Received 19 October 2014
Revised 1 February 2015
14 March 2015
26 March 2015
8 May 2015
Accepted 9 May 2015

"Privacy by default" and active "informed consent" by layers

Essential measures to protect ICT users' privacy

Amaya Noain-Sánchez
Complutense University, Madrid, Spain

Abstract

Purpose – The purpose of this paper is to lay out an approach to addressing the problem of privacy protection in the global digital environment based on the importance that information has to improve users' informational self-determination. Following this reasoning, this paper focuses on the suitable way to provide user with the correct amount of information they may need to maintain a desirable grade of autonomy as far as their privacy protection is concerned and decide whether or not to put their personal data on the internet.

Design/methodology/approach – The authors arrive at this point in their analysis by qualitative discourse analysis of the most relevant scientific papers and dossiers relating to privacy protection.

Findings – The goal of this paper is twofold. The first is to illustrate the importance of privacy by default and informed consent working together to protect information and communication technology (ICT) users' privacy. The second goal is to develop a suitable way to administrate the mentioned "informed consent" to users.

Originality/value – To fulfil this purpose, the authors present a new concept of informed consent: active "informed consent" or "Opt-in" model by layers. "Opt-in" regimens have already been used with cookies but never with 2.0 applications, as, for instance, social network sites (SNS).

Keywords Privacy, Internet ethics, Users

Paper type Viewpoint

1. Introduction

The protection of personal data in the internet has gained significant attention because of the increased collection of private information online and the superior capabilities for searching, tagging and aggregating this information that new information and communication technologies (ICTs) provide. This is not a minor issue; therefore, it is not surprising that in recent years, there has been a lot of interest in studying issues relating to privacy concerns that users have and how these might affect their online activities. Governments from several democratic countries, as well as public and private institutions, are forced to face these new challenges for data protection, underlining an urge for a new set of rules and technical improvements aimed principally to enforce users' control over data and enhance their informational self-determination.

In line with it, in 2011, the German National Academy of Science and Engineering (ACATECH) launched a project that focuses on the privacy dilemmas associated with the internet, developing recommendations for a "culture of privacy and trust", core values and conditions to increase a safer use of ICT. The term "culture" has not been chosen at random. It is used to emphasize that dealing with the privacy dilemmas

Journal of Information, Communication and Ethics in Society
Vol. 14 No. 2, 2016
pp. 124-138

1477-996X
DOI 10.1108/JICES-10-2014-0040

requires a complex approach that combines education and good practices with appropriate legislation and technology. Culture allows users to assess and choose the suitable degree of privacy on the internet depending on their preferences and the respective context, hence its importance. Within this culture of privacy, education, good practices, law and technology are developed in such a way that this choice becomes possible (ACATECH, 2013).

Addressing the translational dimension of this issue, in 2012, the European Commission proposed a major reform of the European Union (EU) legal framework on the personal data protection (European Commission, 2012a). The current EU Data Protection Directive 95/46/EC does not consider important aspects like globalization and some ICT developments; therefore, a proposal for a regulation was released on January 25, 2012, published in 2013, and it is expected to be finally adopted in 2015.

This reform aims to unify data protection with a single law, the General Data Protection Regulation (GDPR). This new draft European Data Protection Regulation strengthens individual rights and tackles the challenges of globalization and new technologies, seeking to extend the scope of data protection legislation beyond the EU boundaries for the first time. The changes introduced will help to improve personal data protection for individuals in the following ways:

- Imposing the "Right to be Forgotten" to allow people to delete their data if there are no legitimate reasons for retaining it "so that third persons can no longer trace them" (Weber, 2011, p. 121). Although the concept described is derived from several pre-existing European ideals, the term "Right to be Forgotten" is relatively new. It was on May 30, 2010 when the European Court of Justice legally solidified that it is a human right when they ruled against Google in the Costeja case (Court of Justice of the European Union, 2014).

The 2012 draft European Data Protection Regulation Article 17 details the "Right to be Forgotten" for the first time. Under Article 17, individuals will be able to:

> Obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject whilst he or she was a child or where the data is no longer necessary for the purpose it was collected for, the subject withdraws consent, the storage period has expired, the data subject objects to the processing of personal data or the processing of data does not comply with other regulation (European Commission, 2012c):

- Reinforcing the role of National Data Authorities.
- There will be increased responsibility and accountability for those processing personal data. At this point, new regulation introduces a notably innovation: People will be able to refer cases where their data have been breached or rules on data protection violated to the Data Protection Authority in their country, even when their data are processed by an organization based outside the EU. Additionally, it will apply in those cases where personal data are processed abroad by companies that are active in the European Market. This will give people in the EU confidence that their data are still protected wherever it may be handled in the world.
- People will have easier access to their own data and be able to transfer personal data from one service provider to another more easily.

- Introduction of "privacy by default" and "informed consent". Both are key concepts in the protection of personal data, as much qualitative research into ICT users' behaviour shows that they are usually unaware of how their information is being stored, for how long and the purpose of this collection. (Young *et al.*, 2011; Lipford and Besmer, 2010).

Within this framework, the present paper aims to explain first the importance of "informed consent" as an instrument to provide users appropriate information to protect their privacy. Subsequently, it underlines the suitability of its implementation as "opt-in" model by layers.

1.1 The importance of user's knowledge to protect their privacy and develop their "informational self-determination"

Within this "culture of privacy and trust" and in conjunction with an updated regulation, knowledge and digital competences play an essential role to mitigate privacy breaches in online-mediated environments. They both represent common themes linked to user's necessities to understand the functioning of digital environments to evaluate the possible repercussions their actions may involve for their privacy. Therefore, knowledge in the form of a correct flow of information becomes necessary to understand correctly the contextual norms governing in this scenery, indicating the quantity of personal information it is necessary to display in each context to satisfy social interaction (Nissenbaum, 2004). At the same time, it helps users to evaluate the privacy expectations when introducing their personal data in mediated public spaces. For that reason, it has been frequently mentioned Nissenbaum's "contextual integrity" theory, as it provides a useful framework to consider the protection of privacy on digital environments. In addition, it is able to deal with many different conceptions of privacy enrooted in every culture (Capurro, 2005, p. 37), as well as the dynamic process of boundary negotiation that distinguishes privacy and publicity according to circumstances (Altman, 1975). Furthermore, it links with essential concepts concerning the protection of personal data on mediated environments: the necessity of a correct flow of information to identify every context and respect the contextual integrity, as well as the suitability of improving an active role of users to enforce their decisional autonomy.

From this premise, users may be able to choose which data display depending on the context, and thus, privacy protection could be translated as "the ability for people to choose and control what they disclose and what the hide" (ACATECH, 2013, p. 14). As a result, privacy is closely connected to the basic right to "informational self-determination[1]", and consequently, knowledge about digital environments becomes an essential requirement to enable citizens to eject efficiently their privacy rights.

As Rössler points out, protecting privacy may take into account at least three different dimensions: "decisional privacy", "informational privacy" and "local privacy"; three necessary areas for individuals to control aspects of themselves, to be able to express themselves and to act accordingly to their own values and plans (Rössler, 2005). On her view, the violation of the right to privacy is a violation to the person's autonomy, as:

> […] privacy protects autonomy in those respects in which the exercise of autonomy is dependent upon my control of the access of others to me, to my person, to my (reflects on) decisions and to information about me (Rössler, 2005, p. 73).

The connections between privacy, autonomy and democracy are so close that it does not seem accurate to say that one is instrumental to the other. As Deborah Johnson outlines, "privacy, autonomy and democracy are so intertwined that one is inconceivable without the other. Privacy is not just instrumental to autonomy or democracy; it is essential to both" (Johnson, 2009, p. 97):

> The idea of democracy is the idea that citizens have the freedom to exercise their autonomy and in so doing develop their capacities to do things that have not been thought of before. Democracy requires citizens who are capable of critical thinking, individuals who can argue about the issues of the day and learn from the argument so that they can vote in […]. The argument for privacy is, then, an argument for the space that individuals need to develop autonomy (Johnson, 2009, p. 97).

1.2 User's knowledge, a key concept to make conscious decisions in social network sites

A correct flow of information about the possible repercussions of introducing private data in some of the contexts created by ICT plays an essential role both, to ensure informational self-determination and to avoid breaches on the contextual integrity. Therefore, receiving transparent information becomes fundamental to prevent users from suffering undesirable privacy intromissions. From this premise, Nissenbaum' theory provides a valuable framework to mitigate privacy breaches on mediated environments. Nonetheless, from the point of view of its practical execution, applying contextual norms is not so simple. One field of study that has drawn particular concern is the provision of private data on social network sites (SNS) defined as.

Web-based services that allow individuals to:

- construct a public or semi-public profile within a bounded system;
- articulate a list of other users with whom they share a connection; and
- view and traverse their list of connections and those made by others within the system (Boyd, and Ellison, 2007).

There are two main reasons for such increased concern:

(1) SNS symbolize a unique social sphere, where huge amounts of private information are stored and aggregated (Govani and Pashley, 2005).

(2) Information provided on these sites can easily be copied, forwarded, replicated and taken out of context (Boyd, 2006).

Users may find several difficulties to understand and control boundaries in these mediated environments (Palen and Dourish, 2003). Moreover, contextual integrity depends on the contextual information, whereas offline privacy is mediated by highly granular social contexts, digital communication, especially SNS, lack much this granularity, and thus, users find themselves incapable of exercising their right to informational self-determination (Hull *et al.*, 2010, p. 289). Furthermore, the ambiguity of some SNS such as Facebook, make it difficult for users to determinate whether it is a public space or not (Young and Quan-Hasse, 2013, p. 482) and even when users are aware of that, third developers create added functionalities that may break the contextual norms prescribed by Nissenbaum. As a result, online tools seem to create a new environment characterized by the collapsing of contexts (Boyd, 2008, p. 3).

Therefore, despite developing a more suitable regulation and enhancing a culture of privacy, the main drawback we find when trying to protect users' privacy is the ambiguity inherent to SNS. Thus, the challenge we may face is how to proportionate SNS users enough information to become them capable of deciding which and how many private information is needed to display in each context to protect them and, at the same time, to satisfy social interaction.

2. Why informed consent

From the point of view of legal theories, the right to privacy is considered a personality right, directly pointing at "informed consent" as the specific tool to draw the line between the legitimated or unauthorized use of personal information. In addition, as one of the key concepts for data protection is the purpose given to our data after collection, wherever consent is required for data to be processed, it will have to be given explicitly, rather than assumed as is sometimes the case now.

For that reason, it is common to see calls for "informed consent" from National Data Protection Authorities, organizations and several groups of citizens. Focusing on Europe, according to *Special Eurobarometer 359* from European Commission, over 70 per cent people said they were concerned about how companies use their data and over 74 per cent wanted to give their specific consent before their data are collected and processed on the internet (European Commission, 2011).

As a rule, the acquisition and use of personal data requires the informed and voluntary consent of the person in question (ACATECH, 2013, p. 25). In fact, the current Data Directive ensures that processing of personal data meets three conditions: "transparency", "legitimacy" of purpose and "proportionality" (European Parliament and the Council of the European Union, 1995). "Transparency" means that a person is explicitly informed of the specific purpose when their personal data are processed. "Legitimacy" of purpose means that the purposes for which personal data are processed are legitimately related to the business needs of the data controller. "Proportionality" means that personal data must be processed only to extend compatible with the explicitly stated purpose (Fairweather *et al.*, 2011, p. 474). "Informed consent" comes to fulfil these three requirements; therefore, most probably new Data Protection Regulation will include this measure.

This implementation is a technical tool aimed to explain users how their data will be used and with whom will be shared, as well as the use given by third companies' applications. In other words, it is an imposition upon actors who collect or use information to provide and explain users the purposes of such data collection and how they will manage it (Nissenbaum and Barocas, 2009). After receiving the information, users being aware of the possible consequences of introducing private data on the internet (informed) are supposed to be capable of deciding whether they display personal information or not (consent).

The correct introduction of "informed consent" may prevent people from suffering much of the privacy violations they experiment when interacting with some ICT, in particular as far as SNS are concerned. Among them, Facebook, created in 2004 by Mark Zuckerberg, has received criticism on a wide range of issues relating to privacy, including targeting and tracking down users and using tricky privacy policies. Besides, there is a huge amount of research showing that users do not understand completely the

implications of some actions even after having read security dialogs and warnings, usually because of the misleading statements writing on these texts.

For that reason and to verify the efficiency of "informed consent", it should be obtained in such a way as to ensure that users know exactly what they are consenting to. Therefore, it has to be easy enough to be understood by the whole audience in contraposition to those illegible privacy policies or the current SNS "Terms of Use" written in a tricky and complex language.

2.1 Passive informed consent or "opt-out" model

The moral legitimating of informed consent stems from the belief that it respects individual autonomy, specifically, that it reflects rational and informed decisions as far as the management of private data is concerned (Nissenbaum and Barocas, 2009). If the social contract signed by all the actors involved in the digital world become a moral imperative to certificate a correct functioning of the ICT (Mason, 1986, p. 11), then it seems to be logical that a tool to give freely and informed permission might solve the majority of the privacy infringements produced.

Nonetheless, much of the controversy that surrounds "informed consent" derives from the competing views of the proper implementation of this tool. This controversy refers to hegemonic approach to informed consent as an "opt-out" model, forming it as a defensive tool based on a passive role of users. That really means that it is the user who constantly is forced to refuse the permission to prevent their data from being public, on the grounds that default settings provide the minimum level of protection. Accordingly, "opt-out" model is based on a notion of passive consent with opportunities for revocation and users are forced to deny a predefining action which is aimed to confer the higher level of visibility to their data. In view of that, it seems to be though by some internet companies to give users false expectations of privacy control. Hence, this model is, in all likelihood, a tricky manoeuvre to extend the mistaken belief that people have informational self-determination.

On its implementation over Facebook's Beacon, "opt-out" regimens were also a factor for controversy. Facebook Beacon was a part of Facebook's advertisement system which works sending data from external websites to Facebook, for the purpose of allowing targeted advertisements. Beacon would report to Facebook on its member's activities on third-party sites that also participate with Beacon. This Facebook's advertisement program announced to one's friend what one had just bough using "opt-out" model to agree o decline permission. However, if user forgot to decline to share something, then the application still went ahead and shared it with their friends (Johnson, 2009, p. 104).

These reasons come to underline the fact that though "informed consent" might assure a safer navigation as far as ICT are concerned, it is fundamentally inadequate under the technical conditions that it currently holds. Consequently, we must rethink this tool which could become much more effective under a necessary redefinition, as well as working in conjunction with the implementation of "privacy by default".

3. Privacy by default and active informed consent

"Privacy by design" means that data protection is designed into the development of business processes for products and services, and therefore, privacy settings are set at a high level by default (European Commission, 2012c). Within this framework, "informed consent" would be improved as an "opt-in" model and in the way that we propose in the following lines.

3.1 Privacy by default

"Privacy by design" and "privacy by default[2]" means that privacy safeguards will have to be integrated into products as they are developed – an approach to systems engineering which takes privacy into account throughout the whole engineering process – as well as in social networking, the default settings must protect the privacy of individuals. The concept was originated in 1995, in a report on "Privacy Enhancing Technologies" by a joint team of the Information and Privacy Commissioner of Ontario, Canada, the Dutch Data Protection Authority and The Netherlands Organisation for Applied Scientific Research (Hustinx, 2010, p. 253). "Privacy by design" which framework was developed by Dr Ann Cavoukian, the former Information and Privacy Commissioner of Ontario, starts from the point that the future of privacy cannot be assured solely by compliance with legislation and regulatory frameworks; rather, privacy assurance must become an organization's default mode of operation. (Cavoukian, 2009). In October 2010, this new framework was recognized as the global privacy standard in a landmark resolution by the International Conference of Data Protection and Privacy Commissioners in Jerusalem.

"Privacy by default", which is already mentioned as an innovative principle in the new EU Draft Data Protection, means that data protection safeguards should be built into products and services from the early stage of development and privacy-friendly default settings should be the norm, for example, on SNS. This change would strengthen individual's right in a practical way, as all the applications would provide, by design, the higher level of protection. In this context, it is the user who decide whether changing or not privacy settings depending on their desires for privacy or their visibility objectives. To embed privacy standards by design would avoid some privacy breaches taking place as, for instance, the automatic index of personal information without users' permission.

3.2 Active informed consent or "opt- in" model

Within the new scenery created by setting in "privacy by design", "informed consent" would be improved as an "opt-in" model. This would return to users the active role in their privacy protection. Thus, it suggests that less effort is required of users who would not find themselves forced to deny permission whenever they introduce personal information. On the contrary, consent would be required only in those cases when they decide to confer more visibility to their data.

"Opt-out" regimens come to justify the use of personal data by digital applications rather than providing users' control over their data. By implementing "opt-in" models, however, it is the user, from the very beginning, who controls whether to give visibility to their data or not, reason why it is also known as "active consent". As Deborah Johnson states, the use of "opt-in" rather than "opt-out" goes hand in hand with transparency, treating us as rational beings capable of making decisions, rather than passive objects to be manipulated:

> Given how little information consumers, clients and citizens have about information practices, the "opt-out" strategy seems unfair if not deceptive. Personal information is gathered and used and if we figure out what is happening we can opt-out. By contrast, if organizations cannot use personal information about us unless they get our permission, then they have to inform us of their practices and convince us that we want to opt-in (Johnson, 2009, p. 105).

Currently, no SNS introduce "informed consent" as an active (or "opt-in" regime) nor even it is mentioned in any data protection rule in force. However, in the present

research, we do affirm that it could become an interesting instrument to both protect users' privacy and to confer a certain degree of control over personal data. In the following pages, we will offer a suitable way in which it could be brought into play.

4. Active "informed consent" by layers

One of the main shortcomings we find when introducing informative tools such as "informed consent" is how to provide users with enough easy-to-understand information to illustrate them with the possible repercussions of giving more visibility to their data. In addition, we must reflect on how to proportionate information in the most useful way. For that reasons, we recommend a system of informative layers, a model which is already in use to agree or deny permission regarding the cookies, but has never been applied to consent.

4.1 Design heuristics

For user competence to be possible, they need to know which of their data are being held, where they are being held and what the consequences for their privacy are (ACATECH, 2013, p. 29). To accomplish these requirements, the system we propose would work in two informative layers that would appear automatically. Each one will have as many levels as possible actions the user might carry out. In developing this approach, the information provided by layers would appear in the following way (Table I).

To fulfil users' mental models, the cases explained on first layer must be completed with more potential cases, always depending on the visibility level users have decided to confer to their data. This information would be enunciated via propositions:

> When you activate this setting/if you permit this action you consent that […].

To supply illustrating examples from "layer two", we could bring into play not only text but preferably interfaces created by simulation programs to explain, in a more visual way, how our data would be shown to others or how it may be used by thirds parties. It is important, at this point, to mention simulation programs as, for instance, the one developed in University of North Carolina at Charlotte by Lipford (2010).

First layer Basic information (provided in a schematic way)		Second layer Further information
The purpose of data collection	How data will be used How long it will be stored Where will be stored	Depending on the level of visibility chosen by the user, it will appear an informative layer showing the consequences of giving more publicity to their data
Property rights involved	How the property of information will change	
Data collected by cookies Data collected by third companies	Data shared when using applications	Illustrating examples will be provided and there will be an explanation of how to deny any action
Privacy protection and others' actions	Public indexations How our data will be showed to others	
How to turn down actions previously taken		

Table I.
Informed consent by layers

4.1.1 Enhancing usability. "Informed consent" application should be illustrated using specific colours and icons to facilitate users to identify the potential risks that a change for more visibility may involve, as well as to help them to internalize these processes. In addition, the application would save a file recording the actions formerly taken, such as previous settings or prior actions details. This file is aimed to remind them which data were made public, thus avoiding users feeling forced to rely on their own memory for something the system already knows. Additionally, the interface may provide, automatically, visual cues, reminders, lists of choices and other aids. We can not forget that humans' brain works better with recognition than recall and by choosing to be consistent with references an interface can be made easier to learn. Consequently, the introduction of images and concepts users already know and recognize will contribute to make them feel comfortable with any action taken. If user's actions cause not expected outcomes, then there will be the possibility of turning it down – users feel more comfortable with interfaces in which their actions do not cause irreversible consequences.

Within the "privacy by default" framework, it is the user who decides whether or not to change by design settings to confer more visibility to their data. When they post, for instance, they may change privacy settings from "only visible to my friends" to "public to all the people" using the platform. Consequently, it would appear a first layer of information, indicating the likely repercussions this action may involve regarding their privacy protection. At this point, users have three ways of action:

(1) to assume the possible outcomes of changing their privacy protection level and agree the consent;

(2) to deny consent; and

(3) to continue to the second layer to obtain more information.

And the same sequence would appear on the second layer.

Some users decide to confer less privacy protection to their data. This is because they do not think there is a good reason to hide it or they feel there will not be regrettable consequences. In those cases, whenever users decide to change for a higher level of visibility, they will receive much more information than at lower visibility levels – more visibility involves more risks; therefore, a larger amount of information is needed. As the system of information in two layers would appear only when the users decide to confer a higher level of publicity to their data, it would be much more comfortable for users than passive "informed consent" which forces them to deny or agree at whatever time they introduce a data or activate any change.

In a schematic way, the actions to be taken by users when modifying by default settings would be shown as a vector going from the inside to the outside of several concentric circles, from the maximum level of protection to the minimum at any time users confer more visibility to their data.

4.2 Limitations

As far as privacy protection is regarded, we must admit that there are no catch-all solutions, not even using "informed consent". Taking this into account, we have to outline the following disadvantages.

4.2.1 Users' contradictory behaviour. Commonly, when we examine the relation between supplying with information and its impact on users' decisions, we observe

contradictory behaviours towards protection. We must admit that it is not always the expectation of privacy what motivates users' actions in SNS. Users are currently willing to share large amounts of personal information and giving up the control over it (Wester and Sandin, 2011, p. 90). Additionally, it has been already observed the phenomena known as the "privacy paradox" which involves users' paradoxical behaviour relating to privacy concerns on SNS (Barnes, 2006). Moreover, the majority of worries were not about privacy protection: users usually show regrets when there was a possible breach in reputation (Lampe *et al.*, 2008, p. 720; Madden and Smith, 2010; Young and Quan-Hasse, 2013, p. 483). With regards to children and young people, we must point out that although privacy by default seems to be an effective tool to protect them, we can find problems relating to "informed consent". This is because the complex sceneries which may appear turn into a difficult task to translate into a simple language the wide range of potential risks and its further repercussions.

4.2.2 Legal limitations. As far as responsibility and accountability for those processing personal data are concerned, new European Data Protection Regulation introduces a notably innovation: European citizens will be able to refer cases where their data have been breached or rules on data protection violated to the Data Protection Authority in their country, even when it is processed by an organization based outside the EU. Additionally, this set of rules will apply even if personal data are processed abroad by companies that are active in the European Market. Nevertheless, there is no explicit mention relating to the use of "informed consent" or "privacy by default" if an enterprise is based outside the EU as it is the case of the majority of SNS.

Taking into account that SNS platform businesses depend on collecting as much as possible information from users – including personal information – to target and track people, it is unlikely they will be willing to support a measure which most probably would damage their business model.

In this context, despite the Data Commissioner claiming that new EU rules will apply even if personal data are processed abroad by companies which are based on the European Market (European Commision, 2012b), there might probably be disputes over competences and attributions of each jurisdiction. SNS and other internet companies may allege that if their main headquarters are based on the USA, they are force to act within the USA normative framework which tends to be laxer with the protection of privacy data. And even when several companies such as Facebook have opened headquarters in Europe, if they are mainly based in USA, they could allege legal reasons not to collaborate with European Data Authorities. There should be, in this case, overlapping of competences, functions and powers between jurisdictions.

In the USA, there is no single, comprehensive federal (national) law regulating the collection and use of personal data. Instead, the USA has a patchwork system of federal and state laws and regulations that overlap, dovetail and may contradict one another. In addition, there are many guidelines, developed by Governmental Agencies and industry groups that are not legally enforceable but are part of self-regulatory efforts and are considered best practices. Among aforementioned myriad of regulations, there is no outlook of implementing "informed consent" in mediated environments. Furthermore, the many legal gaps which exist and the fact that data protection is, by far, much laxer than in Europe could benefit the business model of companies like Facebook.

In spite of the many petitions from the National Data Authorities, administrations and other institutions to clarify which data collect and for which purposes, there is, as

yet, no uniformity in how many and what kind of data capture companies like Facebook – and not only Facebook, after several requirements from the US authorities, as well as some governments in Europe, powerful enterprises such as Google have never clarified the kind and amount of data they collect. Under such conditions, therefore, the implementation and correct functioning of "informed consent" would turn into an impossible task.

4.2.3 Conceptual limitations: consent and the information of others. One of the main challenges for our privacy since the arrival of SNS is the possibility of our privacy being damaged by other's action. This is prone to happen as a result of the lack of control over personal data that the use of some ICT involves. Consequently, when sharing information on SNS, "it is not only necessary to consider the privacy of, but the privacy of the information of others who may be tied to the information being shared" (Parrish, 2010). The digital landscape with its ever-increasing ability to capture, compute and communicate data facilitate that the contents we put on the SNS may involve other's personal information. In this case, "informed consent" might not be a suitable tool to prevent the countless data breaches produced by other's sharing data, as it refers, by essence, to one's personal information, that is to say, to one's self-informative determination.

Following this line of reasoning and taking into account Parrish reflections on social contracts (Parrish, 2010) that may govern actions in the interconnected world, we must admit that even using "informed consent" the expectation of whole privacy is not always valid.

Parrish introduces this problematic with the following example:

> Imagine that an individual takes pictures at a private social gathering and posts them on a SNS. What if a member […] who is pictures in those images desactivates their account? Do they disappear from the images? […] Furthermore, what are the chances the person posting in the pictures provides informed consent to every individual captures in the images? What about those individuals who indicate what others are doing in their status updates, do they provide informed consent? (Parrish, 2010).

The practical implications of revealing personal data about oneself and others extend beyond immediate impact in virtual world and when information is released on the SNS, it is difficult to regain control over. In addition, as it becomes opaque to what extend their personal data are on the internet, this information could build a dossier of people even if they decide not to participate in the digital world.

4.2.4 Technical limitations. There are, of course, certain technical features that limit the efficiency of this application. The technical shortcomings refers, mainly, to the diversity and amount of potentially dangerous context that may appear in some moments as, for instance, when registering into a SNS, posting or sharing a photograph, especially if it involves tags relating to others. The amount of information the user might receive in that moment may be excessive and the quantity of layers which might appear could discourage users from using that service. This complexity might well go further especially as far as users with mobile devices are concerned, for that reason we must face the challenge of how to provide large amounts of information in smaller interfaces, whilst being highly illustrative at the same time.

Nevertheless, the main drawback may be the difficulty to explain exactly to what extend their personal data may be used, that is to say, which are the concrete implications of giving more visibility to their personal data or using some applications.

In line with Nissenbaum and Barocas' (2009) argumentations, this tool is not enough to confer informed permission, as "it attempts to render participation a matter of choice, but generally fails to explain whether a user agrees to tracking, targeting or both". To ask the user whether they permit or deny being targeted, tracked down or both, may be a difficult task, as it is not so easy to explain the possible repercussions of carrying out each action. In addition, it may pose a real challenge to develop this tool, as internet enterprises rarely contribute to clarify how they manage that information.

5. Conclusion

Current research contributes to conceptualise "informed concept" as "opt-in" model by layers to protect users' privacy with a view to informing a future prototype. The paper has portrayed the necessity of this technology underlying users' requirements for information to carry out informed decisions about their actions in mediated environments, especially as far as SNS are concerned.

Despite disclosing information on the internet – including personal data – is an increasing part of modern life, it is necessary to ensure that privacy is protected in a way that does not prevent users from continuing using ICT. In line with it, the development of "informed consent" would offer users a reasonable degree of privacy, as well as confidence that their interaction with digital media may not involve undesirable repercussions.

For user competence to be possible, they need to know which of their data are being collected and what the consequences for their privacy are. Once they understand the possible repercussions, they are capable of making conscious decisions relating to their expectations for privacy, defining and configuring their preferences. For that reason, a correct implementation of this measure could contribute to strengthening users' informational self-determination by giving them the capacity of decide whether to introduce their privacy data or not, depending on their visibility objectives. To fulfil all the requirements, "informed consent" as a privacy-friendly design would clearly call for users' decisions and degrees of opting-in should support users' needs for informational autonomy, in getting out of the trap of submitting all their private data as a trade-off for functionality.

This premise works together with the majority of recommendations for privacy regulation and guidelines the development of a culture of privacy involves: a complex approach that combines education and good practices with appropriate legislation and technology in such a way that this choice becomes possible. Taking into account that it is the citizen the main actor in the digital revolution, authorities, enterprises, institutions and all the agents involved are duty bound to improve this culture of privacy as far as digital technologies are regarded. It is particularly important, as these technologies have become, nowadays, the most important instrument to obtain and spread information, and therefore, its correct use is a key concept to promote and preserve the values of a democratic society.

Concerning regulation, to guarantee the right to personal data protection in the future and focusing on the importance of giving more control over personal data to users, the European Commission proposes update and modernises the principles enshrined in the 1995 Data Protection Directive underlining explicitly "privacy by default" and "informed consent" as essential tools to preserve users' desires for privacy.

The implementation of "informed consent" under the conditions explained above offers flexibility with respect to other tools to protect privacy and interoperability with respect to existing "privacy by design". We must underline, however, the complexities of digital environments have to be taken into account when designing privacy protection strategies, specially pointing at such described shortcomings which may obscure the process of implementation. Still, supplying "informed consent" should not absolve digital platforms, third parties or other agents involved of their responsibilities.

The implementation of measures and regulation should be used, nevertheless, not only to define privacy responsibilities but to promote a safer navigation. Safety is a collective good necessary for a democratic society (Regan, 2003), which goes hand in hand with the supplying with correct flows of information to improve user's understanding of digital environments. As a result, "informed consent" may help to provide them the suitable critical framework they may need to carry out their decisions and, therefore, their informational self-determination desires.

We expect the findings of current research to supply viable solutions both for users to improve their privacy needs and for promoting a safer use of new information and communication technologies.

Notes

1. The notion comes from the German concept "*Recht auf informationelle Selbstbetsimmung*".
2. We use the expression "privacy by design" when we refer to the industry and "privacy by default" relating to users.

References

ACATECH (Ed.) (2013), *Internet Privacy: Taking Opportunities, Assesing Risk, Building Trust*, ACATECH Position Paper Series, Munich.

Altman, I. (1975), *The Environment and Social Behaviour*, Brooks/Cole, Monterey, CA.

Barnes, S.B. (2006), "A privacy paradox: social networking in the United States", *First Monday*, Vol. 11 No. 9, available at: http://firstmonday.org/ojs/index.php/fm/article/view/1394/1312 (accessed 29 May 2014).

Boyd, D. (2006), "Friends, friendsters, and myspace top 8: writing community into being on social network sites", *First Monday*, Vol. 12 No. 11, available at: www.danah.org/papers/FriendsFriendsterTop8.pdf (accessed 2 October 2013).

Boyd, D. (2008), "Taken out of context: Americam teen sociability in networked publics", available at: www.danah.org/papers/TakenOutOfContext.pdf (accessed 3 October 2014).

Boyd, D.M. and Ellison, N.B. (2007), "Social network sites: definition, history, and scholarship", *Journal of Computer-Mediated Communication*, Vol. 13 No. 1, pp. 210-230.

Capurro, R. (2005), "Privacy: an intercultural perspective", *Ethics and Information Technology*, Vol. 7 No. 1, pp. 37-47.

Cavoukian, A. (2009), *Privacy by Design*, Office of the Information and Privacy Commissioner, available at: www.privacybydesign.ca/content/uploads/2009/01/privacybydesign.pdf (accessed 3 October 2014).

Court of Justice of the European Union (2014), *Judgment in Case C-131/12 Google Spain SL, Google Inc v Agencia Española de Protección de Datos*, Mario Costeja Gonzalez, available at: http://europa.eu/rapid/press-release_CJE-14-70_en.htm (accessed 12 February 2015).

European Commission (2011), *Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union*, available at: http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf (accessed1 July 2014).

European Commission (2012a), *Commission Proposes A Comprehensive Reform of Data Protection Rules to increase Users' Control of Their Data And to Cut Costs for Businesses*, available at: http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm european commission (accessed 27 December 2014).

European Commission (2012b), *Data Protection Reform: Frequently Asked Question: Why Do We Need to Reform the EU Data Protection Rules?*, available at: http://europa.eu/rapid/press-release_MEMO-12-41_en.htm?locale=fr (accessed 12 February 2015).

European Commission (2012c), *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), 2012/0011 (COD)*, available at: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=uriserv:OJ.C_.2012.229.01.0090.01.ENG (accessed 12 April 2016).

European Parliament and the Council of the European Union (1995), "Directive 95/46/EC", *Official Journal of the European Union* n. 281, pp. 0031-0050, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.1995.281.01.0031.01.ENG (accessed 12 April 2016).

Fairweather, B., Ashman, H. and Wahlstrom, K. (2011), "Brain computer interfaces: a technical approach to supporting privacy", in Rogerson, S., Arias-oliva, M., Ward Bynum, T. and Torres-Coronas, T. (Eds), *The "Backwards, Forwards and Sideways" Changes of ICT, Proceedings of the Eleventh International Conference, Ethicomp 2010, Universidad Rovira I Virgili, Spain*, pp. 580-586.

Govani, T. and Pashley, H. (2005), "Student awareness of the privacy implications when using Facebook", *Privacy Poster Fair at the School of Library and Information Science*, Carnegie Mellon University, Pittsburgh, PA.

Hull, G., Lipford, H.R. and Llatulipe, C. (2010), "Contextual gaps: privacy issues on Facebook", *Ethics and Information Technology*, Vol. 13 No. 4, pp. 289-302.

Hustinx, P. (2010), "Privacy by design: delivering the promises", *Identity in the Information Society*, Vol. 3 No. 2, pp. 253-265.

Johnson, D. (2009), *Computer Ethics*, Pearson, Upper Saddle River, NJ.

Lampe, C., Ellison, N.B. and Steinfield, C. (2008), "Changes in use and perception of Facebook", *CSCW'08*, ACM Press, San Diego, pp. 721-730.

Lipford, H. (2010), *Improving Privacy on Social Network Sites*, University of North Carolina, Charlotte, available at: www.cs.vt.edu/files/files/Seminar/2010/Lipford-VTseminar.pdf (accessed 1 October 2014).

Lipford, H. and Besmer, A. (2010), "Moving beyond untagging: photo privacy in a tagged world", in Mynatt, E.D. (Ed.), *CHI*, pp. 1563-1572.

Madden, M. and Smith, A. (2010), *Reputation Management and Social Media*, Pew Internet & American Life Project, Washington, DC, available at: www.pewinternet.org/2010/05/26/reputation-management-and-social-media/ (accessed 1 July 2014).

Mason, R.O. (1986), "Four ethical issues of the information age", *MIS Quarterly*, Vol. 10 No. 1, pp. 5-12.

Nissenbaum, H. (2004), "Privacy as contextual integrity", *Washington Law Review*, Vol. 79 No. 1.

Nissenbaum, H. and Barocas, S. (2009), *On Notice: The Trouble with Notice and Consent*, New York University, New York, NY.

Palen, L. and Dourish, P. (2003), "Unpacking 'privacy' for a networked world", *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '03)*, *ACM, New York, NY*, pp. 129-136.

Parrish, J.L. (2010), "PAPA knows best: principles for the ethical sharing of information on social networking sites", *Ethics and Information Technology*, Vol. 12 No. 2, pp. 187-193.

Regan, P. (2003), "Safe harbours or free frontiers? Privacy and transborder data flows", *Journal of Social Issues*, Vol. 59 No. 2, pp. 263-282.

Rössler, B. (2005), *The Value of Privacy*, Polity Press, Cambridge, MA.

Weber, R.H. (2011), "The right to be forgotten: more than a Pandora's box", *Jipitec*, Vol. 2 No. 2, pp. 120-130.

Wester, M. and Sandin, P. (2011), "Privacy and the public – perception and acceptance of various applications of ICT", in Arias-Olivia, M., Ward Bynum, T., Rogerson, S. and Torres-Coronas, T. (Eds), *The "Backwards, Forwards and Sideways" Changes of ICT, 11th International Conference on the Social and Ethical Impacts of Information and Communication Technology (ETHICOMP)*, *Proceedings of the twelfth international conference, Ethicomp 2011, Sheffield University*, pp. 580-586.

Young, A.L., Gurzick, D. and Quan-Haase, A. (2011), "Online multi-contextual analysis: (re)connecting the social network site user with their profile", in Daniel, B.K. (Ed.), *Handbook of Research on Methods and Techniques for Studying Virtual Communities: Paradigms and Phenomena*, IGI Global, Hershey, PA, pp. 542-554.

Young, A.L. and Quan-Hasse, A. (2013), "Privacy protection strategies on Facebook", *Information, Communication and Society*, Vol. 16 No. 4, pp. 479-500.

Further reading

Citron, D. (2011), "Aligning privacy expectations with technical tools", Opiniones Concurrentes, available at: www.concurringopinions.com/archives/2011/04/aligning-privacy-expectations-with-technical-tools.html (accessed 25 July 2014).

Gross, R. and Acquisiti, A. (2005), "Information revelation and privacy in online social networks", *Proceedings of ACM Workshop on Privacy in the Electronic Society'05, ACM Press*, *New York, NY*, pp. 71-80.

Nissenbaum, H. (2010), *Privacy in Context*, Stanford University Press, Standford, CA.

Thompson, J. (1998), *Los media y la modernidad: Una teoría de los medios de comunicación*, Paidós, Barcelona.

About the author

Amaya Noain-Sánchez is a Journalist and Researcher at the Department Journalism III, Communication Sciences Faculty at Complutense University, Madrid. She has participated in some research into New Information and Communication Technologies at Goethe-Universität Frankfurt am Main in conjunction with Fraunhofer-Institut für Sichere Informationstechnologie SIT. Nowadays, she develops several research into the relation between privacy and web 2.0 applications. Amaya Noain-Sánchez can be contacted at: amayanoain@hotmail.com