Discussing Transparency of Privacy Policies in the Age of Big Data. Towards the «Social Norm» as a New Rule of Law

Discutiendo la transparencia de las políticas de privacidad en la Era del Big Data. Hacia la «Norma Social» como nueva Regla de Derecho

María Estrella Gutiérrez David
Profesora Contratado Doctor de
la Universidad Rey Juan Carlos
estrella.gutierrez@urjc.es

Abstract: The aim of this paper is the study of substantive and formal transparency of privacy policies as an essential prerequisite of a meaningful consent to fair data processing practices by third parties. In particular, Big Data techniques raise serious concerns on massive data processing, given the lack of explicit notice about such practices in privacy policies. In this sense, this paper will examine some paradigmatic cases, and will analyse why users' perception and Data Protection Authorities investigations are coincident in concluding the lack of transparency of privacy policies. Albeit EU General Data Protection Regulation has codified the principle of transparency, one of the main findings of this paper is that privacy policies are still designed to foster legitimization of the «Social Norm» to the detriment of the «privacy by default» principle.

Keywords: Big Data, transparency, privacy policies, personal data processing, EU General Data Protection Regulation (2016).

Resumen: El objeto de este trabajo es el estudio de la transparencia sustantiva y formal de las políticas de privacidad como requisito esencial de un consentimiento informado con relación al tratamiento legítimo de datos personales por terceros. Especialmente, las técnicas de Big Data suscitan serias preocupaciones acerca del tratamiento masivo de datos personales, al no explicitarse siempre dichos tratamientos en las políticas de privacidad. En este sentido, este trabajo se centrará en algunos casos paradigmáticos, y analizará por qué la percepción de usuarios e investigaciones de Autoridades de Protección de Datos coinciden en señalar la falta de transparencia de las políticas de privacidad de los prestadores de servicios. Aunque el Reglamento Europeo de Protección de Datos ha consagrado el principio de transparencia, cabe concluir que las políticas de privacidad parecen seguir diseñadas para propiciar la legitimación de la «Norma Social», en detrimento del principio de «privacidad por defecto».

Palabras clave: Big Data, transparencia, políticas de privacidad, tratamiento de datos personales, Reglamento Europeo de Protección de Datos (2016)

ISSN 1989-7022

1. Why transparency?

User data are "the oil of digital economy" (Williams et al., 2016, 26). Likewise, big data means big privacy concerns as technology allows organisations to collect and make use of personal data on an unprecedented scale: "[…] it is critical to remember that access to so much data, from so many different sources, […], increasingly means we can perceive patterns, engage in discoveries, and discover secrets that were heretofore hidden" (Kuner *et al*., 2012, 46-47).

An innocent *click on* Facebook's social plug-in «Likes» may reveal much of our personality. Kosinski *et al* (2013) showed that digitally mediated behaviours can be easily recorded, analysed and used to accurately predict a range of highly

Received: 24/04/2017
Accepted: 14/05/2017

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 165-184

sensitive personal attributes including age, gender, personality traits, sexual orientation, ethnicity, religious and political views.

Are people aware of such risks? The Privacy Commissioner in Hong Kong (2013, 43) came to the conclusion that the level of transparency of smartphone apps privacy policies was "low and unsatisfactory". In consequence, smartphone users cannot make "an informed decision on whether they should exchange their personal data stored on their smartphone for the benefits (or risks) of using the app".

Not by chance, in the Age of Big Data, the new General Data Protection Regulation (GDPR)[1], which shall apply from 25 May 2018, has expressly embraced transparency as general principle of personal data processing.

Some commentators have described the consequences of the lack of transparency in this way: "Users are ill placed to make responsible decisions about their online data […] Imposing this burden on users places them at an inherent disadvantage and ultimately compromises their rights" (Tene; Polenski, 2012, 285).

This being the perception of Internet and apps users, such perception does not differ from the conclusions reached by Data Protection Authorities (DPA): representations made by ISP's privacy policies are usually misleading and, thus they constitute a breach of data protection Law.

In this sense, the analysis of privacy policies of Internet service providers (ISP) and cases investigated by Authorities reveal two things. On the one hand, Authorities' approach on these cases has been based on a specific understanding of transparency as data processing principle (formal and in substance), even much before the adoption of GDPR. On the other hand, many data breaches are due to lack of transparency of privacy policies, and this usually arises from the following **«maladies»**: the cost of reading privacy policies (formal transparency); and misrepresentation of privacy in terms of real extent and purposes of data processing (substantive transparency).

Contrary to the official «parlance», this paper will try to evidence how the «social by default» rule is replacing in practice the «privacy by default» rule. Put it in another way, the fashion-forward principle that the «Social Norm is the new rule of Law» is being broadly legitimised.

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 165-184

2. Big Data, big privacy concerns

Big Data is usually characterised by four 'V's: (i) the *volume* of data (according to CISCO's 2016 Index, by 2020, global IP traffic will reach 2.3 ZB per year); (ii) the *velocity* at which data is collected and processed thanks to big data analytics; (iii) the *variety* of personal information aggregated for individual's profiling purposes; (iv) the *value* of the data such as geo-localisation data or data on energy consumption patterns (Stuck; Grunes, 2016, 16-28).

In 2016, Outlook.com had 400 million of active users; more than 1.2 billion people use Microsoft Office in 140 countries and 107 languages (Microsft, 2016); and, Google's Gmail had also crossed "the 1 billion monthly active user milestone" (Gibbs, 2016). In 2017, statistics have shown that Facebook has reached almost 2 billion of active users; WhatsApp, 1.2 billion; YouTube, 1 billion; Instagram, 600 million; Twitter, 319 million (Statista, 2017).

To put it in perspective, if one zettabyte equals one trillion of gigabytes, billions of users do mean many zettabytes of personal data collected and processed by data-driven business. And also data of many categories: demographic data, sensitive data, locational data, social data, behavioural data, user-generated-content like photos, videos, comments on social media, official data (Stuck; Grunes, 2016, 15).

It is clear then that the more personal information is collected, the more privacy concerns arise regarding "profiling, tracking, discrimination, exclusion, government surveillance, and loss of control" (Tene; Polonetsky, 2013, 250).

Much before the invalidation of the US-Europe Safe Harbour Agreement by the European Court of Justice (ECJ, 2015), the «David and Goliath» dispute between a law student, Maximiliam Schrems, and Facebook had illustrated to which extent ISP were able to store many types of data about their users.

In fact, Facebook answer to Schrems request of access to all his personal data in 2010[2] revealed how the social network had processed at least 57 different categories of data displayed within a 1,222 pages file covering three past years of requester's activity in Facebook. In the course of subsequent claims following to that request, it was discovered that Facebook had not informed at all about many categories of data, eg. «like-function» data, tracking on other webpages, face recognition, videos,

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 165-184

postings on other walls, indicators for the intensity of relationships, cookie-related information, profile status change, verified mobile numbers, and even deleted information (europe-v-facebook.org; Consumer Report, 2012).

2.1. Promises

According to Williams *et al.* (2016, 420), "a helpful and almost universal principle for handling personal data", supported by the UK Information Commissioner's Office (ICO), is that "always say what you are going to do, and always do what you say".

But purposes of data processing are not always clearly represented by privacy policies, and big data has reinforced perception of both individuals and regulators about the "obscure purposes" in the uses of personal information (Tene; Polonetsky, 2013, 268).

Far beyond the invalidation of the Safe Harbour Scheme, there are further lessons to be learnt from Schrems case about privacy promises and real practices. In essence, the ECJ suggested that one of weaknesses in the application of the international data transfers scheme to third countries was precisely the "structural shortcomings related to *transparency* and enforcement [of] the substantive Safe Harbour principles".

In reality, the ECJ finding in Schrems case was not a novelty. The FTC had found that, from 2007 to 2012, the social network had misrepresented in its Privacy Policy that it adhered to, and/or complied with "the EU Safe Harbour Privacy Framework as set forth by the United States Department of Commerce" (In the Matter of Facebook, July 2012).

Facebook is not an isolated case. From October 2005 until October 2011, Google had been also representing that, prior to the launch of its social network Buzz associated to Gmail product, it had adhered to the US-EU Safe Harbour Privacy Principles. After an investigation, the FTC found that such representations were "false or misleading and constitute[ed] a deceptive act or practice" (In the Matter of Google, March 2011).

Market strategies of big data business may also pose competition and privacy concerns at the same time. In effect, "monopolies' data-driven exclusionary practices can hamper innovative alternatives that afford consumers greater privacy protection" (Stucke; Grunes, 2016, 4).

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 165-184

Although Facebook's acquisition of WhatsApp was authorised, the European Commission (2014, par. 102) expressed its worries on weather Facebook would rely on the promises made by WhatsApp's privacy policy of not sharing personal data, given that "Facebook Messenger enables Facebook to collect data regarding its users that it uses for the purposes of its advertising activities".

Suspicions seemed to be well-funded. In August 2016, WhatsApp announced the update of its Terms of Service and Privacy Policy, and the possibility of synchronising WhatsApp user phone numbers with Facebook user identities with a view to improve "user's experience".

After the announcement, on 20 December 2016 the European Commission opened a formal investigation and sent a Statement of Objections to Facebook:

> *"In today's Statement of Objections, the Commission takes the preliminary view that, contrary to Facebook's statements and reply during the merger review, the technical possibility of automatically matching Facebook users' IDs with WhatsApp users' IDs already existed in 2014. At this stage, the Commission therefore has concerns that Facebook intentionally, or negligently, submitted* incorrect or misleading information to the Commission*, in breach of its obligations under the EU Merger Regulation".*

2.2. What «we understand»

"Studies show privacy policies are hard to read, read infrequently, and do not support rational decision making", said McDonald and Cranor (2008, 544).

Different surveys run by public authorities at European and national level have measured the degree of awareness of and trust in ISP privacy policies. In 2014, a survey conducted amongst undergraduate and postgraduate students of two Spanish Universities[3] (Spanish survey) assessing the degree of transparency of Facebook's privacy policies came to similar conclusions.

In particular, Eurobarometer 2010 run by the European Commission showed that one third of EU consumers did not read any of the privacy notices on the websites they visited, while another 15% said that they did this "rarely".

A year later, European consumers were asked again whether they usually read privacy statements on the Internet. Although 58% of respondents said that they read the privacy statements on the Internet, this result was undermined by the fact

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 165-184

that 24% said that they read them without fully understanding privacy statements and that 38% of Internet users said that they do not read them at all (Eurobarometer 2011, 112).

The Spanish survey evidenced a dramatic lower rate of respondents who acknowledged having read Facebook's Data Use Policy (DUP): only one in ten (11%).

When measuring the degree of distrust in privacy policies, the 2011 Eurobarometer noted that companies holding personal information might use it for purposes other than those for which such information was collected (namely, for direct marketing or targeted online advertising) without informing the data subject concerned. A large majority of respondents were concerned (70%) about this opaque practice.

Similar findings were evidenced in the UK. Three in five agreed that organisations handled personal information on individuals in an unfair and improper way (60%). Only 32% of respondents thought that online companies collected and kept personal details in a secure and proper way (ICO, 2013).

In the Spanish survey, respondents were much more sceptical. 96% of them thought that social networks and, more specifically Facebook, did not handle their personal data in an appropriate and respectful way.

User's perceptions about information provided by online IPS regarding their data processing practices have not improved too much. The Eurobarometer 2015 has confirmed that only two out of ten respondents are always informed about data collection and the way data are used. In particular, 41% of respondents said they were only sometimes informed; 22% of them said they were rarely informed about these issues, and 11% said they were never informed (Eurobarometer 2015, 81).

3. Transparency and privacy models

If the degree of user awareness depends upon transparency, and transparency is a prerequisite for an informed and meaningful consent, then users should be noticed in a transparent way about data collected and data processing practices.

Existing legal frameworks on privacy protection emphasize either *consent based-model* (Europe) or *notice and choice based-model* (United States). In both cases,

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 165-184

transparency of information given by ISP is the cornerstone of privacy rules. Differences in these models have to do with the binding or voluntary basis to enforce compliance with the principle.

3.1. Existing privacy models, a clash of interests

In the opinion of Tene and Polonetsky (2012a, 285), "by emphasizing «transparency and user consent,» in European data protection terms, or «notice and choice,» in United States parlance, the current legal framework imposes a burden on business and users that both parties struggle to lift."

Approaches on data privacy in Europe and the United States are far different, and in essence, they are focused on different interests. In the view of the German Data Protection Commissioner in Schleswig-Holstein (2013), the objective of European data protection law is "the protection of individuals, not of companies".

European data protection model has taken a more "paternalistic approach" than that of its American neighbours (Lloyd, 2011, 13). European approach is based on consent as a manifestation of individual control (Tene; Polonetsky, 2012, 338).

In effect, relying on the principles of human dignity and personal liberty, European constitutional traditions consider that the fundamental right to personal data protects the freedom of an individual to decide whether data concerning his person may be accessed and used by third parties. The Spanish Constitutional Court' landmark Judgment 292/2000, of 30 November, firmly inspired by the "right to self-determination" of its German counterpart, has considered that the so-called *habeas data* –literally, *you should have the data*– is the "power of an individual to exercise control over their personal data, and to object the use of such data for purposes other than the legitimate interest which originally justified its collection".

By contrast, the "notice and choice" approach favoured in the United States is "designed to put the individual in the centre of the action to let him a large voice in decisions as to what information will be collected, used and disseminated about him" (Lloyd, 2011, 22).

By such "flexible approach" to privacy protection, it is sought to facilitate "innovation" and spur "technologically advanced services". In order to foster business innovation, it

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 165-184

is assumed that protection of personal data is better governed by voluntary enforceable codes of conduct together with sectorial privacy laws covering certain information categories, e.g. health, finance, education (US Department of Commerce, 2014, 9, 12).

In practice, this means that online businesses have been producing privacy policies free from any formal or substantive requirements legally binding upon them. As voluntary disclosure have formed the basis of their privacy policies, there have been "no requirements for the existence of a policy let alone any restrictions as to the format, length, readability, or content of a given privacy policy" (McDonald; Cranor, 2008, 546).

In fact, Statements of the European Data Protection Authority, Article 29 Working Party (WP29) addressed to tech giants –most of them with US-based headquarters, strongly evidence that personal data processing practices affecting European citizens are usually an ongoing concern[4].

The public consultation process run by the European Commission (from 4 November 2010 to 15 January 2011) on its Communication on a «Comprehensive Approach on Personal Data Protection in the European Union» (2010) showed the online businesses' reluctance to the adoption of "standard forms" for privacy information notices imposed by data regulation.

An oft-repeated *mantra* was that binding obligations "would run counter to innovative approaches by service providers" (Facebook) or "could prevent innovation in new and more meaningful forms of transparency" (Yahoo!). According to such approach, the use of standard notices would be put in practice, at best, on a "voluntary" basis (Yahoo!). Arguments given by Microsoft were representative of this view:

> *"While we support an obligation to provide clear and thorough notices, we do not believe that legislation should dictate the method by which users are informed […] Likewise, because the effectiveness of notices can be undermined by providing too much information just as it can be by providing too little, data controllers should have reasonable discretion about what information to disclose".*

3.2. Codifying transparency in the GDPR

On the side of the European Union, some investigations conducted by DPA before the adoption of the GDPR evidenced that relevant provisions of the Directive 95/46/

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 165-184

EC on the information to be disclosed to data subjects were not sufficient enough to ensure an informed and meaningful consent.

The announcement by Google on 1 March 2012 that its new privacy policy and terms of service would apply to most of its services raised numerous questions about Google's data processing and profiling practices. The WP29 launched an in-depth investigation to assess the compliance of Google's new Privacy Policy with the Data Protection Directive. In particular, the investigation confirmed not only WP29 concerns about the combination of data across services, but also the lack of transparency in the way that Google have informed about such practices:

> *"[…] Google provides* insufficient information *to its users (including passive users), especially on the purposes and the categories of data being processed. As a result, a Google user is unable to determine which categories of data are processed in the service he uses, and for which purpose these data are processed. Internet companies should not develop privacy notices that are* too complex, law-oriented or excessively long*".*

In the long discussion-process preceding the GDPR, transparency started to be considered expressly a fundamental premise for enabling individuals to exercise control over their personal data. Approach on transparency was twofold, in substance and formal (European Commission, 2010, p.6).

Ultimately, Article 5.1.a) GDPR has endorsed transparency as basic data processing principle. Accordingly, personal data shall be processed "lawfully, fairly and in a *transparent manner* in relation to the data subject ('lawfulness, fairness and transparency')", along with other principles such as purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, and accountability with respect to the ability of data controller to demonstrate compliance with the foregoing principles.

Pursuant to Article 12 GDPR "transparent information" is required to data controller on both existing data processing and modalities for the exercise of the rights of data subject. The said provision defines transparency in terms of what relevant information (substantive transparency) should be disclosed to data subject and how this information must be presented (formal transparency):

> *"The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject [*substantive transparency*] in a concise, transparent, intelligible and easily*

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 165-184

> *accessible form, using clear and plain language [*formal transparency*], in particular for any information addressed specifically to a child […]"*

On the one hand, *substantive transparency* imposes an obligation on data processors to disclose information where personal data are collected directly from the data subject (Article 13) or from anyone else different from data subject (Article 14); information related to the exercise of the rights of access by the data subject (Article 15), to rectification of inaccurate data (Article 16), to erasure or the 'right to be forgotten' (Article 17), to restriction of processing (Article 18), to data portability (Article 20), and to object any decision based solely on automated processing, including profiling (Articles 21-22), and appropriate communication of any personal data breach to the data subject (Article 34).

On the other hand, Article 12 construed in connection with Recitals 58 and 60 GDPR explains how to put in practice *formal transparency*. Formalities refer to a set of requirements to be applied to privacy notices: (i) Clear and plain language, conciseness, and legibility; (ii) In writing, including electronic means, and if provided orally, it should be to the request of data subject, but the burden of prove identity of data subject will be on data controller; (iii) Prominent visualization and accessibility; (iv) In combination with standardised and machine-readable icons. The aim of such formalities is to provide, by means of privacy notices "in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing".

4. Transparency in practice: lessons from the past

McDonald and Cranor (2008, 314) pertinently referred to the "cost of reading privacy policies." The US Department of Commerce (2010, 30-31) was of the same view:

> *"Merely providing general information about data practices is not effective transparency; this information must be accessible, clear, meaningful, salient, and comprehensible to its intended audience. When information is presented in a way that is highly complex or detailed, it may not be transparent […] The shortcomings of many privacy policies […] are widely recognized: they can be dense, lengthy, written in 'legalese,' and 'overwhelming' to the few consumers who actually venture to read them."*

Are these complex privacy policies responsible for users' failure to read notices which will govern collection and use of their personal data?

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 165-184

Although it is difficult to ascertain a direct relationship between both parameters, namely, design of privacy policies and failure to reading, it is undeniable that the former may play an important role in undermining users' willingness to take a long time in reading privacy statements.

4.1. The Minotaur Labyrinth: endless, fragmented and hyperlinked privacy policies

Almost ten years ago, McDonald and Cranor (2008, 543) calculated that skimming privacy policies per person would take an average of 40 minutes a day. Remarkably, such estimation was based upon an average word length of privacy policies ranging from 144 words (short policy) to 7,669 words –about 15 pages of text– (long policy).

Facebook's policies are good examples of how privacy notices are getting longer and more complex for ordinary users.

Facebook's services are rendered under their privacy policy, the Data Policy (DP), and their Statement of Rights and Responsibilities (SRR), along with other ancillary documents. More importantly, privacy rules applied by Facebook are contained not only in DP, but also in SRR and ancillary documents.

In the 2014 Spanish survey, 78% of the respondents considered that the 2013 DP length was not reasonable at all. In fact, 2013 DUP consisted of almost 10,000 words, containing approximately 45 hyperlinks to further information, and SRR had about 4,500 words including approximately 15 hyperlinks.

In addition, information displayed in 2013 DUP and SRR was dispersedly supplemented in different pages with ancillary information about cookies (about 3,700 words), other websites and applications (about 2,500 words), advertising on Facebook (about 1,900 words), amongst others (cf. McCallig, 2013, 112). Moreover, this ancillary information included additional hyperlinks which contained specific provisions governing personal data processing.

Today, both September 2016 DP and January 2015 SRR have apparently reduced its lengthy to 2,711 and 3.803 words, 23 and 30 hyperlinks respectively, but they live together with other 24 labels governing other Facebook services (Messenger, Facebook Lite, Ad Choices, Find Friends, Instagram, Mobile, etc). More specifically, Cookies' policy

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 165-184

covers 1.677 words and Privacy Shield provisions (replacing Safe Harbour Agreement) comprises 855 words. In addition, DUP contains 5 subsequent hyperlinks, and 6 secondary links to "more resources" resulting in a «never ending labyrinth».

According to the Spanish Data Protection Agency, "the existence of multiple hyperlinks hinders full knowledge of Privacy Policy". "When privacy policies, -opines the AEPD- its nuances, exceptions, and information to exercise statutory rights is covered by an indeterminate number of pages, this shows to what extent it is necessary to be an expert to understand such privacy policy" (AEPD, 2013).

4.2. Inconsistencies and legalese

Eurobarometer 2010 showed that 45% of European consumers who actually read privacy policies did not understand them, as they found such policies "quite unclear" or "very unclear". The results of the Spanish survey in 2014 were overwhelming: almost all respondents (97%) think that the DUP is not clear and understandable.

Perceptions have not changed over the time. And, in analysing the reasons for not reading privacy policies, two-thirds of European respondents (67%) say that they find the statements too long to read, nearly four out of ten (38%) find them unclear or too difficult to understand, and, remarkably, 15% of respondents think the websites do not honour the statements anyway (Eurobarometer 2015, 87).

The «story» of «sponsored stories» is illustrative. 2012 changes in Facebook's privacy policies misleadingly introduced this kind of social advertising where users' data became the raw material furnishing the advertisement.

Spanish students were prompted to examine clause 10 displayed in Facebook's 15 November 2013 SRR update, where the social network openly recognised that its goal was "to deliver advertising and other commercial or *sponsored content* that is valuable to our users and advertisers". In doing so, users agreed to the following:

> "*1.* You give us permission *to use your name, profile picture, content, and information in connection with commercial, sponsored, or related content (such as a brand you like) served or enhanced by us. This means, for example, that you permit a business or other entity to pay us to display your name and/or profile picture with your content or information, without any*

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 165-184

compensation to you. If you have selected a specific audience for your content or information, we will respect your choice when we use it.

2. We do not give your content or information to advertisers without your consent.*"*

Only 30% of the Spanish survey respondents did understand properly that clause 10.1 entitled Facebook to use their personal data as an endorsement for a paid advertisement. In addition, respondents were asked to identify the extent of their consent in relation to sponsored stories. In this sense, 28% of respondents assumed that an almost blanket consent was given and their information could be used in sponsored stories in accordance with clause 10.1. By contrast, 72% of respondents felt that specific and explicit permission would be required by Facebook as clause 10.2 seemed to suggest.

The wording of the statement was everything but clear. Whereas clause 10.1 suggested that users had no choice to opt-out or to opt-in Facebook's use of their information, clause 10.2 seemed to say the opposite: that specific and explicit consent (opt-in) would be asked for using users' content and information in sponsored stories.

Legalese is another difficulty. "Too often, privacy policies appear designed more to limit companies' liability than to inform consumers about how their information will be used", has observed the FCT (2010, 19).

To avoid unfair terms in consumer contracts, the UK Office of Fair Trading (OFT, 2008) has pertinently indicated that: "[…] what is required is that terms are intelligible to *ordinary* members of the public, *not just lawyers*. They need to have a proper understanding of them for sensible and practical purposes".

Accordingly, Spanish respondents were asked to read carefully clause number 16.3 of Facebook's November 2013 SRR update related to "disputes". In particular, this clause contained a typical disclaimer of liabilities and warranties. Respondents were prompted to assess whether or not they had understood the consequences of such clause.

The wording of this clause –as it was disclosed by Facebook to Spanish users– included a literal translation into Spanish of legal terms such as, "Facebook as is", "express or implied warranties", "implied warranties of merchantability", "fitness for a particular purpose", "lost profits" or "consequential, special, indirect, or incidental damages"[5]. Most of those legal terms and disclaimers are not familiar

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 165-184

with Civil Law traditions as it is the case of the Spanish Law, and much less for an ordinary user.

94% of respondents said that they didn't understand the consequences of this clause, and only 6% of respondents said "Don't know/ don't answer". It is needless to say that Spanish users –even those with legal expertise- are not likely to be familiar with the jargon of Anglo-American disclaimers.

The current version of this clause in January 2015 SRR update is not significantly different from the 2013 version.

5. Misrepresenting privacy

Continuous changes on ISP's privacy policies may represent an illustrative example of the said «maladies».

The in-depth investigation started by the WP29 after 2012 Google's Privacy Policy update determined the creation of a task force including representatives of the French, Spanish, Italian, German, Dutch, and UK DPA to consider the Privacy Policy's compliance with their national legislation. A common allegation was that descriptions of the purposes for data processing in the Privacy Policy were too vague. In the formal investigation conducted by the Spanish AEPD (18 December 2013) and leading to a €900,000 in fines for serious breaching of national data Law, the Agency opined:

> *"Google's privacy policy is undetermined, given wide and unclear expressions that it uses, as well as the multitude of links that need to be handled to know it in its entirety. It refers to a series of purposes characterized by their inaccuracy and does not specify services and personal data associated with said purposes".*

For example, the AEPD noted that Google performed filtering of email content and files attached to insert personalized advertising without explicitly noticing to Gmail users nor asking them to give their consent. In addition, information on key aspects such as consent, exercise of statutory rights or transference of data were displayed along 8 pages document using vague and ambiguous expressions such as "we can" (twice) or "it is possible (4 times), or "improving user experience".

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 165-184

After December 2009 privacy notices update, on 29 November 2011 Facebook agreed to settle eight FTC charges that it had deceived consumers. It seems an irony that, on the same date, the founder of Facebook said: "Overall, I think we have a good history of providing transparency and control over who can see your information."

Most of counts alleged by the FCT's complaint had to do with false or misleading statements made by Facebook in its privacy policy.

Chart 1. *Misrepresentation of privacy policies*

In the Matter of Facebook, Inc., 27 July 2012		
Complaints	Count 1	Facebook's deceptive privacy settings conveying that users could restrict access to their profile information to specific groups when using Platform Applications (PA).
	Counts 2 and 3	Facebook's unfair and deceptive December 2009 privacy changes which made public certain information that users designated as private without their informed consent.
	Count 4	Facebook's false or misleading representation of the scope of PA' access to users' information limited to user profile information that the PA needed to operate.
	Count 5	Facebook's false or misleading representation of non-disclosure of user information to advertisers.
	Count 6	Facebook's deceptive verified apps program.
	Count 7	Facebook's false or misleading representation of non-disclosure of user photos and videos from deactivated or deleted accounts.
	Count 8	Facebook's false or misleading representation of compliance with US-EU Safe Harbour Framework in transferring personal data outside of the EU.

Source: FTC and own elaboration

For example, the FTC alleged that Facebook's December 2009 privacy changes were unfair and deceptive, by making public certain information that users had previously designated as private, including at least ten types of profile information (e.g., photos and videos, birthday, family and relationships, affiliations).

In the view of the FTC, Facebook failed to disclose, or did it inadequately, that users could no longer restrict access to that profile information by using privacy settings previously available to them. By making publicly available certain user profile information, and doing so retroactively without users' informed consent, "Facebook materially changed its promises that users could keep such information private", and had exposed "potentially sensitive information to third parties, namely, political views". The FTC considered that in light of

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 165-184

representations made by Facebook, the foregoing constituted "a deceptive act or practice" (FTC, 2012, 27, 28).

The settlement required Facebook to take several steps to keep its promises in future, by giving:

> *"A. Clearly and prominently disclose to the user, separate and apart from any "privacy policy," "data use policy," "statement of rights and responsibilities" page, or other similar document: (1) the categories of nonpublic user information that will be disclosed to such third parties, (2) the identity or specific categories of such third parties, and (3) that such sharing exceeds the restrictions imposed by the privacy setting(s) in effect for the user; and*
>
> *B. Obtain the user's affirmative express consent."*

According to the settlement, "clearly and prominently" would mean "in textual communications (e.g., printed publications or words displayed on the screen of a computer or mobile device), the required disclosures are of a type, size, and location sufficiently noticeable for an ordinary consumer to read and comprehend them, in print that contrasts highly with the background on which they appear." The settlement also explained the meaning of "clear and prominent notice" in communications disseminated orally or through audible means (e.g., streaming audio), or through video means (e.g., streaming video). In all instances, the settlement required disclosures which: "(1) are presented in an understandable language and syntax; and (2) include nothing contrary to, inconsistent with, or in mitigation of any statement contained within the disclosure or within any document linked to or referenced therein."

6. Concluding remarks: Legitimising the «Social Norm»

When asked in 2015 about their attitudes towards privacy, only 18% of European respondents said they read the privacy statements fully, while roughly half (49%) acknowledged to read them partially, and nearly a third of respondents (31%) said they did not read them at all (Eurobarometer, 2015, 84).

McCalling (2013, 124) thinks that it would be unfair to be "overly critical" of ISP's policy just because "[t]hey are merely protecting what they believe to be the expectation of their users in relation to their privacy settings and choices […]".

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 165-184

The UK Commissioner has stressed the contradictions of people's expectations: in first place, their willingness to share information on social media and mobile apps and their unwillingness to read lengthy privacy notices; in second place, their concerns about how organisations handle their data and how users want to retain control over its further use (2016, 3).

It is clear that former expectations have been used to enhance the so-called «Social Norm» by industry. By January 2010, Zuckerberg was of the view that "people have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people. That social norm is just something that has evolved over time." (CNET News, 10 January 2010). He later completed his view of what he called the «Social Norm»: "We are building a web where the default is social" (Schonfeld, 2010).

Remarkably, the WP29 (2009) had clearly stated just the opposite to Facebook´s «Social Norm», namely, the default should be "privacy" and any further access should be an explicit choice by the user on an opt-in basis, more protective towards privacy rather than opt-out consent.

A rationale behind the so-called "Social Norm" seems to be a fashionable construction of the old principle *caveat emptor*: «beware user». Or put it in a simple way: «user, you take all the risk», which in privacy notices parlance means "improving user experience".

Despite the foregoing approach on substantive and formal transparency as a prerequisite of meaningful consent and control over personal data, decisions made by such Authorities have not always been consistent with their findings.

Albeit in many investigations on ISP's privacy practices, Authorities have openly acknowledged the existence of misrepresentation, and lack of transparency of privacy policies, final decisions issued by them have been merely «recommendations» of "corrective measures" and "best practice[s] in the interest of clarity for users" (cf. Denham, 2009, 139, 141).

In some cases, dismissals of claims have avoided going into the consequences for users of such deceptive and misleading language. The Decision of 6 November 2008 issued by the Spanish AEPD, dismissed the claim of FACUA, a Spanish

ISSN 1989-7022
DILEMATA, año 9 (2017), nº 24, 165-184

Association representing consumers interests, against processing of users' data by Gmail service which neither permitted an opt out option nor required affirmative opt-in in relation to behavioural advertising. Though the Agency observed relevant "deficiencies" in privacy notices given by Google (e.g. the dissemination of information "through subsequent hyperlinks"), it concluded that registered users of Gmail had given an explicit –and thus valid– consent to such data processing. But there was a likely determinant argument subtly suggested by the AEPD: that behavioural advertising was price owed by users "in consideration of the *free service* rendered" by Gmail.

The Social Norm is here to remain, and today privacy seems to be not built anymore on the premise of individual's awareness and control. Instead, the rule of Law is slowly moving towards an understanding of privacy dealing with the handle "by default" of private information in the public domain consistent enough with the Social Norm.

One may agree with Warren and Brandeis' statement in their classic approach on *The Right to Privacy* that "[t]here are others who, in varying degrees, have renounced the right to live their lives screened from public observation" (1890-91, 215). If both prominent jurists had lived today, it is more than likely that they would have wrote that sharing our personal photos or marital status legitimises the «Social Norm» and means waiving any «legitimate expectation of privacy». Moreover, it might be reasonable to wonder, as Eady J. did in *Mosley v News Group Papers Limited* (2008), to what extent are we the authors of our "own misfortune".

References

Aleecia M. McDonald; Lorrie Faith Cranor (2008): The Cost of Reading Privacy Policies, *Journal of Law and Policy for the Information Society*, Vol. 4.

Article 29 WP (2009): *Opinion 5/2009 on online social networking* (WP 163), 12 June.

CISCO (2016): Visual Networking Index. Forecast and Methodology, 2015–2020, White Paper, June, http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/complete-white-paper-c11-481360.pdf

Denham, Elizabeth (2009): *Report of findings into the complaint filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc. under the Personal Information Protection and Electronic Documents Act*, Assistant Privacy Commissioner of Canada, 16 July, pp. 139, 141, 253.

European Commission (2010): *A comprehensive approach on personal data protection in the European Union*, COM(2010)609 final, 4 November.

(2010): *Attitudes towards Cross-Border Sales and Consumer Protection* (Flash Eurobarometer), March, No. 282.

(2011): *Attitudes on Data Protection and Electronic Identity in the European Union* (Special Eurobarometer), June, No. 359.

(2014): Case No COMP/M.7217 - FACEBOOK/ WHATSAPP, C(2014) 7239 final, 3 October.

(2015): *Data Protection Report* (Special Eurobarometer), June, No. 431.

(2016): *Mergers: Commission alleges Facebook provided misleading information about WhatsApp takeover*, 20 December, IP/16/4473.

Gibbs, Samuel (2016): WhatsApp and Gmail join the 1 billion user club, *The Guardian*, 2 February, https://www.theguardian.com/technology/2016/feb/02/whatsapp-gmail-google-facebook-user-app

Information Commissioner's Office (2013): *Annual Track 2013*, June, http://ico.org.uk/about_us/research/~/media/documents/library/corporate/research_and_reports/annual-track-2012-individuals.pdf

(2016): *Privacy notices, transparency and control. A code of practice on communicating privacy information to individuals*, 7 October, https://ico.org.uk/media/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control-1-0.pdf

Kosinski, Michal; Stillwell, David; Graepel, Thore (2013): Private traits and attributes are predictable from digital records of human behavior, *Proceedings of the National Academy of the Sciences of the United States of America*, Vol. 110, No. 15, http://www.pnas.org/content/110/15/5802.full

Kuner, Christopher *et al*. (2012): The challenge of 'big data' for data protection, *International Data Privacy Law*, Vol. 2, No. 2.

Lloyd, Ian J. (2011): *Information Technology Law*, Oxford, Oxford University Press.

McCallig, Damien (2013): Facebook after death: an evolving policy in a social network, *International Journal Law Information Technology*, Vol. 22, No. 2, http://ijlit.oxfordjournals.org/content/early/2013/09/25/ijlit.eat012.full.pdf+html

Spanish Data Protection Agency (2013): Decision R/02892/2013, of 18 December 2013.

Decision E/01544/2007, of 6 November 2008.

Schonfeld, Eric (2010): Zuckerberg: We are building a web where the default is social, *Techcrunch*, 21 April, http://techcrunch.com/2010/04/21/zuckerbergs-buildin-web-default-social/

Stucke, Maurice E.; Grunes, Allen P. (2016): *Big Data and Competition Policy*, New York, Oxford University Press.

Tene, Omer; Polonetsky, Jules (2012): To Track or «Do Not Track»: Advancing Transparency and Individual Control in Online Behavioral Advertising, *Minnesota Journal of Law, Science & Technology*, Vol. 3, Iss. 1, p. 321, http://cyberlaw.stanford.edu/files/publication/files/totrack-or-donotrack.pdf

(2013): Big Data for All: Privacy and User Control in the Age of Analytics, *Northwestern Journal of Technology and Intellectual Property*, Vo. 11, Iss. 5, http://scholarlycommons.law.northwestern.edu/njtip/vol11/iss5/1

United Kingdom Office of Fair Trading (2008), *Unfair contract terms guidance. Guidance for the Unfair Terms in Consumer Contracts Regulations 1999*, (Guideline 19.3), September, http://www.oft.gov.uk/shared_oft/reports/unfair_contract_terms/oft311.pdf

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 165-184

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 165-184

United States Department of Commerce (2010), *Green Paper: Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework*, Internet Policy Task Force, (December), http://www.commerce.gov/sites/default/files/documents/2010/december/iptf-privacy-green-paper.pdf

United States Federal Trade Commission (2010): *Protecting consumer privacy in an era of rapid change: a proposed framework for businesses and policymakers*, December, http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf

(2012), *In the Matter of Facebook, Inc., a Corporation*, Docket No. C-4365 (27 July) http://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookcmpt.pdf

(2013), *In the matter of Google, Inc., a Corporation*, Docket No. C-4336 (24 October) https://www.ftc.gov/sites/default/files/documents/cases/2011/10/111024googlebuzzcmpt.pdf

Williams, Alan; Calowm Duncan; Lee, Andrew (2015): *Drafting Agreements for the Digital Media Industry*, 2nd. Edition, New York, Oxford University Press.

Weichert, Thilo (2013): *Current Data Protection Challenges in Social Networks*, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, 19 November, https://www.datenschutzzentrum.de/vortraege/20131119-weichert-data-protection-social-networks.html

Notes

1. REGULATION (EU) 2016/679, of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

2. As to Article 12 of the Directive 95/46/EC, the data subject has the right to obtain from the data controller "confirmation as to whether or not *data relating to him are being processed* and information at least as to the purposes of the processing, the *categories of data concerned*, and the recipients or categories of recipients to whom the data are disclosed".

3. The results of the Spanish survey were presented by this author (2014): The people v. Facebook: transparency of privacy policies, *Winchester Conference on Trust, Risk, Information and the Law* [not published] 29 April, University of Winchester, http://www.winchester.ac.uk/academicdepartments/Law/Centre%20for%20Information%20Rights/Next%20Event/Documents/TRILCon%20prog%20final%20v0.2.docx. The sample included 100 students aged 21-25 of Universidad Carlos III de Madrid, and CES Felipe II which was then affiliated to the Universidad Complutense de Madrid.

4. Letter to Facebook regarding WhatsApp updated Terms of Service and Privacy Policy (27/10/2016); Letters to Microsoft and Yahoo! (16/01/2015), and Google (6/01/2015) on the right to be delisted; Letter to Google regarding Google Glass, a type of wearable computing in the form of glasses (18/06/2013); Letter to Google regarding the upcoming change in their privacy policy (02/02/2012); Letter to search engine operators Google, Microsoft and Yahoo! (26/05/2010), amongst others.

5. Question number 8 of the questionnaire reproduced an excerpt of the Spanish version of the clause: "PROPORCIONAMOS FACEBOOK TAL CUAL, SIN GARANTÍA ALGUNA EXPRESA O IMPLÍCITA, INCLUIDAS, ENTRE OTRAS, LAS GARANTÍAS DE COMERCIABILIDAD, ADECUACIÓN A UN FIN PARTICULAR Y NO INCUMPLIMIENTO […] NO SEREMOS RESPONSABLES DE NINGUNA PÉRDIDA DE BENEFICIOS, ASÍ COMO DE OTROS DAÑOS RESULTANTES, ESPECIALES, INDIRECTOS O INCIDENTALES […]"