novática
Revista de la Asociación de Técnicos de Informática

Novática, founded in 1975, is the oldest periodical publication amongst those specialized in Information and Communications Technology (ICT) existing today in Spain. It is published by **ATI** (*Asociación de Técnicos de Informática*) which also publishes **REICIS** (*Revista Española de Innovación, Calidad e Ingeniería del Software*).

<http://www.ati.es/novatica/>
<http://www.ati.es/reicis/>

ATI is a founding member of **CEPIS** (Council of European Professional Informatics Socities), an organization with a global membership of above 200,000 European informatics professionals, and the Spain's representative in **IFIP** (International Federation for Information Processing), a worldwide umbrella organization for national societies working in the field of information processing. It has a collaboration agreement with **ACM** (Association for Computing Machinery) as well as with **AdaSpain**, **AI2**, **ASTIC**, **RITSI** and **Hispalux** among other organisations in the ICT field.

Editorial Office, Advertising and Madrid Office
Plaza de España 6, 2ª planta, 28008 Madrid
Tlfn.914029391; fax.913093685 <novatica@ati.es>
Layout and Comunidad Valenciana Office
Av. del Reino de Valencia 23, 46005 Valencia; Tlfn. 963740173 <novatica_prod@ati.es>
Accounting, Subscriptions and Catalonia Office
Via Laietana 46, ppal. 1ª, 08003 Barcelona
Tlfn.934125235; fax 934127713 <secregen@ati.es>; <novatica.subscripciones@atinet.es>
Aragon Office
Lagasca 9, 3-B, 50006 Zaragoza Tlfn./fax 976235181 <secreara@ati.es>
Andalucía Office <secreand@ati.es>
Galicia Office<secregal@ati.es>
Advertising Plaza de España 6, 2ª planta, 28008 Madrid.
Tlnf.914029391; fax.913093685 <novatica@ati.es>
Legal deposit: B 15.154-1975 -- ISSN: 0211-2124; CODEN NOVAEC
Cover Page: Dancing House - Concha Arias Pérez / © ATI
Layout Design: Fernando Agresta / © ATI 2003

Special English Edition
2012/2013 Annual Selection of Articles

summary

Cristina Blasi Casagran[1], Eduard Blasi Casagran[2]
[1]Researcher at the European University Institute, Florence (Italy); [2]Lawyer at Prodat, Barcelona (Spain)

<cristina.blasi@eui.eu>, <eblasi@prodatcatalunya.com>

Google: Navigating Security, Rights to Information and Privacy

Abstract: *In the last few years, the rapid development of new technologies and the expansion of the Internet have required multinational businesses to adapt to both national and international laws accordingly.. Thus, companies like Google, Inc. (which today are leading the net) collect and process huge amounts of personal data on a daily basis, without specific legislation to combat the current loopholes in such practices. This study analyses a number of controversial issues related to Google. First, it examines the increase in behavioural advertising, highlighting the potential impact that recent proposals in both the EU and the US could have on this form of advertising. Likewise, it studies the so-called right to be forgotten according to the EU proposal for a General Data Protection Regulation, as well as the impact that this right could have on Google. It then examines the controversy stemming from the blurry dividing line between data collected and processed by private companies (e.g. Google) for commercial purposes, and data processed by public agencies for law enforcement purposes. Finally, the study refers to the new Google privacy policy, which came into force in March 2012. The above areas of inquiry seek to illustrate the enormous power Google has at its disposal with respect to processing internet users' personal data. As such, Google could have a major role in determining global legislative issues such as defining the borders between privacy, rights to information, and collective security.*

Keywords*: Behavioural Advertising, Collective Security, Data Protection, Google, Law Enforcement, Privacy, Right to be Forgotten, Right(s) to Information.*

Authors

Cristina Blasi Casagran is currently a PhD Researcher at the European University Institute (Florence, Italy) on "*The External Dimension of the Area of Freedom, Security, and Justice. Data Protection within the framework of the external relations*". She has previously obtained an LL.M in European Law at Europa Institut (Universität des Saarlandes Germany), an M.A in European Integration at the Institut Universitari d'Estudis Europeus, and a law degree from the Universitat Autònoma de Barcelona. She carried out apprenticeships in the Legal Service of the European Commission, as well as in the Office of the European Data Protection Supervisor.

Eduard Blasi Casagran is a specialised lawyer in data protection and new technologies from Prodat (Barcelona Area, Spain). He is also a member of the Asociacioìn Profesional EspanÞola de Privacidad (APEP) and IT Member in the Sabadell Bar Association. Previously, he worked with the legal service of the Catalan DPA and in the Office of the European Data Protection Supervisor. In addition, he has also done additional postgraduate study on data protection and privacy at the Universidad de Murcia.

1. Introduction: The Internet and the New Concept of Commerce

In the last twenty years, rapid technological change has had a great impact on the creation and proliferation of new forms of commerce. Such commerce is mainly based on knowing as much as possible about each targeted person, so that he/she can be offered a product or service according to his/her preferences and location.

The expansion of the Internet has facilitated the mass collection and storage of personal data. Commercial companies have seen this phenomenon as the best tool to reach the highest number of consumers and as a means to considerably increase their sales.

While users have taken advantage of this fascinating tool (which makes available information from all over the world, enables contact between persons separated by great distances, and simplifies any kind of commercial and recreational operation) companies have found an incentive in acquiring precise information about potential customers online.

The "Internet giants" are behind all of this entire web of interests. These are companies that have been placed in an intermediate position between the interesting information for the user and the attractive data for marketing and advertising companies. They are the Internet search engines.

Today, Google is the search engine *par excellence*. In fact, this company has eclipsed other search engines such as Yahoo Search! or Bing, constituting its own virtual monopoly[1]. But Google is not only the most popular search engine in the net, but also one of the top-three email providers, a social network, and the owner of both Blogger and the biggest video platform online – Youtube [1]. Hence, considering that the main objective of Google is the collection and storage of the greatest amount of data in order to sell this to marketing companies afterwards, Google's competitors are no longer other search engines but the other Internet giants, such as Facebook, Twitter, Microsoft, and Apple.

Accordingly, this study will first examine the impact of the privacy policy that Google adopted on 1 March 2012. After that, the present analysis will look at a few controversial practices resulting from Google's collection and storage of personal data. In particular, it will examine behavioral advertising, the right to be forgotten, and the frequent link between the main Internet companies like Google, with government and law enforcement agencies. This study seeks to highlight some of the main controversial aspects between the massive processing of data from Google (for informational, commercial, or security purposes), and the right to data protection and privacy, according to both future European and U.S. laws.

2. Google's New Privacy Policy

Companies' privacy legislation is mainly adopted through self-regulation, namely, they decide on the privacy clauses that they apply to their users. Companies are entitled to decide which kind of information to take, when cookies will be installed and, in general, the company's privacy standards. In this regard, on 24 January 2012, Google decided to launch a new privacy policy, which came into force on 1 March 2012. This new policy replaces the more than 60 different policies with which Google previously had to comply, and it consists of integrating user data introduced into the net every time a person uses any of Google's platforms: Gmail, Google Maps, Google Apps, Blobber, Chrome, Android, Youtube and Google+, among others.

In terms of the EU's legal framework, the new privacy policy is being reviewed by the DPA of the various member states[2], which unsuccessfully asked to postpone the change in policy coming into force until it could have been properly examined and determined that it did not clash with European and national laws. However, Google justified the rush in

> "Likewise, eight members of the US Congress sent a letter to Google, in which they asked for more information related to the change of its privacy policy"

adopting its policy as being necessary to simplify its services, as well as to improve users' experience every time they use its platforms[3].

After the *Commission National de l'Informatique et des Libertés* (CNIL) sent Google an 18-page letter requesting the above postponement, together with an extended annex of 69 questions on its effects[4], Google answered on 5 April maintaining that its privacy policy was completely legitimate[5].

In the United States, numerous debates have stemmed from the adoption of the new policy. The Electronic Privacy Information Center (EPIC) lodged a complaint against the Federal Trade Commission (FTC) before the federal court with the aim of pushing the FTC to act against such policy[6]. However, on 24 February 2012, the federal court dismissed the complaint stating that there was insufficient evidence to prove that Google's privacy policy conflicted with relevant US law[7].

Likewise, eight members of the US Congress sent a letter to Google, in which they asked for more information related to the change of its privacy policy[8]. Further, the National Association of Attorneys General sent a letter expressing its discomfort with the new policy, since the consumer is forced to provide information to Google without offering an opt-out possibility. The Association also regretted that Google does not inform its users that the profiling, collection and storage of their personal data may affect their privacy [2].

As for the complaints lodged by citizens, there are currently many lawsuits brought by Google users before the U.S. courts claiming infringement of the previous policies. They argue that those policies guaranteed that the information updated by the user would not be used for other purposes unless the user gives his/her consent [3], and they argue that such clauses have not been respected.

Thus, Google's new privacy policy is having many implications within the privacy sector, since it has become the largest database to date, ahead of its rival Facebook. Consequently, it is still too early to determine what are the uses and limits in the processing of its data. However, an uncontrolled use of this data could turn into the most dangerous weapon against the fundamental right to data protection—an outcome which the EU is tring to prevent. Nevertheless, Google's new privacy policy would not be so controversial if it did not lead to practices such as the promotion of behavioral advertising, difficulties in being forgotten on the net, and the frequent passing of data to public agencies for law enforcement purposes. The next section will analyse each of these aspects from a legal perspective.

3. The Legitimacy of Google within and beyond the EU

Google has put at users' disposal all the information they could possibly ever require. However, this information often includes personal data, and this is responsible for several tensions between the right to be informed and an individual's right to data protection. To be clear, the right to data protection, the right to information, and the right to collective security are not absolute rights. Therefore, this section will examine how these rights interact with Google's practices, and how this search engine, due to current legal loopholes, has often sacrificed the right to data protection for the benefit of government and commerce.

3.1. Behavioural Advertising

For many years now, we have been victims of monitoring systems, which have been collecting everything about what we search on the Internet and, surprisingly, it has often been done without our consent (e.g. Google Trends or, more intrusively, the content filters used by Gmail in order to provide personalised advertisements).

Google is and has been one of the main leaders on the Internet in behavioural advertising (alongside Microsoft, Yahoo, Apple, and Facebook). Thus, through so-called "cookies", which are tiny files installed on a user's computer, Google controls users' activities over the Internet, as well as their preferences, tastes and interests. This data is then sold to advertising and marketing industries. For instance, in Minneapolis a man found out that his teen daughter was pregnant when he received baby food and clothes coupons sent to his home by a department store. The girl had not subscribed to that department store's mailing list, but she had been identified by a system which detects pregnant women's profiles via their purchases [4].

In order to avoid situations like the one above, the user occasionally has the possibility to request an opt-out from the website. In other words, the user is able to expressly reject these kinds of personalised advertisements, but here is where the controversy arises. In the United States, this model of opt-out advertisements saw the light of day in 1997 from the Clinton Administration, when the expansion of e-commerce was starting, and it allowed industries to self-regulate their behavioural advertising and their cookies.

However, within the EU legal framework, the user's prior consent is required before installing cookies in the browser as per e-Directive 2009[9]. In particular, article 5(3) of the directive states that: "*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 […]".* Hence, the directive set up a system of opt-in (and not opt-out) among member states, which was to be implemented on 25 May 2011 at the latest. Spain has recently transposed the directive through the Spanish Royal Decree 13/2012[10], which, as of 1 April 2012, has modified former Spanish legislation on telecommunications. Article 22(2) of the decree introduces the requirement of consent by user's express action, which must be also prior and informed. This new requirement increases users' control, and in particular, that they may accept or reject the installation of cookies every time they use the Internet.

Accordingly, two big European advertising companies, EASA and IAB, have published "Recommendations on Best Practices" on April 2011[11]. These initiatives were supported by the Vice-president of the Commission Kroes [5], but they were not welcomed by the Article 29 Data Protection Working Party (hereinafter, Art.29WP), which announced that it would launch a survey on codes of conduct within the field of behavioural advertising in order to establish a basis for the self-regulation system[12].

Recently, two big events have taken place, which could have consequences in the field of behavioural advertising. First, the European Commission published a Proposal for General Data Protection Regulation on 25 January 2012; and second, the Obama Administration launched the Guidelines on Consumer Privacy Bill of Rights on 23 February 2012[13].

On the one hand, article 3(2) of the Regulation establishes that "*This Regulation applies to the processing of personal data of data subjects residing in the Union by a controller*

> "The Russo case is only one of numerous current cases in which both the Data Protection Authority's (DPAs) and users can be seen as powerless in terms of removing users' personal data from the net"

not established in the Union, where the processing activities are related to: (a) the offering of goods or services to such data subjects in the Union; or (b) the monitoring of their behaviour". In other words, Google would be subject to the Regulation through this extraterritorial clause. Thus, every time Google creates profiles by collecting personal data, the company would have to comply with article 20 of the Regulation. Paragraph 2(c) of article 20 refers to the requirement of consent, which has to be specific, informed and explicit[14] (article 4(8) of the Regulation).

On the other hand, the US Guidelines on the Privacy Bill of Rights opt for a legislative procedure which allows the participation of private sector (including Google) during the drafting of future codes of conduct. The report also refers to the so-called Do-Not-Track (DNT) rules, by which consumers are able to block data collection from Internet companies. In this regards, Mozilla browser already applies DNT technology in its software [6] and it seems that the Digital Advertising Alliance, which includes companies such as Google, which is willing to introduce this technology in the future. However, this alliance has already announced that DNT will only be possible for advertisments focused on a specific sector [7], so even if users' requests on not being included are taken into account, there will be cases in which these companies will be allowed to keep collecting behavioural data for a variety of purposes [8] (for instance, in the case of the social network Google+, by the option Google+1).

Therefore, it seems that the flexibility of the system proposed by the US could clash with the more rigid legal framework launched by the EU, as regards the requirements for processing behavioural data. The problem is that global enterprises such as Google are more attracted to the US proposal, since it is more flexible, and this could push the EU to make its proposal softer, in order to bring it closer to the US legal approach.

For all that is said above, the tension between both legal orders could be solved through a project launched by Kroes consisting of creating DNT global standards as part of its programme, Digital Agenda for Europe [9]. However, it remains to be seen to what extent companies like Google will influence the drafting of those standards, as well as their efficiency in protecting users' personal data.

3.2. The Right to be Forgotten

Thanks to Google, users today have access to all kinds of information, from news stories to official documents (even confidential ones). Companies have found on the net an effective way to advertise while users are online, regardless of the user's location.

However, legal conflict arises when the right of freedom of expression and the right of information (article 20 of the Spanish Constitution) can undermine other fundamental rights, such as the right of data protection and privacy (article 18 of the Spanish Constitution). This was precisely what happenned to Dr. Guidotti Russo, a plastic surgeon who was mentioned in a critical article published by the Spanish journal, *El País* in 1991. The article reported on the legal dispute between Russo and a former patient. The controversy emerged from the fact that Russo, still working as a surgeon today, wanted that article to be removed from Google's search engine, since everytime someone typed his name into the search engine, the *El Pais* article was ranked in the top positions. This negative publicity caused Russo great financial loss to his practice. Despite the Spanish Data Protection Authority's (DPA) dispute with Google over removing this article from the search results, the link to the controversial article is still available online today[15].

The Russo case is only one of numerous current cases in which both the DPAs and users can be seen as powerless in terms of removing users' personal data from the net[16]. In fact, all European citizens have the right of access to the data the entity collects about them[17]. However, paradoxically, the information Google possesses about its users cannot be discovered by applying the right of access (unlike Facebook, as the Austrian student Mark Schrems let as know) [11]. This was the position of Google UK when it was asked to provide all personal data of one of its users. The company said that Google UK did not process any personal data in relation to the search engine, but that it was processed by Google Inc. instead. It is worth highlighting that Google Inc. is governed by US laws, which do not offer the possibility of invoking the right of access to users' own personal data [1].

In order to improve the situation where the individual remains powerless to access, modify, or delete his/her personal data on the Internet, the Proposal for General Data Protection Regulation has introduced in article 17 a new concept called "the right to be forgotten". It consists of enabling users to permanently delete personal data that they no longer wish to be published on the net. The right to be forgotten, thus, seeks to go beyond the right of erasure established in article 12 of Directive 96/46/EC, or in the same way, the rights of opposition and cancellation as stated in articles 16 and 17 of the Spanish LOPJ[18].

This new right is perceived as a threat to companies such as Google, which have been able to abstain from the rights of opposition and cancellation to date because of a current loophole for Internet search engines. In this respect, Google has argued that *"the information obtained through its search results belong to third-party webpages, whose access is public*" and in order to delete the content of such webpages "*the information should disappear from the webmaster of that third-party's webpage*"[19]. Besides this, in Europe, Google has tried to escape from legal constraints in this area, arguing that it is the only company that allows its users to send any complaint or suggestion related to the service it offers[20].

The Vice President of the European Commission Viviane Reding has already clarified that in information societies the information society services, such as Google, or social networks shall control the content, conditions and methods of processing of personal data.

In other words, Reding seeks to impose a duty on information society services to act as data controllers. However, she admits that the posting service should also carry out an important role, such as informing the search engine that a user wants his/her data to be removed [12].

With regard to the future responsibility of search engines, Google could get penalties up to the 2% of its annual incomes if it does not delete pictures or other data that an individual has uploaded, but then later wants to remove [13]. This is the reason why the proposal launched by the European Commission has caused a debate among multinational technology companies with branches in Europe. They have argued that the establishment of the right to be forgotten within the EU could jeopardise more than 15,000 millions of Euros of business in the global economy [14].

Likewise, Google's privacy lawyer distinguished in his blog the difference between services storing data uploaded by the user

> "It is a fact that Big Data offers unquestionable advantages, but a balance between the right of information and collective security on the one hand, and the individual rights of *habeas* data on the other, is needed"

(e.g., Facebook and Youtube) and services providing personal information existing in another webpage (e.g., Google, Bing or Yahoo!). In the latter case, hosting services and not search engines should be the ones entitled to delete personal information. Thus, Google states that search engines only catalogue the available information, but they do not have any direct link with the original content[21].

Moreover, one of the problems emerging from this new concept of the right to be forgotten is deciding what will happen with the subsequent copies of personal data, which remain once the original information has been deleted. Accordingly, Reding has already clarified that only in cases where the data controller has authorised the publication of personal data to a third party, will it be considered responsible for such publication [15].

Finally, it is worth highlighting the potential clash between the right to freedom of expression (as conceived by the US Supreme Court) and the right to be forgotten. Even though the proposed EU regulation predicts a number of exceptions on the enforcement of the right to be forgotten in order to protect the freedom of expression (article 17(3) of the Regulation), the US Supreme Court has expressed that the States are not empowered to adopt legislation that restricts communications (censorship in other words), not even in cases of embarassing information (e.g. the name of a raped person), as long as this information is collected using legitimate means [13]. But the unanswered question is: What if the victim wants this information to be removed?

3.3 Link with Public Authorities

Together with the right of information and the right to data protection, the right to collective security has had implications regarding the activities Google has carried out in the last ten years. In fact, the line dividing the processing of personal data by public and private entities is becoming increasingly blurred. Originally, the division was clear: private companies collected data for commercial purposes; and government and police authorities processed data with the aim of preventing or fighting crime. However, the rise in international terrorism today has required private companies to provide law enforcement with users' personal data for counter-terrorist purposes[22].

Google has admitted that it has given users' information to the US government, since according to 1986 Electronic Communications Privacy Privacy Act, neither court order nor prior notification to the user are required [16]. Likewise, since 9/11 attacks, the USA Patriot Act allows the US authorities to require any kind of personal information collected by private companies during a counter-terrorism investigation.

With the purpose of reducing users' insecurity about not knowing where their data is processed, Google created the Transparency Report[23], which allows users to see the number of governmental requests for their data, as well as the information blocked by governments. The report is classified by semesters and according to the country.

The Transparency Report illustrates how private companies such as Google are gaining important roles in the collection and processing of personal data, since they do not only provide data to other private companies for advertising purposes, but also to the government with the aim of creating profiles of criminal suspects[24].

It is a fact that Big Data[25] offers unquestionable advantages, but a balance between the right of information and collective security on the one hand, and the individual rights of *habeas* data on the other, is needed [7]. The frequent practice of governments to seize massive amounts of data (not only from suspects or criminals) for security purposes is controversial: Where is the limit? Is the intrusion presumptively proportional and justified as long as it is for "counter-terrorism purposes"? The popular argument "I have nothing to hide"[26] shows the priority of collective security over individual privacy. However, more privacy should not imply less security or vice versa [19], but the key issue is to strike the right balance between both rights.

4. Conclusions

As The New York Times stated, personal data is the fuel of the twenty-first century [20]. Massive technological advances, globalisation of markets, and the enhancement of counter-terrorism measures, are some of the major factors driving the mass collection and processing of personal data, from both public and private entities.

Specifically, this study has analysed the way Google processes personal data in the current digital era. It examined the privacy laws and potential clashes between the EU and the US legal approaches, as well as the limits of responsibility in the processing of personal data. Likewise, new phenomena such as the right to be forgotten or behavioural advertising have been examined, focusing on the EU attemps to safeguard the fundamental right to data protection.

The study has also looked at some controversial data protection issues that have emerged due to the expansion of the most popular search engine, Google, which has vowed to fight where opposing viewpoints clash: First, the right of information and freedom of speech; second, the collective security in a world invaded by terrorism and criminality; and third, the duty to protect personal data and individuals' privacy, whose data are constantly collected and processed by private and public actors.

As stated above, it can be concluded that Google has acquired the title of "emperor" on the net, becoming the main obstacle for the DPAs within the EU. Google represents the new digital era, where the power is measured by the control a company has on the net. Despite the US and EU lawmakers' efforts to get both legal approaches closer and removing the current loopholes on privacy and data processing, there is still a long ways away.

Maybe, one day we will be able to speak about global standards on data protection as proposed in the Madrid Declaration in 2009, considering that data protection is already part of all current legislative agendas. Now it remains to be seen to what extent companies such as Google are involved in the decision making, and how it could affect to the protection of our personal data.

References

[1] J. Ball. "Me and my data: how much do the internet giants really know?", *The Guardian*, 22.04.2012. <http://www.guardian.co.uk/technology/2012/apr/22/me-and-my-data-internet-giants?fb=native>.

[2] S. Forden. "Google Privacy Policy Criticized by State Attorneys General", *Bloomberg.com,* 22.02.2012. <http://www.businessweek.com/news/2012-02-22/google-privacy-policy-criticized-by-state-attorneys-general.html>.

[3] J. Ribeiro. "Google faces class action lawsuits against new privacy policy", *Computer World*, 22.03.2012. <http://www.computerworld.com/s/article/9225406/Google_faces_class_action_lawsuits_against_new_privacy_policy?taxonomyId=17>.

[4] C. Duhigg. "How Companies Learn Your Secrets", *The New York Times*, 16.02.2012. <http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?_r=1&pagewanted=all>.

[5] N. Kroes. "*Towards more confidence and more value for European Digital Citizens. European Roundtable on the Benefits of Online Advertising for Consumers*". SPEECH/10/452. Brussels, 17.09.2010.

[6] A. Fowler. "Mozilla Led Effort for DNT Finds Broad Support". *Mozilla Privacy Blog. Covering the latest developments in privacy & data safety*, 23.02.2012. <http://blog.mozilla.com/privacy/2012/02/23/mozilla-led-effort-for-dnt-finds-broad-support/>.

[7] E. Mills. "Firms embrace Do Not Track for targeted ads only", *CNET News*, 23.02.2012. <http://news.cnet.com/8301-31921_3-57384193-281/firms-embrace-do-not-track-for-targeted-ads-only/>.

[8] R. Waters. "Europe and US to clash over online data protection", *Financial Times*, 23.02.2012. <http://www.ft.com/intl/cms/s/0/c039ce50-5e4b-11e1-85f6-00144feabdc0.html#axzz1nLUCGPgH>.

[9] N. Kroes. "*Why we need a sound Do-Not-Track standard for privacy online*", enero 2012. <http://blogs.ec.europa.eu/neelie-kroes/donottrack/>.

[10] V Mayer-Schönberger. "*Delete. The Virtue of Forgetting in the Digital Age*". Princeton University Press, New Jersey, 2009. ISBN-10: 0691138613.

[11] B. Donohue. "Twenty Something Asks Facebook For His File And Gets It - All 1,200 Pages", *Threat Post*, 13.12.2011. <http://threatpost.com/en_us/blogs/twenty-something-asks-facebook-his-file-and-gets-it-all-1200-pages-121311>.

[12] T. Espiner. "Firms face tough new EU fines for data breaches", *ZDNet UK*, 25.01.2012. <http://www.zdnet.co.uk/news/security-management/2012/01/25/firms-face-tough-new-eu-fines-for-data-breaches-40094907/>.

[13] J. Rosen. " The right to be forgotten", *Stanford Law Review*,13.02.2012. <http://www.stanfordlawreview.org/online/privacy-paradox/right-to-be-forgotten>.

[14] S. Sengupta. "Facebook's Sandberg Gently Warns Europe About Privacy Rules", *The New York Times*, 24.01.2012. <http://bits.blogs.nytimes.com/2012/01/24/facebooks-sandberg-gently-warns-europe-about-privacy-rules/>.

[15] D. Meyer. "EU puts Google straight on "right to be forgotten", *ZDNet UK,* 22.02.2012. <http://www.zdnet.co.uk/news/security/2012/02/22/eu-puts-google-straight-on-right-to-be-forgotten-40095097/>.

[16] J.P. Titlow. "Google Hands Wikileaks Volunteer's Gmail Data to U.S. Government", *ReadWriteWeb*, 10.10.2011. <http://www.readwriteweb.com/archives/google_hands_wikileaks_volunteers_gmail_data_to_us.php>.

[17] A. Krotoski. "Big Data age puts privacy in question as information becomes currency", *The Guardian*, 22.04.2012. <http://www.guardian.co.uk/technology/2012/apr/22/big-data-privacy-information-currency?newsfeed=true>.

[18] Daniel J. Solove. "I've Got Nothing to Hide" and Other Misunderstandings of Privacy", *San Diego Law Review, Vol. 44*, p. 745, 2007.

[19] Adam D. Moore. "Privacy, security and accountability", Chapter 10 of "*Privacy Rights. Moral and Legal Foundations*", The Pennsylvania State University Press, USA, 2010.

[20] J. Brustein. "Start-Ups Seek to Help Users Put a Price on Their Personal Data", *The New York Times*, 12.02.2012. <http://www.nytimes.com/2012/02/13/technology/start-ups-aim-to-help-users-put-a-price-on-their-personal-data.html?_r=3>.

Notes

[1] In fact, the European Commission has an investigation open since November 2010 for an alleged violation of Art. 102 TFEU for an abuse of a dominant position. <http://europa.eu/rapid/press-release_IP-10-1624_en.htm>.

[2] Letter from the Article 29 Data Protection Working Party to Google Inc, 02.02.2012. <http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2012/20120202_letter_google_privacy_policy_en.pdf>.

[3] Letter from Google to the Commission Nationale de l'Informatique et des Libertés (CNIL), 03.02.2012. <http://www.cnil.fr/fileadmin/documents/La_CNIL/actualite/questionnaire_to_Google-2012-03-16.pdf>.

[4] CNIL, Ref. IFP/BPS/CE121169. <http://www.cnil.fr/fileadmin/documents/La_CNIL/actualite/questionnaire_to_Google-2012-03-16.pdf>.

[5] Google defends privacy policy to European watchdog, 05.04.2012. <http://www.reuters.com/article/2012/04/05/google-privacy-idUSL6E8F5ASO20120405>.

[6] <http://epic.org/privacy/ftc/google/EPIC-Complaint-Final.pdf>.

[7] <http://epic.org/privacy/ftc/google/EPICvFTC-CtMemo.pdf>.

[8] Letter from the US Congress to Google, 26.01.2012. <http://www.reuters.com/article/2012/01/26/us-google-privacy-idUSTRE80P1YC20120126>.

[9] OJ L337, 18.12.2009, p.11-36. This directive amends the previous Directive 2002/58/EC (ePrivacy), OJ L2012, 31.7.2002, p.37-47. - Note from the reviewers: *It should be noted that not all countries have enacted legislation on this including Germany*.

[10] BOE (Spanish Official State Gazette) 31 March 2012, num. 78, sec I.P 26876-26967.

[11] EASA Best Practice Recommendations on Online Behavioural Advertising. Setting out a European advertising industry-wide self-regulatory standard and compliance mechanism for consumer controls in Online Behavioural Advertising", 13 April 2011; European Self-regulation for Online Behavioural Advertising. Transparency and Control for Consumers, IAB Europe, 27 April 2011.

[12] Press release Article 29 Data Protection Working Part, 15.12.2011.

[13] <http://www.whitehouse.gov/sites/default/files/privacy-final.pdf>.

[14] For a more exhaustive definition of these terms, see Opinion 15/2011 on the definition of consent, WP187, 13.7.2011.

[15] El Paiìs, 28.10.1991, <http://elpais.com/diario/1991/10/28/sociedad/688604403_850215.html>.

[16] For an exhaustive study regarding the right to be forgotten in the digital era, see [10].

[17] Art. 12 of the Directive 95/46/EC.

[18] BOE nuìm. 298, 14.12.1999. *Ley Orgainica 15/1999*, 13 December 1999, on Personal Data Protection.

[19] AEPD, SP/SENT/626428, 320/2008, 7 April 2011.

[20] "Our thoughts on the right to be forgotten". Google European Public Policy Blog, 16.02.2012 <http://googlepolicyeurope.blogspot.com/2012/02/our-thoughts-on-right-to-be-forgotten.html>.

[21] "Our thoughts on the right to be forgotten". Google European Public Policy Blog, 16.02.2012 <http:// googlepolicyeurope.blogspot.com/2012/02/our- thoughts-on-right-to-be-forgotten.html>.

[22] This is the case of PNR agreements, by which airline companies provide passengers' data to the US, Canadian and Australian authorities; or SWIFT agreement, by which this entity send financial data of EU citizens to the US authorities. Both agreements have its rationale in preventing and combating terrorism.

[23] <http://www.google.com/transparencyreport/governmentrequests/userdata/>.

[24] For exemple, the NY police used a picture on Facebook combined with its own pictures files and a facial recognition program to arrest a man suspected of murder. <http://rt.com/usa/new-york-barbershop-shooting-951/>.

[25] For a definition of this term, see <http://mike2.openmethodology.org/wiki/Big_Data_Definition>.

[26] See the debate behind this argument in [18].