ADCAIJ: Advances in Distributed Computing and Articial Intelligence Journal
Regular Issue, Vol. 6 N. 1 (2017), 51-58
eISSN: 2255-2863
DOI: http://dx.doi.org/10.14201/ADCAIJ2017615158

Between the Profiles Pay Per View and the Protection of Personal Data: the Product is You

Ana Karin Chávez Valdivia[a]

[a]Professor Law department, and Director of Social projection department, La Salle University, Arequipa-Perú. achavez@ulasalle.edu.pe

KEYWORD

Personal data; sensitive information; data broker; data minning; Internet.

ABSTRACT

Perhaps in the past was difficult to imagine that the moment in which someone could register each purchase that has been made, each book that has been read or each thing that has been said would come. That there would be companies storing data about our physical activity, behaviors, preferences and choices all the time. Most of the personal data comes from acts as daily as installing an application, completing a form, purchasing a product or requesting a service. This information provided sometimes consciously, voluntarily and with relative knowledge of the destination that will have, contrasts with situations in which data are inferred, deduced, extracted and manipulated. In this sense, within a context in which the only access to the database has been left behind to give way to the creation of these by third parties, we wonder about the possible denaturation of the personal data and sensitive information that when get transformed in raw material through the analysis of existent connections and extraction of new data implicit in the multitude of information compiled in public or private databases, would convert people into an essential product for the market; while the development of citizen profiles pay per view would allow predicting behaviors, selections and multiple deployments in different aspects of our lives. It is probable that in the defenselessness condition where we are now for having passed from personal space to social one and from there to the market many times without our knowledge and consent makes necessary to reconsider the current forms of protection and mechanisms of legal protection around our personal data.

1. Introduction

The data collection and storage industry coupled with technological development have resulted in our data being collected not only by public and private institutions but by several companies operating in cyberspace because of the various web 2.0 services by their nature depend on the participation of the users to produce contents and different kind of information as well as the constant updating of the services or products offered depends on the permanent analysis of their behavior records. In this context «third parties» appear to collect data that the first ones collected to make profiles with ultra precise personal details.

Even though the data have always existed, before technologies advances data were stored in storage medium that limited their storage capacity, conservation and treatment, as well as systematic and automated analysis in massive quantities. Actually many companies collect and refine huge amounts of data and these databases are growing at an unprecedented rate because of the collection and management of information from them is their reason of being and data analysis is an endless source of possibilities for researching and negotiation.

The advertising market was undoubtedly the main engine and promoter of data mining since degenerated itself with the obsessive searching of the perfect consumer handling big amount of information collected by themselves and given by the users on behalf of doing market research. This information was not totally relevant for the purposes of a commercial investigation and was scattered and disorganized this situation contributed in a way to the appearance of the data broker figure.

This new reality forces us to do a deep reflection about the effectiveness of current protection of personal data legislations in an environment where institutions and companies no longer have a legitimate interest in our data and have an interest in accordance with the needs and requirements of the «client».

Although in Peru both the law of personal data protection, Law No. 29733, and its regulation the Supreme Decree No. 003-2013-JUS, pretend to protect our fundamental right to the protection of personal data within the framework of respect to other fundamental rights, our reality seems to place us in a condition of total helplessness.

2. Commercial use of our data and Rigth to the privacy: Data Brokers

It has happened to all of us that after having search for a flight in despegar.com, the next day we get an email with the subject «off%». We may receive a call by offering us a credit card as a product of a previous search we have made in different banks. If we search in an online store for a particular product we get an email with all the offers linked to our search or simply this information will appear linked to our facebook account, not to mention that we have generated an activity that in most cases will follow us along all the websites that we visit later.

The objective of personalized marketing is precisely to personalize each message to each user, but to be able to achieve this it is necessary to compile and analyze information since the more they know about us they will sell more; consequently, it is essential for them to know us. Some typical activities such as buying a car or a house involve that a certain kind of information will be collected by public administration institutions and financial organizations.

When we provide data to obtain a credit card, various companies will have access to this information and the whole purchases that have been made in the department store will be register. If we register in a web site our data will remain in it and additionally the applications keep information about our contacts, calendar, coordinates, etc. Daily our activities on line and off line compromise information that reveals personal data about us; but we are not aware of this information is shared or sold to data brokers. So we can access profiles of people whom we will probably never know; however we could know many things about them and each member of their families; moreover, it is easily possible to infer future behaviors, activities and choices by analyzing the connections between their data and the extraction of new ones; at the same time obtaining conclusions on various aspects of their health which would make them a perfect target to receive information of products pharmaceutical -without considering other sensitive information might be collected in the process- in addition that the insurance companies will find in «them» ideal candidates due to the profile that they present. The same thing will happen with travel agencies, banks – that previously know who are classified as subjects of credit risk- and all kinds of commercial companies in the market.

That is to say, we are faced with what we might call an a la carte profile, that is, a personal profile prepared with not only the collection of data from public and private sources or online or offline sources - since we all know that in one way or another our data are already registered in different bases- but we are facing a profile created on personal data that acquire the quality of raw material on which third parties apply different procedures to analyze, infer and predict our action, future needs or decisions and with these profiles, create and recreate bases of data that allow us to be labeled ourselves within the parameters required by public or private organizations. In this way we become the product that may be needed or forbidden by third parties.

The logical question is obvious: who does this profile?. The answer is obvius, a database does it. Although this provokes an innumerable serie of questions, we focus on those that are the subject of our study. First: Is it legal to draw up a profile pay per view? And secondly what extent does this activity put us in a state of helplessness or abandonment of our fundamental rights? We think that large doses of transparency and strong guarantees of privacy are likely to be needed, especially if we consider that the activities of data brokers neither are regulated in all countries nor are prohibited.

In the economy today mass data is a big business and data brokers – companies that collect personal information from the consumer and resell it or share it with others – play a special role.

3. Between legality, privacy and reality

For decades, American lawmakers have expressed concern about the lack of transparency of companies that buy and sell information without direct consumer interaction. Certainly the lack of transparency between the companies that provide information about the consumer for credits and other eligibility decisions led to the adoption of the Fair Credit Reporting Act that the Federal Trade Commission imposed since its enactment in 1970. This law regulates the provision of information through consumer reporting agencies where it is used or expected to be used for decisions about credit, employment, insurance, housing, and similar eligible decisions. However, it generally does not regulate the sale of consumer information for marketing and other purposes. The trade commission monitored compliance with the law and since the late 1990s has also been careful to examine the practices of data brokers falling outside its scope.

In a 2012 report called «protecting consumer privacy in an era of rapid change» (Federal Trade Comission, 2012) the commission specifically addressed the issue of data brokers, identifying and describing three different categories:

- The entities subject to the law on fair credit reporting.
- Entities that maintain data for marketing purposes.
- Entities that maintain data for non-marketing purposes such as fraud detection, location of persons or others and are not regulated by law.

The commission noted that while the law addresses a critical number on transparency issues associated with companies that sell information for credit, employment and insurance purposes, the data brokers Which are within the other two categories remain hidden. For this reason, recommended in its report the need to have legislation on this subject to improve the transparency of industry practices, noting that although there was a little progress in this field, little was known about practices of the data brokers, specifying that a thorough examination was necessary. It is thus initiated a study on the practices in mention was initiated with the purpose to look for information referring to the following points:

- The collection of data including nature and sources of the consumer data that they collect.
- Practices of use as regards the maintenance and dissemination of data, as well as the tools given to consumers to control these practices: access, modification and possibility to unsubscribe to the option of having their personal information sold or shared.

Product of the study in mention, in May of 2014 the report of the federal trade commission of the United States identified these practices in nine companies: Acxiom, Corelogic, Datalogix, eBureau, ID Analytics, Intelius, Peek You, Rapleaf, Recorded Future, which represent a representative sample of the American industry (Federal Trade Comission, 2014). It was demonstrated, based on the requirements of the Commission, including the information obtained through subsequent publicly available questions, meetings and sources that, in general:

- Data brokers collect consumer information from a wide variety of commercial, government and other public sources, and combine online and offline data to advertise to consumers online.

- These data are collected mostly without the knowledge of the consumer.
- The industry of data brokers is complex, with multiple layers of data brokers providing data between them.
- Data brokers collect information and store billions of data items covering practically every American consumer.
- In the development of their products, data brokers not only use raw data obtained from numerous sources, such as the name of the person, address, property ownership status or age; which are prepared for a variety of purposes. But also use certain data to create derived information that they infer from consumers through the combination and analysis of data they handle, including potentially sensitive inferences. For example, a data broker might infer that a person with a boat license has an interest in browsing, that a consumer has an interest in the technology based on the subscription purchase of a «wired» magazine, or that a consumer who has purchased Two Ford cars are loyal to that brand.
- Data brokers use this current and derived data to create three main classes of products for customers in a wide variety of industries: marketing products, risk reduction products and products that people are looking for.

It should be in mind that because of these companies generally never interact with consumers, consumers are often unaware of their existence, much less the variety of practices in which their personal data are used. The report based on the collection of information and the use of practices of these nine data brokers helped for the first time to give light on this industry that obviously violates a wide range of fundamental rights while creating imminent risks according to each profile.

However, despite the aforementioned findings, the defense that these companies put forward was that the fact of creating consumer profiles and then selling them does not pose any privacy problems, as it does not affect the life of users. Moreover, they maintained that their lists do not influence so that they can veto them obtaining credit or subsidies. Even added that these profiles benefit consumers because thanks to them the advertising they receive will be only of things that interest them, that covers their needs or at least their preferences (travel, mobile, cosmetics, news, among others). In addition, they pointed out that the companies sign a clause with the companies that supply them with data to ensure that the user was informed that they were going to be sold to third parties. As evidenced by these practices not only denature our personal and sensitive data by turning them into raw material used to create derivative information whose final product would be a «personal profile» but also when being the subject of unknown and evidently unauthorized treatments puts us in a state Of total helplessness not only within the market but also to any third party for non-commercial purposes. In this context, technological development places us before two realities in terms of personal data. On the one hand the protection foreseen in the legislation that makes in certain situations the treatment of data can be socially positive, valuable and lawful. On the other hand; however we face a reality outside of all legal protection in which we do not know in which hands are our personal data or worse yet our sensitive data.

In view of the reality the Commission has mentioned some legislative recommendations to Congress to consider including four requirements in any legislation according to relevance, such as:

- The congress should look for ways to allow consumers to identify which data brokers may have information about them and where they should access such information and exercise the rights to unsubscribe. Legislation may require the creation of a centralized mechanism, such as an internet portal, where data brokers can identify themselves, describe their collected information, use practices and provide links to access tools and cancellation of subscription.
- Congress should consider requiring data brokers to clearly disclose to consumers (for example, on other websites) that they not only use raw data from their sources, such as a person's name, age address, and rank Income, but also derived from them certain data elements. Consumers should be allowed to access the data about themselves, particularly the case of sensitive information – and inferences about a consumer's sensitive preferences and their characteristics – such as those related to certain health informatio

- Congress should consider requiring data brokers the divulgation of the names and / or categories of their data sources so that consumers are better able to determine if they need to, for example, correct their data with a source of original public record.
- Finally, it should consider requiring entities to deal directly with the consumer to provide notice that is notorious for indicating that they share their data with data brokers and provide them with options on the use of data; such as the ability to unsubscribe from sharing your information with data brokers.

It should also consider the protection of sensitive information, such as certain health information, requiring that sources of direct treatment obtain explicit affirmative consent from consumers before collecting such information.

In this sense, because of consumers would know of the existence of data brokers, a meaningful advertisement from the data source provides an important opportunity for them to have knowledge that their information is shared with them and to be able to exercise control over the use of data.

Currently in the world there are two main aspects regarding to the protection of personal data: on the one hand is the US model that seeks to protect the information of people with the concept of the right to privacy, which can be extinguished with the death of the subject, The model emerged from commercial motives as companies used this information indiscriminately and as this fact has been shown to have aroused the State's concern.

On the other hand, the European model seeks to protect the information and property of the same, in order to preserve the honorability of the person even if the person has died, the motivation of this model is based on the human rights of individuals (Sánchez, 2012).

Current legislation tends to seek the protection of personal data, sensitive data and biometric data, although these concepts are not covered in the various regulations in a precise and separate way most often involved with each other. In order to achieve this protection, personal data protection laws have been enacted and in each country it has sought to adapt the bases of one of the two existing models of personal data protection to its own cultural, economic and political conditions. Among these we find:

- Organization of the United Nations (UN). In 1984, it adopted the document known as the Universal Declaration of Human Rights, in which article 12 states that no one shall be subjected to arbitrary interference with his private life, family, home or correspondence, or attacks on his honor or Its reputation, that every person has the right to the protection of the law against such interference or attacks.
- Germany. In 1970 the first law of protection of data (Datenschutz) was approved. In 1977, the German Federal Parliament approved the Federal Law Bundesdatenschutzgesetz. These laws prevent the transmission of any personal data without the authorization of the person concerned.
- Sweden. In 1973 it was published which was one of the first data protection laws in the world.
- United States of America. Data protection is based on the Privacy Act of 1974.
- European Union. The first international data protection Convention was signed in 1981 by Germany, France, Denmark, Austria and Luxembourg. It is known as «Convention 108» or «Strasbourg Convention». In the 1990s, a common standard rule was established that was called Directive 95/46 / CE. The directive concerns the protection of natural persons with regard to the processing of personal data and the free movement of such data. It should be borne in mind that the European Union has several directives on Data Protection and Laws of the Member States.
- Spain. The Organic law of Protection of Personal Data of 15 of 1999, establishes the Protection of Data of Personal Character. This law has been important for Latin America because it has been used as a strong reference of the European model. Also, in May of this year came into force the General Regulation on Data Protection, although it will not begin to be applied until two years later, it is important that organizations adapt their processes, since the new regulations imply a different management the one that is being used. The Spanish Agency for Data Protection, in its preventive aspect, wants to encourage that the entities can know the possible difficulties in its application to take measures that allow to solve them.

It should be noted that this legislation seeks to ensure that citizens have more control over their private information and incorporates among other regulations:

1. The right to «forgetfulness», through the rectification or suppresion of personal data.
2. The need for «clear and affirmative consent» of the person concerned to the treatment of their personal data, which cannot be inferred from silence or inaction.
3. «Portability», or the right to transfer the data to another service provider.
4. The right to be informed if the personal data has been pirated.
5. Clear and understandable language on privacy clauses.
6. Fines of up to 4% of global billing of the companies in case of infringement.

- Latin America. In Latin America, personal data protection laws arise as a need derived from the increase in the use of information technologies and the increase of associated vulnerabilities. Mostly, these laws resemble the European model.
- Russia. In 2006, an exhaustive law on the protection of personal data was approved.
- Mexico. The Federal Law on the Protection of Personal Data in the possession of private individuals was published in the Official Newspaper of the Federation on July 5, 2010, entered into force one day later and takes effect as of January 2012.
- In Peru, the Law of Personal Data Protection Law No. 29733 was promulgated in 2011 and states in its article 13, subsection 1 that the treatment of personal data must be carried out with full respect for the fundamental rights of its owners and that same rule applies to its use by third parties. In this same sense the subsection 5 states that personal data can only be treated with the consent of the owner, prior, informed, express and unequivocal consent. For its part, subsection 9 indicates that the commercialization of personal data contained or intended to be contained in personal data banks is subject to the principles provided by law. The principles to which they are mentioned are: Principle of legality, principle of consent, purpose, proportionality, quality, safety, disposition of resource and principle of adequate level of protection. Although the regulations would expressly prohibit the treatment of data, and it is therefore illegal to draw up a profile a la carte in our country, reality shows by far the opposite. In Peru the black market of databases with personal information has a surprising scope.
- In the Cercado de Lima – capital city – around Garcilazo de la Vega Avenue we can easily find a place where technology and crime are combined with what we could call pseudo wit for the personal data of millions of Peruvians sold freely. Curiously, the information offered in Wilson galleries is not only real, but is obtained legally by public and private institutions and with the consent of the clients, through virtual or physical forms or telephone calls. Remember that article 18 of the same legal body establishes that if personal data are collected online through electronic communication networks, the obligations related to the holder's right to information can be satisfied by the publication of privacy policies that must be easily accessible and identifiable, but at the same time Article 3 expressly states that the application of the rule is limited to the national territory when in reality happens that when giving our data on line it is most likely that in very few occasions will deal with entities or institutions established only within the national territory.

The data obtained come from banks, financiers, telephone companies, pharmacies, clubs, schools, discotheques, schools, professionals, discos, restaurants, insurers, AFP, hotels, among others, including public institutions. The information that can be found in this database includes from a simple name and email to credit lines, salaries and labor charges. A CD containing a large and detailed database can cost from thirty-five to one hundred dollars, evidently the information is offered according to the «customer's need». In this disk can be private information of up to four million people, in addition the price varies according to the antiquity of the data. They even sell a database of Spain, so that the call center can offer, from Lima, internet plans. Because the empire of illegality goes a long way, such as hacking emails and central credit risk, the preparation of «profiles

pay per view» only requires the request of the interested party and the respective payment. It is obvious that anyone in our country – not just companies offering products or services, but also extortionists, kidnappers, or any third party – may have access to our personal information, including sensitive data.

Consequently, this reality places us in a total state of defenselessness and complete affectation of our fundamental rights, which is not only theoretically contemplated in the Law of Protection of personal data establishing fines ranging from 0.5 to 100 TTU (Tax Tributary Unit) in case of non-compliance with its provisions, but also the Penal Code punishes improper treatment (access, copy, traffic and sale) of databases with penalties of up to five years in prison – an aggravating circumstance if it puts at risk National security. On the other hand, the law establishes that the National Authority for the Protection of Personal Data of the Ministry of Justice is the institution responsible for ensuring the proper use and administration of this information, pointing out that any institution or person that manages a database must register it in the National Registry of Personal Data Protection, which should specify the number of people included and the way in which the information was obtained. Non-registration of the database constitutes a serious offense sanctioned with more than 5 UIT up to 50 UIT while at the same time processing personal data in contravention of the principles established in the Law or in breach of its other provisions or those of its Regulations, when they are prevented or violated against the exercise of fundamental rights is planned with a sanction between 50 and 100 UIT.

Although on the one hand we have that the main objective of the National Authority of Personal Data Protection of the Ministry of Justice is to cut the chain of exit of personal information to avoid it circulating in the market – for which several informative talks are realized for the companies as well as control actions – and on the other hand we have a regulation that expressly refers in its article 2, subsection 17 to the treatment of personal data, such as any automated or non-automated technical operation or procedure, which allows the collection, registration, Organization, storage, preservation, elaboration, modification, extraction, consultation, utilization, blocking, suppression, communication by transfer or diffusion or any other form of processing that facilitates access, correlation or interconnection of personal data, in addition the corresponding Regulation of the law, Supreme Decree No. 003-2013-JUS, states that the treatment of personal data must be carried out with full respect for the fundamental rights of its holders; The reality still presents a huge gap between the treatment given by third parties and the protection that the law intends to grant and guarantee. However, from Peruvian legislation and international regulations on the protection of personal data can be inferred that the figure of data brokers would be implicitly regulated and, consequently, the unauthorized treatment of the data expressly prohibited. So we ask ourselves about the need for a specific regulation that contemplates a prohibition and consequent penalty for nonobservance, even more so when our legislation in criminal matters expressly sanctions this behavior.

In this sense although online and offline companies are subject to regulations regarding the way in which our personal data should be handled, it happens that their privacy policies and their terms of service often lack clarity about the protocols used to safeguard our information. While the Internet user Ignore the fact of considering that their data could begin to circulate indiscriminately on the Internet with the use of mobile phones alone that can collect data on localization, language patterns, movement, among others, and application developers save various kind of personal information. Being so, every time we upload a photograph to a social network we are sending metadata about the place, date and time it was taken including the model of the phone that made it. In a country such as ours where crimes that are «socially acceptable» still exist, it is almost common for databases to be offered and acquired according to rubrics, sectors, seniority and categories, so it is clear that we still have a long way to go.

6. Conclusions

- Despite having a normative framework that seems to have provided all the probable forms of affectation to our personal data and sensitive data, the environment makes us rethink the possibility of having additional mechanisms of guardianship that probably go beyond the legislative system and that allow us to help achieve the purposes for which the rule was created, perhaps one of the main aspects to consider is the awareness about the extreme importance of our data and the permanent risk to which we are exposed with a liable treatment.

- It is necessary to have a special legislation to improve the transparency of industry practices in relation to the collection of data and its disposition to third parties as well as to establish minimum standards regarding the privacy policies and terms of service of companies.
- We must reflect about the process of denaturation that our data are suffering to the point of having lost its intrinsic nature to become a raw material of great demand and utility in the market.
- The legislation must provide for specific protection modalities in relation to the profiles created on demand, since the fact that third parties are able to predict our behavior, selections or personal deployments entails a serious chain of violations of many fundamental rights.
- It is important to consider the initiative of the American Commission in order to replicate a similar experience in Peru tending not only to identify those companies that have been carrying out these practices but also, after a relevant analysis based on the results obtained, to determine to what extent it would be possible to take as a reference the recommendations offered by the Commission.

7. References

Federal Trade Commission., 2012 (accessed October 15, 2015). Recommendations for Businesses and Policymakers. Available at: https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers.

Federal Trade Commission., 2014 (accessed October 12, 2015). Data Brokers a call for transparency and accountability. Available at: https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

MINJUS., 2011 (Accessed October 10, 2015). Personal Data Protection Act, Act Nº 29733, 2011. Available at: http://www.minjus.gob.pe/wp-content/uploads/2013/04/LEY-29733.pdf.

MINJUS., 2013 (Accessed October 10, 2015). Regulation of the Act Nº 29733, Personal Data Protection Act-SUPREME DECREE Nº 003-2013-JUS. Available at: http://www.minjus.gob.pe/wp-content/uploads/2013/04/DS-3-2013 JUS.REGLAMENTO.LPDP_.pdf.

Sánchez, G., Rojas, I., 2016 (accessed July 12, 2016). Laws of protection of personal data in the world and protection of biometric data - Part I. Available at: http://revista.seguridad.unam.mx/numero-13/leyes-de-protecci%C3%B3n-de-datos-personales-en-el-mundo-y-la-protecci%C3%B3n-de-datos-biom%C3%A9tricos-%E2%80%93.