evercookies is Javascript API that produces very powerful and persistent cookies, enabling the storage of cookie data in several types of storage mechanisms in the local browser.¹⁷ Because of their particular storage, Evercookies are therefore meant to remain, even when the standard and Flash cookies have been removed from the browser.¹⁸ Indeed, because they remain even after the user has deleted them, they clearly conflict with user's freedom and autonomy if the latter would wish to delete them.

2.1.2.5 Location Tracking

The geo-location plug-in installed on most of the popular browser and now installed on every smartphone, can be used as a tracking tool. On the basis of the user's consent, the browser shares information such as the IP address, the MAC address,

¹²ENISA, *Privacy considerations of online behavioural tracking*, (October 2012) available at <http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-considerations-of-online-behavioural-tracking>, 7.

¹³S. Schoen, *New cookies technologies: Harder to see and remove, widely used to track you* (2009) available at <https://www.eff.org/deeplinks/2009/09/new-cookie-technologies-harder-see-and-remove-wide>.

¹⁴Clause Castellucia, *Behavioral tracking on the Internet, a technical perspective*, in *European Data Protection: In Good Health?* (Springer Netherlands, 2012), 29.

¹⁵Soltani, Ashkan, et al., *Flash Cookies and Privacy* (AAAI Spring Symposium: Intelligent Information Privacy Management, 2010).

¹⁶Niklas Schmücker *Web Tracking* (Department of Telecommunication Systems, SNET2 Seminar, Paper-Summer, 2011).

¹⁷Samy Kamkar, *Evercookie – never forget* (October 2011), available at: <http://samy.pl/evercookie>.

¹⁸Claude Castellucia, *Behavioral tracking on the Internet, a technical perspective*, in R. Leenes, *European Data Protection in good health?*, 25.

and so on. Although a consent is asked to start this function, the users generally do not measure the impact of their consent and the frequency and accuracy of the localization performed.

Finally, users lose their location privacy, defined as “*the ability of an individual to move in public space with the expectation that under normal circumstances their location will not be systematically and secretly recorded for later use*”.¹⁹ Location privacy is considered as part of each individual’s privacy and is important to preserve. The concern here is that the new technologies enabling location tracking are becoming an increasingly widespread, cheap, easy, and accepted method to track users and collect valuable information.

2.1.2.6 Online Social Network Tracking

Social networks do not represent a particular “technology” or “tracking method” as the types of tracking techniques outlined above. Yet, online social networks constitute today an extremely popular trend encouraging people to stay continually “in contact”, “be watched” or “followed”. Surprisingly enough, such networks sometimes even promote the “tracking” as an asset of their website (for example, through an additional subscription fee, it could be possible for members to learn who other member looked at their personal details – like a cv – or who clicked on their profile to learn more about them).

Many users not only find this type of “tracking” trend normal but, all the more, they are seeking for it and are ready to pay extra to get it. On the other hand, there are social network members who usually consider the extra “tracking” features of social networking as “a necessary bad” that has to be tolerated, given that the privacy threats it entails are outweighed by the pleasure and other benefits resulting from users’ interaction on social networking sites.

This type of tracking uses users’ addiction to social networks in order to track every detail of the users’ every-day activities including those of their close family and friends. A number of heavily-used and well-known networks, such as Facebook,²⁰ Twitter,²¹ Pinterest²² and LinkedIn²³ have recourse to this on-line tracking technique.

Take the example provided by A. Roosendaal: *the Facebook Like Button*.²⁴ According to Facebook, this widget allows users to share their interests and

¹⁹A. Blumberg, and P. Eckersley, *On locational privacy, and how to avoid losing it forever*, available at <http://www.eff.org/wp/locational-privacy>, 1.

²⁰<http://facebook.com/>.

²¹<http://twitter.com/>.

²²<http://www.pinterest.com/>.

²³<http://www.linkedin.com/>.

²⁴A. Roosendaal, *We Are All connected to Facebook . . . by Facebook!* in *European Data Protection: In Good Health?* (Springer Netherlands, 2012).

preferences between them. However, the scope of this tool is far broader than what Facebook seems to tell. As explained by Roosendaal, when the users click on the Like button, a login field opens and requires the user to log in his Facebook account. After the user has logged in, a link will be created in the feed of news in Facebook and the network of the user will be able to see the content of the link. No need to be connected to an account to be tracked. The simple fact of visiting a website on which a Like button has been placed is sufficient to track Facebook members, and even non-members. Non-members can also be traced if they have already visited the social network website once. The scope is therefore enlarged to other subjects than the subscribers, and to other websites than the social media website. In addition, the awareness around this tracking technique is not very extensive and, therefore, the volume of data processed is incredibly high, which represents a very high financial value.

2.1.3 *Risks of On-line Tracking*

A major, common trend of some of the on-line tracking techniques discussed above is that the captured information is used for an array of intentions and purposes, predominantly for marketing reasons. It is rare that users are sufficiently aware of all the current, envisaged and potential (over time) uses of their data by the companies they are interacting with on the Internet. Yet, in our view, it is encouraging that some improvement can be noticed in this direction since the entry into force of the e-Privacy directive (as discussed below). Commercial and marketing agents have well understood the financial potential²⁵ of this knowledge and have built entire businesses on the potential of on-line behavioral tracking. Through the capturing and processing of different traces an internet user leaves on-line while visiting the same or different websites, companies are capable of creating user profiles.

Profiling is the recording and classification of behaviors. Although profiling has already been an intelligent marketing method based on information that can also be collected off-line (property and bank records, subscriptions selling, publicly available records, and so on), the Internet dynamics added an efficient, new dimension to it. Companies and on-line vendors can now track individuals *constantly*, and quite often, through a “voluntary” submission of personal information by the user to the network. Worse than that, many users consider the sharing of certain personal information through the internet as a “necessary bad” or a “societal necessity” (e.g., in order to adhere to a popular social network or to receive considerably

²⁵ “In 2011, Europe’s online advertising market grew 14.5 % year-on-year to a market value of €20.9bn in 2011. By comparison the overall European advertising market - excluding online - grew at just 0.8 % in the same time period”: See IAB, ADEX 2011, *Online Advertising in Europe* (6th edition): *Key Findings*, available online at http://www.iabeurope.eu/files/6613/6852/1900/2012_interact_presentation_final_delivered.pdf.

discounted offers by online vendors). Profiling in general has sparked an entire industry euphemistically labeled “Customer Relations Management” (CRM) or “Personalization”.²⁶ On-line profiling, in particular, has significantly expanded the sources for performing data correlations with a view to compiling users’ dossier of behavior, that may be correct but might even not. These dossiers of behavior may be used by marketers for target advertising but they can also be sold to governments for law enforcement or other government related purposes (national security, national defense and so on).

Moreover, today’s behavioral tracking techniques are so powerful that they allow to link anonymous data to specific individuals. The Like Button of Facebook is a good example. Marketing companies’ websites being in possession of named (true or not) profiles which are not properly secured, are more vulnerable to cyber incidents and data breach threats. It is probably not exaggerating to say that all these profiles could at the end be accessed by professional hackers, either to commit criminal acts against the profiled individuals or in their name by using their profile and identity.²⁷

Further, one of the ultimate objectives of the on-line behavioral tracking is the personalization of the website content presented to the users. Despite the well-intended purpose of method (gain in time, result-oriented web surfing, tailored content to the users’ needs), it is not always a given that the operator using automated web personalization through cookies knows better the user’s preferences and needs than the user himself. On the contrary, a user could arguably claim that, as he is automatically directed to content which is presumed to be of interest to him, he may miss the opportunity to look at other content which is useful to him or which becomes relevant because of a change in the person’s habits or way of living. At the end, the tracking technology restricts users’ freedom to look at “neutral” information being objectively communicated to all users.

2.2 On-line Tracking Under the Current Data Protection Legal Framework

On-line tracking as a market trend supported by specific technologies (as discussed above) falls under the applicability scope of the core data protection regulation currently in-force in Europe. We briefly outline below how the major rules and core foundations of the applicable data protection framework become relevant to on-line tracking. This means that, today, on-line tracking technologies are not developed and used in a legal vacuum as explained below.

²⁶Electronic Privacy Information Center, *Privacy and Consumer Profiling*, “The Product is you”, available at <http://www.epic.org/privacy/profiling>.

²⁷Along these lines, note the “@N” incident on Twitter: <http://arstechnica.com/security/2014/02/twitter-restores-50000-n-username-to-its-owner/>.

2.2.1 *Personal Data Protection Directive*

The processing of personal data by the use of on-line behavioral techniques as the ones referred above is subject to the requirements of the general EU Data Protection Directive (Directive 95/46/EC, herein the “Data Protection Directive”). The cornerstone principles of this directive must be observed and applied effectively by the parties involved in on-line tracking. Besides the citizen being the party who can benefit from the protection of this law, other parties concerned are: i) vendors of such on-line tracking technologies (software/hardware companies) and ii) the implementers of such applications (advertising and market research companies, as well as any other company wishing to reap up the benefits of such technologies for their own marketing and selling activities or other purposes).²⁸

On top of the Data Protection Directive, another EU legal act specifies the requirements of the processing of personal *data in the electronic communications sector (EU Directive 2002/58 as amended)*. One of the major changes brought by the latter Directive, the so-called e-Privacy Directive, tackled a core aspect of the subject matter under discussion here, namely the type of consent that should be obtained from the individual subject to on-line tracing techniques, including on-line behavioral tracking.

Specifically, current Article 5 §3 of the e-Privacy Directive reads:

*Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed **on condition that the subscriber or user concerned has given his or her consent**, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.*

In the same vein, Recital 66 of the directive which introduced the latest amendments to the e-Privacy Directive,²⁹ stressed the importance for users to be provided with clear and comprehensive information when engaging in an activity which could result in behavioral tracking. In the same Recital, it is emphasized that the methods of providing information and offering the right to refuse should be as user-friendly as possible.

Although the aspect of user notice (consent) has appeared to be probably the biggest challenge in the interpretation of the revised e-Privacy directive (see below, Sect. 2.2.2.4), the other privacy foundations as enshrined into the Data Protection Directive are also worthy of commenting.

²⁸To note that the “on-line” tracking market is quite sophisticated and other market actors besides the categories cited here (vendors of on-line tracking tools and the companies involved in on-line tracking) may also be subject to data protection rules.

²⁹*Supra*, footnote 8.

2.2.2 Applicability of the Core Foundations of Personal Data Protection

2.2.2.1 Purpose Limitation

Personal data must be collected for a purpose defined in advance.³⁰ With regard to on-line tracking tools, the purpose for collecting data must be legitimate. The collection and storage of data must then be aligned with the defined purpose.³¹ In addition, the collection of data cannot override the purpose for which the on-line user has given his consent.³² Let us take as example the privacy statement published on the website of a market research organization explaining that, while it uses on-line tracking tools, the captured data will only be used to build up statistics on the number of visits that “hit” the website. If the market research company then uses the data for another purpose that is not directly linked to verifying the initial purpose, for example in order to sell those data to a number of companies interested in sending their on-line surveys to new prospects, then the “purpose limitation” rule has clearly been infringed.

2.2.2.2 Data Subject Notice

This requirement sets forth the obligation of the data controller to provide clear information to the internet users about the collection and processing of their personal data.³³ The requirement is directly relevant to on-line monitoring activities, especially because a great part of the data processing operations is “invisible” to the individual. Moreover, on-line monitoring often involves many actors, meaning the company interacting with the individual but, very often, the “processor” who will analyze and correlate the data by using marketing intelligence or other techniques and probably other data “recipients”. It is a general but correct perception that on-line activities increase by definition the risk that the data will be spread around with no ultimate control from the end-user.

2.2.2.3 Proportionality

Personal data must be adequate, relevant, and not excessive in relation to the purposes for which they are collected and/ or further processed. Let us take again

³⁰ Article 6 of Directive 95/46/EC.

³¹ Article 6(1)(b) of Directive 95/46/EC.

³² Article 29 Data Protection Working Party, Opinion 2/2010 on online behavioural advertising, adopted on 22 June 2010, 00909/10/EN WP 171, p. 20.

³³ Article 10 of Directive 95/46/EC.

the example of the market research organization referred to above. In the company's privacy statement there is no word about whether the company is using personally identifiable information or other forms of data (aggregate, de-identified, etc.) to achieve the purpose of data collection. However, in the light of the purpose formally mentioned in the privacy statement (checking the number of visits on the website), one can easily understand that the company in question does not need to process personal data. On the contrary, to attain the declared purpose, the market research company is even obliged to use on-line monitoring means and techniques which will enable it to track users anonymously, thus without having to know exactly the person (or an identifier of him) being behind each "click" on the company's website. There are many on-line tracking applications which are designed, or could be reconfigured, in order to collect data only on an aggregate level. Such method of using aggregate information instead of personal identifiers or other personal data could be used in our example here to align with the proportionality principle.

2.2.2.4 Obligation to Obtain Prior Consent

The consent rule practically means that the implementers of the on-line tracking tools must seek to obtain the prior acceptance of the on-line user before any tracking begins.³⁴

There are many ways to collect consent, and to, *a priori*, meet the requirements of article 5(3) of the Directive. Nevertheless, the practice and doctrine have demonstrated that the concept of consent as stated in the Directive is not very clear and requires further developments.³⁵

Pursuant to article 5(3), the consent should be obtained after having informed the data subject on the nature and purpose of the collection. Adapted to the use of tracking tools, this means that the subject should be informed prior to the placement of tools intended to collect information on individuals navigating in the World Wide Web.

In practice, many techniques have emerged to meet the requirements of consent. Yet, not all of them are necessarily in line with the legal prerequisite of consent as laid down in the e-Privacy Directive. In its opinion on on-line behavioral advertising, the Article 29 Working Party provides an interpretation of the notion of "consent" as meant in the latter Directive. In the same opinion, the Article 29 Working Party attempts to lay the foundations of a correct interpretation of the obligation to obtain prior and informed consent.³⁶

³⁴Article 5(3) of Directive 2002/58/EC.

³⁵Matthew S. Kirsch, *Do-Not-Track: Revising the EU's Data Protection Framework to Require Meaningful Consent for Behavioral Advertising*, (XVIII RICH. J.L. TECH. 2) available at <http://jolt.richmond.edu/v18i1/article2.pdf>, 12-18.

³⁶Article 29 Data Protection Working Party, Opinion 2/2010 on online behavioural advertising, adopted on 22 June 2010, 00909/10/EN WP 171, 12-17.

Consent Obtained by Browser Settings

According to the Article 29 Working Party, a consent obtained by means of browser settings is not sufficient under the law. Obtaining the consent by way of the browser settings relies on the placing of cookies as default. If the user does not turn the cookie function off, the default configuration remains intact, implying that the user has consented to the cookie given that he has not actively prompted to change the browser settings (although he was given the information to do so). Such “consent” obtained “by default” has been questioned by the European regulator.

Consent Given by Opt-out Mechanisms

Service providers are increasingly using opt-out mechanisms enabling users to refuse receiving target advertising. Although we can recognize the benefits of this approach, the mechanism is not adequate and sufficient as a way to obtain informed consent.³⁷ First, the lack of users’ awareness of users is tricky, as many of them do not know where to opt-out despite the fact that they may be given the possibility to do so. Second, when the user does not opt-out, the provider will consider this as an implicit consent. However, the consent should be derived from an affirmative action of the user, and not from inaction.

Prior Opt-in Consent

The Article 29 Working Party has interpreted the article 5(3) in a strict way: the user should first be provided with information on the processing in general and, second, consent to the processing and collection of data. These two conditions are cumulative. It must be given prior to the processing.³⁸ Furthermore, the consent should be the result of an affirmative action of the users. In addition, the consent should be considered as valid only for a limited period of time. Finally, the on-line users should be given the possibility to revoke their consent easily.

2.2.2.5 Data Destruction/Retention

This requirement basically means that any personal data that have been collected and used throughout the on-line tracking operations must at the end be destroyed,

³⁷Article 29 Data Protection Working Party, Opinion 2/2010 on online behavioural advertising, adopted on 22 June 2010, 00909/10/EN WP 171, p. 15.

³⁸E. Kosta, *Peeking into the cookie jar: the European Approach towards the regulation of cookies*, (International Journal of Law and Information Technology, vol. 21, No 4, 2013), 392.

at least when they are no longer needed for achieving the purpose of data collection or at a shorter time period (that has to be defined by the company using the tracking technique).

Data retention associated with on-line tracking methods is even more challenging than other more ordinary forms of data processing. Let us imagine the market research company of our example above, attempting to meet practically the data destruction/retention requirement while the purpose of data collection is now user profiling. Having this new purpose in mind, the company has deployed a tracking technique online (based on certain observer tags or cookies for example). In this case, these data are precisely collected now with the intention to be used for long time-periods. Especially in cases where those data will form the data repository (or “stock”) against which new data from “new” users, will continue to enter and will require correlation. Thus, the more data the company has, the more chances it has to mix correctly all these data and form more “accurate” profiles. It is quite common that companies like this of the example will use aggregate or anonymous data especially if the storage entails data retention for a long period of time. Yet, in case that, the company of the example, probably assisted by specialist service providers achieves to correlate the data at a later point of time with individual users, namely to re-identify individuals, there is very little likelihood and only when specific conditions are fulfilled,³⁹ that such correlation activity will be compliant with data protection rules. Second, even if the company finds out satisfactory ways to achieve its purpose while meeting the data destruction requirement (which is technically possible), another challenge it may have to encounter is how controlling that the range of service providers it cooperates with in order to implement the profiling technique, to map data and adduce conclusions of such mapping. The situation becomes more complex if the market research organization in question may request services from a cloud provider which will, for example, provide data repository services or will help in data analysis and users’ clustering in specific profiles.

At the end, the market research company will have to ensure that appropriate data deletion and retention practices have been implemented not only by itself but also from the range of providers mentioned above.

2.3 Future Personal Data Protection Framework: How Will It Affect Behavioral On-line Tracking?

In order to address efficiently the challenge of personal data protection in view of the economic, market, and technological challenges since the adoption of the Data Protection Directive (1995), a reform of the regulatory framework is now underway.

³⁹Such as clear and specific notice to user and consent.

Accordingly, a proposal for a new Data Protection Regulation likely to replace the Data Protection Directive is now under negotiation for adoption by the European Parliament and the Council.⁴⁰

The basic motives of the EU regulators' decision to reshape the current data protection regulation are directly relevant to the topic of this article: according to Recital 5 of the new act under discussion, "...*the scale of data sharing and collecting has increased spectacularly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Individuals increasingly make personal information available publicly and globally*".

Although the adoption of the new draft is not certain yet and despite the fact that the content of the draft under discussion here will in all likelihood still change, it is widely admitted that a regulatory reform in the area of personal data protection is necessary and must continue. Based on this assumption, we summarize below a few elements of the proposed Data Protection Regulation (herein "Regulation") which, in our view, if they are adopted, they will have a significant impact on the way on-line tracking technologies and all the market actors behind it (designers, vendors, and implementers) will have to deploy such technologies in the future.

The points of attention listed below are not exhaustive although, in our opinion, they depict noticeable changes if they come through:

2.3.1 Scope of Application

It often happens that companies not established in Europe are those conducting on-line tracking. Under the current application scope of the Data Protection Directive, such companies are highly likely to escape the rigorous European privacy rules, especially if it is difficult to demonstrate that the means used to process the personal data are established in Europe. To change this, the Regulation suggests that non-based EU companies (be controllers or processors) will henceforth be subject to the controls and requirements set forth in the new legislative framework insofar as they perform activities related to "*the monitoring of data subjects*".⁴¹ It is the first time that primary regulation in Europe renders the monitoring (including the on-line one) as a sufficient element *per se* to decide on the applicability of the European privacy laws. In addition, the Regulation sheds some more light into the activities that one may take into account to determine whether a company performs *monitoring*.

⁴⁰Proposal for a regulation of the European Parliament and of the Council on the protection of individual 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). To be noted: this version of the draft act may not be the most recent one at the time this article will be published.

⁴¹*Supra* reference 41, art. 3 "*Territorial Scope*", §2, (b).

Therefore, any technique consisting of applying a “profile”, particularly in order to take decisions concerning a person or for analyzing or predicting such person’s personal preferences, behavior or attitude fall under the scope of “monitoring”.⁴²

In our view, this is a considerable change clearly demonstrating that on-line tracking was one of the key factors taken into account to decide on the need of legislative reshuffling.

2.3.2 Definitions

Another element reaffirming the intention of the regulator to confirm that the privacy rules will be relevant to any type of monitoring and profiling affecting individual’s privacy is the new definition of “profiling” currently inserted in the new text. Accordingly, profiling is defined as “*any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person or to analyse or predict in particular that natural person’s performance at work, economic situation, location, health, personal preferences, reliability, or behaviour*”.⁴³

We infer from the new text, that data mining and data correlating methods enabling the evaluation, analysis, or forecasting of any parameter of the economic, social, and working life of an individual; as well as of any aspect of his personality (interests, preferences, etc.) may be caught by this definition of “profiling”. More precisely on on-line tracking tools, the Regulation explicitly mentions that “cookie identifiers” (as well as RFID tags) should be considered as personal data eligible for protection under the EU privacy regulatory framework on condition that such identifiers relate to identified or identifiable natural person.⁴⁴

2.3.3 Consent

The requirements around the consent, representing probably the most critical factor of legitimizing on-line tracking and profiling techniques, become stricter under the Regulation. Although the main conditions for recognizing that the consent provided is valid do not change in essence (freely-given, specific, and informed), the proposed text sets forth explicitly that mere use of a service or inactivity should not constitute a valid consent.⁴⁵ On this point, the Regulation seems to be consistent with the conditions set forth on the e-Privacy Directive and the market practice that is now being shaped around the implementation of such cookies’ consent, requesting an

⁴² *Supra* reference 41, Recital 21.

⁴³ *Supra* reference 41, art. 4 “Definitions”, §3a.

⁴⁴ *Supra* ref. 41, Recital 24.

⁴⁵ *Supra* ref. 41, Recital 25.

affirmative action of the on-line user (be it through clicking on an “I accept” or “ok” box on a website banner or by use of another technique) before installing the tracking application. In consequence, pre-configuration of the browser settings so that cookies are installed unless the individual opts out do not appear to be in-line with the “affirmative” action that the notion of “consent” as confirmed by the Regulation seems to request.⁴⁶

If the current language of the Regulations’ text over the user’s consent is adopted the notion of consent through an action (as set forth in the e-Privacy directive) will be reinforced.⁴⁷ Consequently, companies deploying on-line tools on their websites will increasingly be obliged to promote solutions explicitly supporting an “action” from the individual who agrees to be subject to tracking. If this element is considered as a confirmation of prerequisites already set forth in current laws (e-Privacy directive), an innovative element of the Regulation concerns the burden of proving that a valid consent has been provided. According to the Regulation’s text under adoption, in case that the individual subject to tracking questions the mechanism through which he provided his consent, it will be the controller who will have the obligation to demonstrate that the said individual has indeed provided his consent.⁴⁸

Another innovative element is that, for the first time, an EU primary law on privacy will emphasize explicitly the conditions that should be fulfilled to accept that the consent given by a child is valid. This is particularly relevant when we talk about internet usage, knowing how many children are using the internet today and, hence, how vulnerable they could be to on-line tracking techniques. Under the Regulation, it seems that children above 13 are considered mature enough to provide valid consent, whereas, the consent of the parent or guardian is requested for children under 13.⁴⁹ Although one could argue about the practical effect of such provision (which might mean practically that a clear “opt in” by parents is requested for children to be able to continue navigation on a website), it is already a positive sign that the new rules recognize that children merit more special attention than adults when they have to make a choice affecting their privacy.

⁴⁶The fact that browser settings are not yet sophisticated enough to secure by themselves a user’s affirmative action has been stressed in many recommendations of Member States’ privacy oversight bodies, such as the Information Commissioner’s Office in the UK (ICO). In a recent guideline provided on the use of cookies of ICO, it is mentioned that “*For consent to be clearly signified by the browser settings it would need to be clear that subscribers had been prompted to consider their current browser settings and, had either indicated in some way they were happy with the default, or have made the decision to change the settings*”, Information Commissioner’s Office, *Guidance on the rules on use of cookies and similar technologies* (May 2012, v. 3, p. 15). In the same vein, the Regulation states that “*the use of default options which the data subject is required to modify to object to the processing, such as pre-ticked boxes* (or, we infer, browser settings – our addition -) *does not express free consent* (Supra ref. 41, Recital 33).

⁴⁷It is noteworthy that the Regulation seems to introduce a new right of the data subject, being the right to object to profiling (Supra ref. 41, art. 10a “*General principles for data subject rights*”, §2.

⁴⁸Supra ref. 41, Recital 7 “*Conditions for Consent*”, §1.

⁴⁹Supra ref. 41, Recital 29.

2.3.4 Notice

In the same vein as the requirements around consent, the Regulation seems to strengthen the conditions regarding the information data controllers must provide to the data subjects about the processing of their personal information.

First, the Regulation explicitly requests data controllers to communicate appropriate *policies* informing the data subjects about how their personal information is handled. This requirement means primarily that data controllers shall draft in a clear and user-friendly language relevant personal data protection policies.⁵⁰ For internet users, it is particularly interesting that the new text requires now explicitly that such policies are easily accessible (for example, through an obvious, catchy to the eyes, reference on the company's website) and drafted in clear and plain language. What is more noteworthy is that the Regulation makes an explicit reference to on-line advertising requesting companies involved in such practices to clearly indicate to the on-line users if personal data are collected, by whom and for what purposes.⁵¹ In particular, websites addressed to children must communicate in a language that children can understand the above elements.

Second, in order to ensure that the minimum requirements of a data protection policy are covered in the documentation that all controllers will be providing to data subjects and this in a consistent and concise language, the Regulation suggests the adoption of a series of particulars.⁵² It will be quite interesting to follow how the mandatory content of policies as meant by the EU regulator (i.e., the adoption of the specific particulars set forth now in the Regulation) will consistently be followed by the market practice. This will probably be even more challenging for non-EU based companies, such as the ones active in on-line tracking and profiling that as noted above, will become subject to the requirements of this Regulation. Such foreign companies will in all probability not have similar "notice standards" (particulars) in the country where they are based.

Third, it is particularly relevant to the context discussed herein, that the EU regulator envisages extending the scope of information that should be communicated to the data subjects to include, *"where applicable, information about the existence of profiling, of measures based on profiling, and the envisaged effects of profiling"*

⁵⁰Yet, in our interpretation, the Regulation covers indirectly the adoption of other internal regulations and policies, except from the data protection policies, if these would be relevant to the protection of personal information too (e.g., documentation relevant to the security of information, data classification, confidential information and so on).

⁵¹*Supra* ref. 41, Recital 46 reads: "...*This (the principle of transparency – our addition) is particularly relevant where in situations, such as online advertising, the proliferation of actors and the technological complexity of practice makes it difficult for the data subject to know and understand if personal data relating to them are being collected, by whom and for what purposes*".

⁵²It appears that the current draft of the Regulation requests the adoption of specific graphical forms showing whether personal data are collected, stored, shared with other parties and so on, that would be made easily visible and clearly legible on a website. *Supra* ref. 41, article 13a and Annex 1.

on the data subjects; . . .".⁵³ This is a real novelty introduced by the Regulation. If this phrasing is finally maintained in the adopted text, this requirement may considerably change the content and level of detail in the majority of the privacy notices and statements that companies currently publish on their websites to inform their customers of on-line profiling, tracking, and behavioral monitoring activities. In most of the cases today, it is a common (and we would even say, widely acknowledged practice) to apply very general and all-inclusive language in order to describe on-line tracking activities. Thus, standard *language* is often used by service providers, such as that cookies are used "*to enhance the user's experience on the website*" or "*for marketing purposes*" or to "*improve the quality of the (provider's) website*", and so on. Such type of wording may not be sufficient anymore when the new law comes into force.

Finally, relevant to the notice requirement is the new right formulated in the Regulation with regard to end-user's objection to profiling. Accordingly, the user shall be informed about the right to object to profiling in a *highly visible manner*.⁵⁴

2.3.5 The Right of Erasure ("Right to Be Forgotten")

Besides the rule of data destruction (outlined above, Sect. 2.2.2.5), the Regulation introduces a new right of the data subject/user, being the right to demand from the data controller that he deleted the user's personal data or, more relevant to the on-line activities, *that the data controller stops copying or replicating* such data.⁵⁵ Relevant to the example of the market research company referred to above (Sect. 2.2.2.5), according to the new text, the data controller shall also take *all reasonable steps* to ensure that third parties having received the user's data will erase them accordingly. Moreover, if possible, the data controller will have the obligation to inform the on-line user of the action third parties have taken to align with this requirement.⁵⁶ Yet, the Regulation provides a number of derogations to the obligation to erase the personal data, which may actually be used in the case of on-line profiling/monitoring too. Indicatively here, if the controller needs to keep the personal data for evidence purposes or if the storage application used does not technically allow data erasure, it will be possible to archive those data and not satisfy the user's request of erasure. The requirements that should be fulfilled for the archiving of the collected personal data in this case are spelled out in the Regulation.⁵⁷

Some discussion of the problems that might arise here is advised.

⁵³Supra ref. 41, art. 14, new letter (ga).

⁵⁴Supra ref. 41, art. 20, §1.

⁵⁵Supra ref. 41, art. 17, §1.

⁵⁶Supra ref. 41, art. 17, §2.

⁵⁷Supra ref. 41, art. 17, §4.

2.3.6 Data Protection “by Design”

The new concept of data protection “by design” as introduced in the Regulation will oblige both data controllers and processors to ensure that they will implement appropriate technical and organizational measures and procedures to protect the personal information. The time for choosing the appropriate measures and procedures should be the time at which the purposes and the means of the data processing operation are determined, as well as the time at which the said processing starts.

The privacy by design principle is one of the most innovative elements of the Regulation: “*this approach transforms consumer privacy issues from a pure policy or compliance issue into a business imperative*”.⁵⁸ According to this requirement, privacy concerns should be incorporated in the design phase of new information technologies, business practices, and networked infrastructures. As the famous quote “better preventing than curing”, business should focus on privacy during the entire lifecycle of the management of personal data and should implement safeguards in order to protect those data.

In the context of on-line tracking techniques, the concept of “data protection” by design is particularly pertinent. Threats and risks that a specific “intelligent” on-line application may entail to the user’s privacy shall be determined from the design phase of the tool once the purposes of the envisaged data tracking and the technical options to achieve those are formed. At the end, the “data protection” by design will not only affect tracking technology implementers (i.e., companies implementing the tool and other parties supporting it in the implementation or the data analysis, etc.) but also the designers (and probably vendors) of such tools. This is because, in order to satisfy the requirement put upon them, the data controller and/or processor will have to ensure that: a) the design of the on-line tracking tool can be technically adjusted to fit the data processing purpose and the controls that will be put in place and b) “privacy protection” requirements have been considered right from the phase of product conception in order to avoid costly adjustments and changes at the implementation phase.

2.3.7 Towards a “Privacy Friendlier” Internet Tracking: The Role of Society, (Social) Media and Education

The provisions of the New Regulation outlined above constitute only a limited part of many provisions that will potentially have an impact on the deployment of on-line tracking technologies and the way the designers and users of such technologies

⁵⁸Cavoukian A., *Privacy by Design in Law, Policy and Practice, A White Paper for Regulators, Decision-makers and Policy-makers*, (August 2011, Information and Privacy Commissioner, Ontario, Canada) available at <http://www.ipc.on.ca/images/Resources/PbDBook-From-Rhetoric-to-Reality.pdf>, 13.

will process personal data captured through them. Some more examples of legal measures that will affect companies' conducting profiling/on-line activities are for example: the definition of high fines' scales to sanction data protection infringements or the obligation to conduct privacy impact assessments before the implementation of a technology or project which may be threatening to individuals' privacy or the mandatory designation of personal data protection officers in data processing environments. At the time of drafting this article, the relevant articles of the Regulation are being reviewed meticulously and their exact scope may change.

Should however regulation be perceived as a "panacea" to the exponential growth of on-line tracking trends in our society? Definitely, no. The letter of laws is never a solution *per se* if such laws are not accompanied by measures that can effectively raise awareness about the problems explaining their adoption and on how the rules should be interpreted in practice. Let us also not forget that for a legal measure to be effective, it is necessary that the societal actors concerned accept at the end the "*raison d'être*" of the act and implement the rules effectively.

Translating the above experience in the case of "on-line" tracking, means that besides the regulators' intention to provide enhanced data protection through a stringent legal framework, there is a lot more that needs to be done to objectively educate users about the opportunities and risks entailed while surfing on the internet. If social networking is a "privacy-evasive" trend of today's society, it can also be transformed into a very powerful tool to promote privacy and educate users. Along the same lines, self-regulatory approaches, and other initiatives encouraging the private-public dialogue, as well as standardization work could help market stakeholders and public interest bodies to take actively part in the way the new or amended data protection framework should be interpreted. European institutions and agencies, but also public-private initiatives at country level, could be the instigators of such dialogue that would require academy and data protection oversight bodies to engage in it actively.

If regulatory reforms are difficult to be launched and their concrete effects become many times visible only in the long term, soft regulation and societal initiatives may prove to be more efficient on condition that they are coordinated well and motivate market stakeholders to participate.

2.4 Conclusion

The current European legislation, namely the Data Protection Directive and the e-Privacy Directive (after its last revision) constitute the basic legal framework for the protection of the privacy of on-line users when they become subject to on-line tracking techniques. If the new Regulation on personal data protection is finally adopted without major changes to the latest draft published, the manufacturing and design industry of behavioral tracking tools, as well as the companies that implement on-line tracking technologies, will be encountered with stricter requirements in terms of personal data protection. To summarize, these requirements mainly refer to the adoption of documentation, procedures, and controls that companies active in

the design phase or using on-line tracking applications will have to create or update. The Regulation seems to recognize explicitly that data collection and processing through tracking techniques pose major threats to citizen's privacy. Therefore, it sets forth new rights of the data subject particularly relevant to on-line activities (right to data erasure, right to object). Finally, the Regulation's text in the current version attempts to switch the "mindset" of designers, controllers and processors to better "predict" privacy than "remedy" privacy, by introducing the core principle of data protection "by design".

It is however the view of the authors that, in practical terms the new (and probably, more rigorous) legal imperatives will not bring the desired change if the perception of the individuals around the fancy "on-line" tools they are offered today to facilitate their integration in the modern society does not change. Additional and stricter regulatory conditions will not be sufficient without sensitizing business about the importance of implementing controls and procedures towards their software vendors and the need for strengthening the privacy contractual guarantees in the services agreements they have with them. Moreover, this also means that some extra effort should be taken to educate on-line users, especially those of young age, of what they should avoid and dare refuse on the internet.

Other initiatives stemming from the public interest stakeholders, as well as professional organizations, could serve as an efficient remedy to today's exponential and abusive on-line tracking of citizens. Dedicated self-regulation on this subject matter, awareness campaigns for citizens to introduce self-defense tools (a number of those are available on the market today⁵⁹), more education about citizens' rights and the recourse mechanisms available in case of infringements could be some other supplementary ways, next to the law, to render citizens' right to control their data meaningful and enforceable in practice.

Bibliography

Academic Sources

- Blumberg A. and Eckersley P. *On locational privacy, and how to avoid losing it forever*. Available at <http://www.eff.org/wp/locational-privacy>.
- Cavoukian A. *Privacy by Design in Law, Policy and Practice, A White Paper for Regulators, Decision-makers and Policy-makers*. August 2011. Information and Privacy Commissioner, Ontario, Canada. Available at <http://www.ipc.on.ca/images/Resources/PbDBook-From-Rhetoric-to-Reality.pdf>.
- Castellucia C. *Behavioral tracking on the Internet, a technical perspective*. In *European Data Protection: In Good Health?* Springer Netherlands, 2012.
- Eckersley P. *What does the "Track" in Do Not Track Mean?* 19 February 2011. Electronic Frontier Foundation. Available at <https://www.eff.org/deeplinks/2011/02/what-does-track-do-not-track-mean>.

⁵⁹ENISA, *Privacy considerations of online behavioural tracking*, October 2012, available at <http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-considerations-of-online-behavioural-tracking>, 18.

- Eckersley P. *How unique is your web browser?* 2010. Privacy Enhancing Technologies, Springer Berlin Heidelberg. In *Consumer Privacy Law 2: Data Collection, Profiling and Targeting*. July 16, 2009. Law And The Internet. L. Edwards & C. Waelde, eds., Hart Publishing. Available at <https://panopticklick.eff.org/browser-uniqueness.pdf>.
- Goldberg I., Wagner D., Brewer E. *Privacy-enhancing Technologies for the Internet*. 1997. Proceedings of IEEE COMPCON '97. Available at <http://www.cs.berkeley.edu/~daw/papers/privacy-compcon97.ps>.
- Hildebrandt M. *Profiling: from data to knowledge*. 2006. DuD: Datenschutz und Datensicherheit 30.
- Kirsch Matthew S. *Do-Not-Track: Revising the EU's Data Protection Framework to Require Meaningful Consent for Behavioral Advertising*. XVIII RICH. J.L. TECH. 2. Available at <http://jolt.richmond.edu/v18i1/article2.pdf>.
- Kamkar S. *Evercookie – never forget*. October 2011. Available at: <http://samy.pl/evercookie>.
- Kosta E. *Peeking into the cookie jar: the European Approach towards the regulation of cookies*. 2013. International Journal of Law and Information Technology, vol. 21, No 4.
- Roosendaal A. *We Are All connected to Facebook . . . by Facebook!* in Gutwirth S., Leenes R., de Hert P., Pouillet Y. (Eds.). *European Data Protection: In Good Health?* 2012. Springer Netherlands.
- Schmücker N. *Web Tracking*. 2011. Department of Telecommunication Systems, SNET2 Seminar, Paper-Summer.
- Schoen S. *New cookies technologies: Harder to see and remove, widely used to track you*. 2009. Available at <https://www.eff.org/deeplinks/2009/09/new-cookie-technologies-harder-see-and-remove-wide>.
- Soltani A. et al. *Cookies and Privacy*. 2010. AAAI Spring Symposium: Intelligent Information Privacy Management.
- Swaminatha T. M. *Privacy Enhancing Technology*. Privacy Enhancing Technology. Guidelines and Testing Methodology, W3C/QA Position Paper. Available at <http://www.w3.org/2001/01/qa-ws/pp/tara-swaminatha-cigital.html>.

Business Sources

- Article 29 Data Protection Working Party, Opinion 2/2010 on online behavioural advertising, adopted on 22 June 2010, 00909/10/EN WP 171.
- Electronic Privacy Information Center. *Privacy and Consumer Profiling, "The Product is you"*. Available at <http://www.epic.org/privacy/profiling>.
- ENISA, *Privacy considerations of online behavioural tracking*, (October 2012) available at <http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-considerations-of-online-behavioural-tracking>.
- Geuss M. *Twitter restores \$50,000 @N username to its owner. A simple social engineering attack list Naoki Hiroshima a very valuable handle*. 26 February 2014. Available at <http://arstechnica.com/security/2014/02/twitter-restores-50000-n-username-to-its-owner/>.
- IAB, ADEX 2011, *Online Advertising in Europe (6th edition): Key Findings*, available at http://www.iabeurope.eu/files/6613/6852/1900/2012_interact_presentation_final_delivered.pdf.

Regulator Sources

- Communication from the Commission to the European Parliament and the Council on promoting data protection by privacy-enhancing technologies. COM(2007)228 final. Available at <http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52007DC0228&from=EN>.
- 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. COM/2010/0609 final. Available at <http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52010DC0609&from=EN>.

- 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). OJ L 201, (31.07.2002).
- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive). OJ L 281, (23.11.1995).
- Draft report on the proposal for a regulation of the European Parliament and of the Council on the protection of individual 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). Available at http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/922/922387/922387en.pdf.
- Information Commissioner's Office. *Guidance on the rules on use of cookies and similar technologies*. May 2012. Available at http://ico.org.uk/~media/documents/library/Privacy_and_electronic/Practical_application/cookies_guidance_v3.pdf.
- Proposal for a regulation of the European Parliament and of the Council on the protection of individual 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). Available at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.
- Study on the economic benefits of privacy-enhancing technologies (PETs), Final Report to The European Commission DG Justice, Freedom and Security, Prepared by London Economics, July 2010. Available at http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_pets_16_07_10_en.pdf.

Reforming European Data Protection Law

Gutwirth, S.; Leenes, R.; de Hert, P. (Eds.)

2015, XX, 406 p. 30 illus., 16 illus. in color., Hardcover

ISBN: 978-94-017-9384-1