From privacy by design to design for privacy

Guilda Rostama, Alborz Bekhradi, Bernard Yannou

FROM PRIVACY BY DESIGN TO DESIGN FOR PRIVACY

Guilda Rostama (a), Alexandre Bekhradi (b), and Bernard Yannou (b)

(a) Independent author
(b) Laboratoire Genie Industriel, CentraleSupélec, Université Paris-Saclay

ABSTRACT

Privacy by design places the user's privacy and the protection of his/her personal data as a basic principle in the early stages of the design and decision-making process. In 2018, Privacy by Design will become a mandatory provision for any entity across the world which collects and processes European residents' personal data. In other words, more than a methodology, Privacy by Design is soon to become a legal requirement, the infringement of which may be subject to fines up to 2% of a company's total worldwide annual turnover. However, we argue in this article that Privacy by design is not merely a legal requirement that solution designers and providers need to comply with, but that the lack of respect for users' privacy is increasingly becoming a pain for users, with the aid of the pain-driven Radical Innovation Design (RID) methodology. Thus, we will show that Privacy by design may increase the value creation of a solution and that integrating privacy as a default setting in the design of a solution is becoming an essential factor for success on the market. This paper is a proposal and first attempt to evolve from Privacy by Design to a Design for Privacy.

1 INTRODUCTION

"*Protecting privacy while meeting the regulatory requirements for data protection around the world is becoming an increasingly challenging task. Taking a comprehensive, properly implemented risk-based approach— where globally defined risks are anticipated and countermeasures are built into systems and operations, by design—can be far more effective, and more likely to respond to the broad range of requirements in multiple jurisdictions*" (Deloitte, 2016). These are the terms used by Dr. Ann Cavoukian to define the challenge that companies face today in respect of privacy and the processing of personal data on the one hand and the technological and business models' evolutions on the other. Furthermore, a recent study (Ponemon Institute LLC, 2016) found that the average consolidated total cost of a data breach grew from $3.5 million in 2014 to $4 million in 2016.

The term privacy may have several definitions. According to Solve (2008), "*Privacy is about respecting the desires of individuals where compatible with the aims of the larger community. Privacy is not just about what people expect but about what they desire. Privacy is not merely an individual right – it is an important component of any flourishing community"*. Other scholars such as Westin (1970) argue that privacy implies a certain degree of control over the information related to one self: "*Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others*". From these principles, policy makers derive regulations to enhance individuals' privacy through the protection of their personal data, defined as "*any information relating to an identified or identifiable natural person (...) who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*" (European Parliament and Council, 2016). In other words, personal data is given a broad definition in the sense that any data which allows the identification of an individual is considered as personal data and falls therefore within the scope of privacy regulations. European regulators (European Union, 2012) even make the protection of individuals in relation to the processing of personal data a fundamental right, emphasizing that "*everyone has the right to the protection of personal data concerning him or her*".

Nevertheless, the realities of the market and the evolution of new technologies are quite different. An increasing number of business models are being built on the monetization of personal data, and private communications are treated as the basis for commercial offer via targeted advertisement. For instance, the business model of many Internet companies such as Google or Facebook is based on providing "free" services to the Internet user, that are mostly if not exclusively financed by advertising. These advertisements are built on the analysis of users' data, for example according to the content of their

emails or their navigational data, or on the observation of the user's behavior over time. Therefore, tensions arise between these business models and the need to protect the privacy of users. A recent report (European Commission, 2016) best illustrates these tensions, revealing that 90,3% of citizens and civil society organizations see an added-value in having rules to ensure the right to privacy and confidentiality, whereas 63,4% of the industry consider that EU rules are not necessary to ensure the protection of privacy and confidentiality.

In this context of inherent tensions, the concept of "Privacy by design" has been developed as an attempt to bridge the gap between the path taken by the market on the one hand and policy makers' requirements on the other. Privacy by Design, which originated in 1995 from a joint paper on Privacy Enhancing Technologies by Dutch and Canadian regulators (Information and Privacy Commissionner Ontario & Registratiekamer (Netherlands), 1995) and coined by Ann Cavoukian (Cavoukian, 2011), is a method for designing a solution that places the privacy of the user as a basic principle for any technological innovation. This procedure is divided into seven fundamental principles, which include transparency and the user's control of its data. These principles are directly integrated into the solution and become one of its essential components.

Policy makers develop a particular interest on Privacy by design. As early as 2010, the European Commission (European Commission, 2010) stated that Privacy by Design "*means that privacy and data protection are embedded throughout the entire life cycle of technologies, from the early design stage to their deployment, use and ultimate disposal*". More interestingly, the 2016 General Data Protection Regulation (GDPR) which will enter into force in 2018 makes Privacy by Design a mandatory provision for companies (European Parliament and Council, 2016), providing in its article 25 that "*Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing (...), the controller*[1] *shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures (...) to protect the rights of data subjects. The controller shall implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons*". In other words, companies and designers will be required to anticipate the issue of the protection of personal data in the early stages of the design and decision-making process, and will need to prove that their solutions protect by default the users' privacy. Privacy by Design will no longer be a mere methodology but a legal requirement for any entity wishing to collect and process European residents' personal data.

However, Privacy by design is difficult to translate into the engineering practice. The European policy makers remain vague on these new obligations for designers, by providing mere few examples in the Recital 78 of the GDPR (European Parliament and Council, 2016): "*Such measures could consist, inter alia, of minimizing the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features*". One of the main issues therefore is the strong lack of guidance on Privacy by design in the design process, as policy makers do not provide clear guidelines to solution designers as to what this concept clearly entails.

In this context, the objectives of this paper are twofold: first, we will present the results of a survey aiming at identifying the degree of importance that users give to privacy. Subsequently, we build on the findings of the survey to show that privacy by design may increase the value creation of a solution with the aid of the pain-driven Radical Innovation Design (RID) methodology (Yannou et al, 2016). We argue here that privacy by design is not another legal requirement that solution designers and providers need to comply with, but that the lack of respect for users' privacy is increasingly becoming a pain for them. In other words, we argue that integrating privacy as a default setting in the design of a solution is becoming an essential factor for success on the market. Building on this hypothesis, we provide in the second part of this article some guidance as to what privacy by design entails on an engineering

[1] A "data controller" is generally understood as the organization which determines the purposes and means of processing of personal data and who holds the responsibility for it.

perspective, with the examples of Uber, Facebook and WhatsApp. Our finding is that privacy by design may technically translate into providing the user with control, along with transparence, and data minimization. Privacy by Design developed by regulators may soon lead to a Design for Privacy, another useful Design for X approach to consider from now on, in a world where user data are being so abundant.

2 IDENTIFICATION OF THE IMPORTANCE OF PRIVACY FOR USERS THROUGH A SURVEY

In order to better grasp the importance that users give to privacy while using online services or connected objects, a quantitative online survey was conducted. The questions were drafted according to policy makers' observations, as well as on the basis of the issues that are generally raised in case-law and inusers' testimonies on various websites and blogs. The survey was shared on social networks and sent via email to the authors' contact lists.107 respondents between the ages of 23 to 70 years were asked to answer the following questions:

1. In general, how important is it to you that an online service (social networks, e-commerce, mobile applications, etc.) and/or connected object protect your privacy?
2. Would the fact that an online service or a connected object protects by default your privacy prompt you to choose this connected object /online service rather than another one of same quality?
3. Does the degree of control you exercise over your data prompt you to choose a connected object and/or an online service rather than another one of same quality?
4. Would you stop using an online service and / or connected object, if you find out that your privacy is violated (e.g. your data is sold to third parties for advertising purposes), even if there was no alternative available?
5. Do you think that current online services and/or connected objects give you enough flexibility to customize the use that is being made of your personal data?
6. If a connected object or a mobile application requires permissions that have nothing to do with the service it provides (e.g. the calendar that requests access to your camera), would you give up the use of this application?
7. Do you think you are sufficiently informed of the risks of violation of your privacy (such as theft of your data, resale to third parties, security breaches, etc.) when you use an online service and/or a connected object?

2.1 RESULTS

91% of the respondents answered that the protection of their privacy is important or very important to them while using an online service and/or connected object, whereas only 3% state that they never think about it (Figure 1).

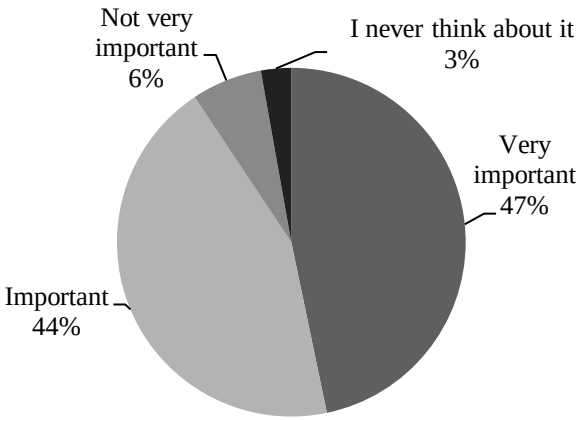

Figure 1 Answer to the question: "In general, how important is it to you that an online service (social networks, e-commerce, mobile application, etc.) and/or connected object protects your privacy"

In addition, 82% of the respondents consider that they are not given enough flexibility to customize the use that is being made of their personal data, and an overwhelming majority of 89% answered that they are not sufficiently informed of the risks of violation of their privacy while they use an online service and/or connected object. This finding demonstrates that privacy has become a true concern for users.
In fact, privacy has become so important that 66% of the respondents answered that they would stop using an online service and/or connected object if they found out that their privacy had been violated, even if there was no alternative available. Users are therefore clearly ready to stop using a product or service if their privacy is not sufficiently respected. For instance, 64% of the respondents declared that they would give up the use of a connected object or mobile application if the latter requires permissions that have nothing to do with the service it provides (the example was given of a calendar application requiring access to one's phone camera).
For what concerns the users' decision to choose a specific product and/or service, 85% of the respondents have answered that they would choose an online service and/or connected object rather than another one of the same quality if they have a sufficient degree of control on their data, as shown in Figure 2. More interestingly, the fact that an online service or connected object protects by default their privacy would prompt 86% of the respondents to choose this connected object/online service rather than another one of the same quality (see Figure 3).

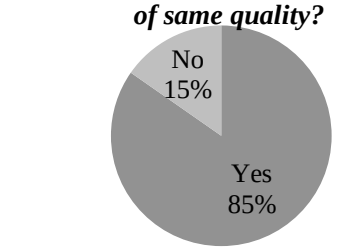

Figure 2 Importance of the degree of control of personal data for users

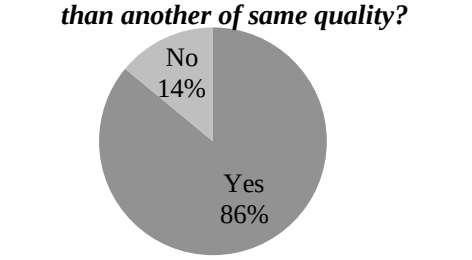

Figure 3 Importance of the protection of privacy by default for users

In other words, it appears that the protection of privacy as become a true concern for users of connected objects and/or online services, and that integrating Privacy by design in the heart of a solution may prompt users to choose this solution rather than another one, and may therefore become a factor of success on the market.

2.2 THE LACK OF PRIVACY IS A PAINFUL SITUATION FOR USERS

This survey clearly highlights that privacy is increasingly becoming a concern for users which is not sufficiently addressed by solution designers or providers. A clear example of this concern is the hacking of the website Ashley Madison, an online service specialized in extramarital relationships. In August 2015, a group calling itself "The Impact Team" released some 30 gigabytes of files containing millions of names, user accounts, e-mails and addresses as well as Ashley Madison's browsing history with even the sexual preferences of some users. This breach of the users' privacy was so painful to some of them that it caused many suicides from users in Canada and the United States (Segall, 2015). Canadian and Australian investigations noted that the security of the site at the time of the attack was "inadequate" or even "absent". Beyond the lack of security of the users' data, it is interesting to note that even though users had deactivated their accounts, Ashley Madison had taken the liberty to retain information associated with the account for 12 months or sometimes indefinitely, which clearly went against users' will to delete their accounts.
In this case, integrating Privacy by design in the core of Ashley Madison's database would have implied that the data would be automatically deleted once the user deactivated the account, or that the database kept track of how long the information had been stored, and deleted it when a fixed period of time had

expired. Many users' pains would have been alleviated and many suicides would have been avoided. Privacy by Design may thus provide an efficient approach to address users' pains.
To achieve this objective, solution designers and providers may adopt various innovation strategies, among which a Need Seeker strategy (focused on understanding and learning as much as possible about the users' expectations, Market Reader strategy (based on the monitoring of the markets, customers and competitors), and Technology Driver strategy (emphasizing on internal technological capabilities to develop new products and services). Among these three strategies, a study (Jaruzelski, et al., 2012) has revealed in 2012 that "*following a Need Seekers strategy, although difficult, offers the greatest potential for superior performance in the long term*".
User-experience and need seeker designs are thus growing in importance, and Privacy by Design fits perfectly in these approaches. Indeed, as argued by Ira Rubinstein and Nathan Good (Rubinstein & Good, 2012), Privacy by design may be understood as an extension of existing user-centered design, "*insofar as it seeks to anticipate and address potential privacy problems that customers may have in using any product*". Privacy by design will help ensure that the expectations of the users regarding their privacy are taken into consideration early in the design process.
A literature review on design and innovation methodologies and tools has shown that few methods focus on how to systematically identify and evaluate pain points of users. One of the main pain-oriented and need seeker methodology is the Radical Innovation Design (RID) methodology (Yannou, et al., 2016), which adopts a pain-driven structured process where problems are identified and prioritized in different usage situations. The objective of the RID methodology is to maximize the potential value creation inside a field of user activities called ideal goal, which defines the initial design boundaries. Furthermore, the RID methodology proposes a set of innovative indicators, UNPC, which help expert designers or innovation jury members at different stages of the ideation and innovation process to assess an innovation (Yannou, et al., 2015). The UNPC indicators are the following: Proofs of Usefulness (U), Proofs of Newness (N), Proofs of Profitability (P) and Proofs of Concept (C). While the proofs of Newness, Profitability and Concept are important but conventional to assess an innovation, designing for increasing Usefulness as much as possible has been defined as a design principle in (Bekhradi, et al., 2015), which allows addressing large user pain areas and consequently leads to user-centered disruptive innovative solutions. Indeed, Usefulness is defined as the "*coverage of usage and needs situations of users / stakeholders for which important needs are covered, and where the suffering is alleviated and / or malfunctions of existing systems are improved*" (Yannou, et al., 2015). In RID's perspective, a robust innovation is considered as the most useful or pain killer one. The first phase of the RID methodology consists in identifying a relevant problem following systematic investigations of users' pains, usage scenarios and existing solutions. A technical, legal and user's observation is thus needed to capture value buckets (i.e. frequent unalleviated pains by the existing solutions on the market). In other words, a value bucket is equivalent to the distance between the existing solutions and the ideal or utopic situations without any pain. This distance (calculated in the form of a delta-Usefulness in the context of RID) characterizes the potential of value to be created by a radically innovative solution.
We argue that Privacy by Design may increase the Usefulness of the solution to reach an ideal situation where there are less pains with fully respected privacy. Our survey has demonstrated that there is a true "Data privacy pain", whether this pain results from a lack of security in the collection and retention of data or from the deliberate use by companies of users' personal data which is incompatible with the respect of their privacy. Privacy by design may therefore increase the Usefulness creation of a solution, as privacy is a pain that needs to be alleviated.
However, defining Privacy by design as a potential increase of a solution's usefulness is not sufficient. It also needs to be translated in engineering terms so that designers may better grasp what it actually entails in the design process.

3 HOW TO TRANSLATE PRIVACY BY DESIGN IN DESIGN ENGINEERING

3.1 THE EXAMPLE OF THE NEWLY-ADOPTED EUROPEAN GDPR

We take the example of the GDPR for many reasons. First, at the time of writing of this article, the GDPR is the most recent major regulation adopted at an international level and exclusively focusing on the privacy and the rules pertaining to the collection and processing of users' personal data. Although the European approach is known to be more restrictive than other legislations adopted across the world,

in particular by the United States, it may still serve as an indicator on the general tendency of policy makers regarding privacy and regulations on personal data.
Second of all, the territorial scope of the GDPR is particularly broad. Indeed, according to its article 3, the GDPR will apply not only to companies established in the European Union (EU) but also to companies established across the world, which collect and process data on individuals residing in the EU. If for instance a Chinese company offers products and/or services to European residents, and by doing so collects data on them, or studies their behavior, all the GDPR requirements will be applicable to the Chinese company as well. In other words, as soon as data is collected on European residents, the GDPR will be applicable, including the Privacy by Design requirement.
Third of all, the GDPR is interesting to study as it establishes for the first time strong sanctions for companies which do not comply with its provisions. For instance, infringements of the provisions regarding the Privacy by design requirement may be subject to administrative fines up to 2% of the total worldwide annual turnover of the preceding financial year. Not complying with the necessity of obtaining the users' consent before the collection and processing of its personal data may be fined up to 4% of the total worldwide annual turnover of the preceding financial year. Needless to say that in the case of global data-driven companies, the fine may be quite high.
Furthermore, the GDPR formalizes the companies' accountability regarding privacy and users' personal data. In other words, the GDPR places the burden of proof on companies so that they are able to demonstrate that the processing of personal data is performed in accordance with the Regulations (article 24). According to European data protection authorities (Article 29 Data Protection Working Party, 2010), "*One way to induce data controllers to put in place such measures would be by adding an accountability principle (...). The expected effects of such a provision would include the implementation of internal measures and procedures putting into effect existing data protection principles, ensuring their effectiveness and the obligation to prove this should data protection authorities request it* ". In other words, companies are expected to be able to constantly prove that they are complying with the GDPR's provisions.
Last but not least, the GDPR makes Privacy by Design for the first time compulsory, and states in article 25 that the company "*shall implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons*". All of these principles refer to data minimization (only personal data which are necessary for each specific purpose of the processing are processed), purpose limitation (the amount of personal data collected, the extent of their processing, the period of storage), and to transparency (the personal data are not made accessible without the individual's intervention, which means that the user needs to be aware of the implications of sharing their personal data).
Therefore, it appears that the enforcement GDPR will in the near future create a substantial value creation potential in the sense of RID value buckets. In other words, the GDPR provisions can be considered as an opportunity to design more disruptive innovations. Some provisions of the GDPR, in particular article 5, provide further explanations on the requirements applicable to personal data and to users' privacy. These principles include Data security, integrity and confidentiality, lawfulness, fairness and transparency, data minimization, data accuracy, and purpose and data retention limitation. We will now explore some of these principles and intend to translate them into the design of a product and/or service.

3.2 PRIVACY BY DESIGN PRINCIPLES: CASE-STUDIES OF UBER, AND FACEBOOK/WHATSAPP DATA SHARING CONTROVERSY

Providing detailed explanations on each one of these principles would be excessively lengthy in the context of this article. Therefore, we further focus on transparency, data minimization and purpose limitation, using the examples of Uber and the WhatsApp/Facebook data sharing controversy.

3.2.1 The purpose limitation and data minimization principles

According to the European Data Protection Supervisor (European Data Protection Supervisor, 2016), "*the principle of "data minimization" means that a company "should limit the collection of personal information to what is directly relevant and necessary to accomplish a specified purpose. They should*

also retain the data only for as long as is necessary to fulfill that purpose. In other words, data controllers should collect only the personal data they really need, and should keep it only for as long as they need it".

In other words, the data must be limited to what is necessary in view of the purposes for which it is processed. Thus, deadlines must be fixed for an automatic erasure or for a regular re-examination of the necessity of the data. Some authors (Gürses, et al., 2011) argue that "*for a given functionality, the data that is absolutely necessary to fulfill the functionality needs to be analyzed. This activity includes a survey of state-of-the-art research to explore which data can be further minimized, as well as an evaluation of alternative architectures, e.g., distributed, centralized, that could contribute to data minimization*". It is therefore necessary that solution designers and providers reflect at the outset on (i) which data is necessary to collect for the purpose of the product or service, (ii) whether the purpose of the processing can be reasonably achieved by other means and (iii) how to limit the amount of data collected to the absolute minimum. To achieve this goal, the functionality of the solution needs to be clearly described. As Gürses et al. point it, "*Vague or implausible descriptions have a high risk of forcing engineers into a design that would collect more data, as massive data collection is needed in order to guarantee that any more specific realization of the system can be accommodated by the design*".

Furthermore, the data should only be processed if the purpose of the processing cannot reasonably be achieved by other means. A recent development in Uber Privacy policy may help illustrating the principle of purpose limitation and data minimization. The latest version of Uber privacy policy now states that Uber will continue tracking passenger even when they are dropped off (Uber Privacy Statement, 2015): "*When you use the Services for transportation or delivery, we collect precise location data about the trip from the Uber app used by the Driver. If you permit the Uber app to access location services through the permission system used by your mobile operating system ("platform"), we may also collect the precise location of your device when the app is running in the foreground or background. We may also derive your approximate location from your IP address*". In other words, even if the user is no longer using the Uber application, the user will continue to be constantly located by the application. According to an Uber spokesperson (Titcomb, 2016), the purpose of this constant geolocalization is to "*improve the rider experience (...) and to identify the best pick up location on a given street. Location is at the heart of the Uber experience, and we're asking riders to provide us with more information to achieve these goals*".

The results of our survey have highlighted that users gave a lot of importance to the permissions required by mobile applications: 64% of them have stated that if an excessive amount of data is required comparing to the purpose achieved by the product or service, users would stop using it. Users have already started complaining about this constant data localization, some of them stating on Twitter that "*I will not use an app that requires to share my location at all times. After 6 years I am switching from Uber to Lyft*" (Titcomb, 2016). In this case, Uber did not respect the data minimization and purpose limitation principles, which is leading users to stop using the application. The proper application of the Privacy by Design methodology should have led the designer of the application to reduce the data collected to the absolute minimum and to "improve the rider experience" by other means. For instance, drivers could enter the best pickup location in the application according to their previous experiences or their analysis of the environment, and the application would then notify to the user the driver's recommendation for the best pickup location within a range of 100 meters for example. The constant tracking of the users' locations would therefore not be required, and the users' pains would not drive them away from Uber application.

3.2.2 The transparency principle

This principle of transparency refers to the fact that all information and communication relating to the processing of data must be given in a manner that is easily accessible, easy to understand and formulated in clear and simple terms for the users. This would imply that the information should not be lost in the middle of an impenetrable and incomprehensible privacy policy published somewhere in a website or in the terms of use of a connected object. This information should be given upon the first use of the online service and/or connected object, by using simple words, or drawings. According to the GDPR, this information should include, among others:

1. the identity and the contact details of the company collecting and processing the data;
2. the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

3. the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
4. the existence of the right to request to access, rectify or erase of personal data;

Furthermore, users need to be informed about changes in the privacy policy and be provided with explanations as to why certain permissions to their data are necessary. This is particularly true in situations where the multiplication of actors and the complexity of the technologies used make it difficult for users to know and understand whether personal data are collected by whom and for what purpose, as it is the case in online advertising. This information should remain available during the entire period of use of the product or service. The application of the transparency principle would contribute to the users' feeling of control and thus alleviate the pains of 85% of the respondents of our survey. As (Lederer, et al., 2004) argue, "*Designs should not require excessive configuration to manage privacy. They should enable users to practice privacy as a natural consequence of their normal engagement with the system*".

In other words, providing accurate, clear and complete information is more than a legal requirement. It may be a selling argument and a factor of success on the market, as it responds to the needs of users for more transparency while using online services and/or connected objects. The importance of the transparency principle may be best illustrated by the WhatsApp/Facebook recent controversy. In August 2016, WhatsApp users were informed that phone numbers, profile names, photos, online status and other activities would be shared with its parent company, Facebook, to test new features that would help them interact with businesses. This raised serious concerns across Europe. For instance, UK Information Commissioner Elizabeth Denham (Lomas, 2016) stated that: "*There's a lot of anger out there. And again it goes back to promises, commitment, fairness and transparency*". Europe's privacy regulators have urged WhatsApp to stop sharing user data with Facebook while it investigates its privacy practices. The Article 29 Working Party, composed of the heads of European data protection authorities, stated that they had "serious concerns" about changes to WhatsApp's terms of service. The European Commission (European Commission, 2016) even went to the extent of stating that Facebook intentionally, or negligently, submitted incorrect or misleading information to the Commission into its acquisition of WhatsApp, insofar as the technical possibility of automatically matching Facebook users' IDs with WhatsApp users' IDs already existed in 2014, and that this fact had not been revealed to the European Commission during the merger review. US privacy group Electronic Privacy Information Center (EPIC) filed a complaint against Facebook, and German regulators as well as Delhi High Court in India ordered WhatsApp to halt the practice. As for users (Tynan, 2016), some observers and users' representatives have noted that "*The sentiment that WhatsApp is an app that protects and cares for your privacy is no longer a reality. It was nice while it lasted.*" Other users voiced their disappointment: "*WhatsApp just lost a user. Was just a matter of time once the FB acquisition went through. Guess it's time to finally give Telegram a whirl.*" This example helps illustrating a case where a company's preference for the increase of revenues over privacy has seriously damaged its image, and has predictably increased the pains of users instead of reducing them, which is now driving them away from the service.

4 CONCLUSION

The main objective of this article was to bridge the gap between policy makers and designers on the question of privacy by design. First, we carried out a survey which has allowed us to showcase that the issue of privacy has become a true concern for users and that the lack of transparency and control is a pain which needs to be addressed by designers. Respondents to our survey stated, in an overwhelming majority, that they would prefer using a solution which protects their privacy by default and that they feel they are not given sufficient information and control over their personal data. Inspired by the pain-driven RID innovation methodology, we have shown that integrating Privacy by design in the creation of a solution may increase its Usefulness and therefore be a source of disruptive innovations and consequently a factor of success on the market. We have subsequently attempted to translate Privacy by design into concrete actions that designers may take in the design process of their solutions. We have seen for instance that implementing the purpose limitation and data minimization principles may help designers to identify at the outset the data that is necessary to collect for the purpose of the product or service and to limit the amount of data collected to the absolute minimum. By taking the example of Uber, we saw that collecting an excessive number of users' data comparing to the purpose of the solution

may easily drive users away from the solution and lead to the deterioration of the image of the company. Another concrete way of implementing Privacy by Design is to be as transparent as possible with the users of the solution, by providing them with clear and easy-to-understand explanations on the data that is collected and the reasons why the collection of this data is necessary. Providing a sense of control to the users is also essential, and we have seen through the Facebook/WhatsApp data sharing controversy that users would not hesitate to stop using an application or an online service if they feel that companies do not respect their privacy enough.

However, the road is still long. Now that Privacy by Design will become a legal obligation for companies across the world intending to collect data on European residents, and that the infringement of this obligation may lead to a fine of up to 2% of the company's global revenue, it has become all the more important to enhance and maintain a dialogue between policy makers and designers. Policy makers and National data protection authorities regularly launch public consultations in order to collect the advice and points of views of professionals, and to gather examples of best practices which may then turn into law or guidelines. Although it is not a legal obligation, we strongly recommend that designers across the world participate in these consultations which truly allow policy makers to clarify the position of the stakeholders and to render the privacy regulations fully operational. Furthermore, policy makers provide tools to designers and companies in order to ensure that they comply with privacy by design requirements. For instance, article 25 of the GDPR states that an approved certification mechanism may help companies, on a voluntary basis, to prove that they comply with the requirements of Privacy by Design. These mechanisms include seals, marks, or codes of conduct approved by national data protection authorities. We strongly recommend that designers and companies wishing to collect and process personal data voluntarily seek these certifications, which not only will ensure that they comply with legal requirements, but would also reassure users that their privacy is respected and increase their confidence in the solution. This paper is a proposal and first attempt to evolve from a Privacy by Design to a Design for Privacy. More sophisticated design guidelines are currently being designed and tested.

REFERENCES

Article 29 Data Protection Working Party, 2010. *Opinion 3/2010 on the principle of accountability*. s.l.:s.n.

Bekhradi, A., Yannou, B., Farel, R. & Zimmer, B., 2015. Usefulness Simulation of Design Concepts. 137(7), pp. 071414-071414-12.

Cavoukian, A., 2011. *Privacy by Design, The 7 Foundational Principles*, s.l.: Information and Privacy Commission of Ontario.

Deloitte, 2016. *Privacy by Design - Setting a new standard for privacy certification.* [Online] [Accessed 2016].

European Commission, 2010. *Communication from the Commission of the European Parliament - A Digital Agenda for Europe*, s.l.: s.n.

European Commission, 2016. *Mergers: Commission alleges Facebook provided misleading information about WhatsApp takeover,* s.l.: s.n.

European Commission, 2016. *Synonpsis Report of the Public Consultation on the Evaluation and Review of the Eprivacy Directive.* s.l.:s.n.

European Data Protection Supervisor, 2016. [Online] Available at: https://secure.edps.europa.eu/EDPSWEB/edps/lang/en/EDPS/Dataprotection/Glossary/pid/74/cache/offonce

European Parliament and Council, 2016. *Regulation (EU) 2016/679 (General Data Protection Regulation)*. s.l.:Official Journal of the European Union.

European Union, 2012. *Consolidated version of the Treaty on the Functioning of the European Union.* s.l.:Official Journal C326.

Gürses, S., Troncoso, C. & Diaz, C., 2011. Engineering Privacy by Design. *K.U. Leuven.*

Information and Privacy Commissionner Ontario & Registratiekamer (Netherlands), 1995. *Privacy-enhancing Technologies: The Path to Anonymity*, s.l.: s.n.

Jaruzelski, B., Loehr, J. & Holman, R., 2012. *The Global Innovation 1000: Making Ideas work,* s.l.: Booz & Company Inc. .

Lederer, S., Hong, J., Dey, A. & Landay, J., 2004. Personal Privacy through Understanding and Action: Five Pitfalls for Designers. *Carnegie Mellon Universty.*

Lomas, N., 2016. WhatsApp's privacy U-turn on sharing data with Facebook draws more heat in Europe. *Techcrunch*.
Ponemon Institute LLC, 2016. *2016 Cost of Data Breach Study: Global Analysis*, s.l.: IBM.
Rubinstein, I. & Good, N., 2012. Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents. *Berkley Technology Law Journal*, Volume 1333.
Segall, L., 2015. Pastor outed on Ashley Madison commits suicide. *CNN*.
Solve, D. J., 2008. *Understanding Privacy*. s.l.:Harvard University Press.
Titcomb, J., 2016. Uber is tracking your location even when rides are finished. *The Telegraph*.
Tynan, D., 2016. WhatsApp privacy backlash: Facebook angers users by harvesting their data. *The Guardian*, 25 August.
Uber Privacy Statement, 2015. *Information We Collect Through Your Use of Our Services*. s.l.:s.n.
Westin, A., 1970. *Privacy and Freedom*. s.l.:The Bodley Head Ltd.
Yannou, B., Cluzel, F., Bekhradi, A. & Zimmer, B., 2015. Innovative idea and project selection and maturation with the UNPC innovativeness model in the context of innovating in healthcare. *International Journal of Design Creativity and Innovation*.
Yannou, B., Cluzel, F. & Farel, R., 2016. Capturing the relevant problems leading to pain and usage drive innovations: the DSM Value Bucket algorithm. *Concurrent Engineering - Research and Applications (CERA)*.