ECONSTOR
Make Your Publications Visible.

A Service of

ZBW Leibniz-Informationszentrum Wirtschaft
Leibniz Information Centre for Economics

Blades, Nicholas; Herrera-González, Fernando

Conference Paper

An Economic Analysis of Personal Data Protection Obligations in the European Union

27th European Regional Conference of the International Telecommunications Society (ITS), Cambridge, United Kingdom, 7th - 9th September 2016

Provided in Cooperation with:
International Telecommunications Society (ITS)

Suggested Citation: Blades, Nicholas; Herrera-González, Fernando (2016) : An Economic Analysis of Personal Data Protection Obligations in the European Union, 27th European Regional Conference of the International Telecommunications Society (ITS), Cambridge, United Kingdom, 7th - 9th September 2016, International Telecommunications Society (ITS), Cambridge, UK

This Version is available at:
http://hdl.handle.net/10419/148661

Standard-Nutzungsbedingungen:

Die Dokumente auf EconStor dürfen zu eigenen wissenschaftlichen Zwecken und zum Privatgebrauch gespeichert und kopiert werden.

Sie dürfen die Dokumente nicht für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, öffentlich zugänglich machen, vertreiben oder anderweitig nutzen.

Sofern die Verfasser die Dokumente unter Open-Content-Lizenzen (insbesondere CC-Lizenzen) zur Verfügung gestellt haben sollten, gelten abweichend von diesen Nutzungsbedingungen die in der dort genannten Lizenz gewährten Nutzungsrechte.

Terms of use:

Documents in EconStor may be saved and copied for your personal and scholarly purposes.

You are not to copy documents for public or commercial purposes, to exhibit the documents publicly, to make them publicly available on the internet, or to distribute or otherwise use the documents in public.

If the documents have been made available under an Open Content Licence (especially Creative Commons Licences), you may exercise further usage rights as specified in the indicated licence.

WWW.ECONSTOR.EU

Mitglied der Leibniz-Gemeinschaft

AN ECONOMIC ANALYSIS OF PERSONAL DATA PROTECTION OBLIGATIONS IN THE EUROPEAN UNION

September 2016

Nicholas Blades

Fernando Herrera-González

Abstract

The collection, storage and processing of data have become easier and cheaper with the development of the Internet and the evolution of ICT technologies in general. This may be a cause (or a consequence) of new business models that rely on the exploitation of these stored data in order to try to extract some kind of value.

If some value is found in personal data and in its processing in large volumes, this value would increase social welfare. In order for the value of an asset to be appraised, entrepreneurial activity is required. This is process of trial and error which may be hindered by regulation, due to the limits that this imposes on economic activity, for different reasons.

In the European Union, the 1995 Data Protection Directive, the ePrivacy Directive and the more recent General Data Protection Regulation put limits to the exploitation of personal data. These limitations can be synthetized around the four rights that they grant individuals, the so-called ARCO rights: access, rectification, cancellation and objection.

In this paper, the consequences of the data protection rights on entrepreneurial activity are analysed, and thus on the value that may be accrued from data related to individuals, and on social welfare. As a conclusion, some policy recommendations are proposed to achieve a balance between legal rights in the EU and possibilities for social welfare improvement.

1. Introduction

The collection, storage and processing of data have become easier and cheaper with the development of Internet and the evolution of ICT technologies in general. This may be a cause (or a consequence) of new business models that rely on the exploitation of the stored data in order to try to extract from it some kind of value.

It seems clear that if some value is found in personal data and in its processing in large volumes, this value would increase social welfare (in the same way that would happen if a new use is found for any existing resource). In turn, this means that the owner/controller of each piece of personal data would become richer, because they would control a more valuable asset. Of course, it could also be the case that personal data has no value or not enough to compensate for the costs of storing and processing it.

In order for the value of an asset to be appraised, entrepreneurial activity is required. Specifically, in the case of personal data, it is necessary that entrepreneurs anticipate resources to collect, store and process these data. Only once this has been done, can the resulting product be offered in the market and the price observed, providing some measure of its value. If at that moment the obtained price allows the recovery of the invested resources, the entrepreneur will obtain a profit and we will be sure that the activity creates value for society.

The entrepreneurial process is one of trial and error in which the entrepreneur should be granted the maximum degree of flexibility. If their possibilities are limited, so are the chances that they are able to find value in the asset, in this case, personal data.

However, regulation puts limits on the freedom of entrepreneurs, for political or other type of reasons. An economic analysis should not care about the political reasons behind a specific regulation, assuming that it comes from the wish of the majority of citizens as can be expected to happen in democratic countries. But it is in any case legitimate for an economist to try to identify the economic effects of regulations and ascertain how they impact social welfare.

In the case of personal data in the European Union, at least two directives define regulation and put limits to the exploitation of personal data: the 1995 Data Protection Directive and the more recent General Data Protection Regulation. These limitations can be synthetized around the four rights that they grant individuals, the so-called ARCO rights: access, rectification, cancellation and objection.

In this paper, we propose to analyse the consequences of the data protection rights granted by the EU regulatory framework on social welfare. In order to do so, we will assess the catallactic efficiency of the personal data market in the EU. Catallactic efficiency defines the optimal conditions in which a market can increase social welfare with a dynamic perspective.

As will be shown, one of the main features of the catallactic efficiency is the requirement of well-defined property rights. Current EU regulation formally precludes the ownership of personal data. However, there are businesses in the EU that are built around the control and processing of personal data, meaning that there are *de facto* some kind of property rights at work. We propose a property right analysis for personal data that conciliates both views and allow us to pursue the analysis of the effects of ARCO rights on social welfare. Absent actual property rights this analysis would be meaningless.

The rest of the paper is structured in the following way. In the second section, the growing literature on economics of privacy will be surveyed, identifying the place that the present contribution holds among the rest of the literature.

In the third section, the concept of catallactic efficiency will be presented, and its suitability for the analysis at hand justified. After that, we will summarize the main features of the current EU regulatory framework for personal data protection, that, as has been said, consists of the Data Protection Directive and the more recent General Data Protection Regulation.

Once presented both the methodology and the subject of the analysis, in section 5 the analysis is actually carried out. In the first subsection, a property rights analysis will be proposed, providing the basis for the analysis of the effects of the ARCO rights

presented in the second subsection. Effects are depicted distinguishing three categories of personal data: provided, generated and inferred data.

The paper closes with section 6, which summarizes the results of the analysis and concludes with the consequent policy recommendations.

2. Current state of the art about the economic theory of privacy

The contribution of this paper may be included in the growing corpus of what is called economic theory of privacy. It deals with the impact on welfare of personal data transactions and of its interruption, be it voluntarily or by means of government intervention.

There have been some recent surveys of this literature, which we use as a base for our own survey. More specifically, we use Acquisti (2011), Padilla (2015) and Larouche et al (2016).

The main focus of the economic theory of privacy is the analysis of the effect on welfare of government intervention on the flow of personal information, that is, the effects of privacy regulation.

Posner (1981) and Stigler (1980) argue against regulation of privacy. Posner (1981) compares the concealment of personal data with that of information about a product when selling it. This concealment "*reduces the amount of the information in the market and hence the efficiency with which the market allocates resources*", and of course no one would "*think it efficient to allow sellers to invoke the law's assistance in concealing defects in their goods*" in the same way that privacy laws would justify the individual being untruthful when offering himself in the labour or in the *"spouses market"* (p.406).

For Stigler (1980, p.635), "*in voluntary transactions there is no reason to interfere to protect one party provided the usual conditions of competition prevail: the efficient amount of information will be provided in transactions, given the tastes of the parties for knowledge and privacy*". He later explains (p.639) that "*privacy legislation in*

general increases the cost of achieving a given level of classification". For Stigler, if legislation supresses the distinguishing mark, some other methods for the required distinction will be used, that are necessarily less efficient (otherwise, they would have been used in the first place).

Noam (1997) formulates the previous idea in a different way, by formulating it in terms of the value of privacy. Accordingly, privacy law would be ineffective because the main force at play is the comparison between the value of privacy for the individual, and the value that the acquiring firm gives the personal data. If the first is above the second, the personal data will remain protected, no matter what the law says. In the contrary case, both parties are interested in the transaction and will likely find a way to achieve it.

From an empirical perspective, Goldfarb and Tucker (2011) provide empirical evidence that privacy regulation may diminish the effectiveness of on-line advertising. Their study refers to the privacy regulation in the EU, which restricts the advertisers' ability to collect data on web users in order to target ad campaigns. It is based on the responses of 3,3 million survey-takers randomly exposed to 9.596 banners.

Tucker (2012) summarizes a set of recent empirical studies. This shows the trade-off between desire of firms to supply targeted information and the disutility imposed on its consumers, to which firms seems to be subject. For example, rational customers may not buy a given product to avoid signaling its willingness to pay or to avoid unsolicited marketing.

The view that voluntary transactions of personal data always increase social welfare has been challenged on the basis of the existence of market failures and on the basis of possible bias in the decision by the individual.

Thus, Varian (1996), although afraid that a "*legislative solution would likely result in a very rigid framework that assigned individuals additional rights with respect to information about themselves, but did not allow for ways to sell such property rights in exchange for other considerations*", identifies a possible negative externality on the consumers in the case of secondary usage of personal data (i.e, resale). In this case, the consumer does not profit and may bear the cost of the misuse of the data by the third

party. Varian (1996) proposes that legislation should forbid the resale of personal data without explicit permission.

With regards to the first basis, most of the literature consists of models showing than in specific circumstances privacy protection (not necessarily through regulation) may be welfare increasing.

For example, Taylor (2004) show that the improvement on social welfare of allowing firms to share personal data depends on the capacity of the consumers to anticipate which use will be given to personal information. He shows that the banishment of the sharing of personal data could be welfare enhancing for those naïve customers that are not able to anticipate the practices of the firm and consequently protect their data. Regulation, however, would not be necessary if consumers were aware of how merchants will exploit their data, and strategic enough to adapt their behaviour accordingly.

Acquisti and Varian (2005) use a two-period model to explore the profitability of history-based pricing, assuming that firms have access to “tracking" technologies and customers are rational and have access to “hiding" technologies. They conclude that profits (and thus social welfare) increase only if the tracking allows the firm the provision of additional personalized services.

Hermalin and Katz (2006) argue that data protection may support some valuable insurance schemes, which would not survive in the absence of privacy protection.

Calzolari and Pavan (2006) study the conditions in which it is optimal for a firm to offer full privacy to the client, using a model of agency. They find that, unless a set of three specific conditions is met, disclosure may be optimal, even when the firm dos not pay for the information. They also show that disclosure may be welfare increasing even for the client.

Shy and Stenbacka (2016) focus on the conditions in which exchange of personal data among firms may be welfare enhancing. According to them, weak privacy protection (only information on past purchases is shared) generates more profits than no protection

(all information may be shared) or strong privacy protection (no info is shared); consumer welfare is highest with strong privacy protection. They conclude that total welfare increase with the degree of privacy protection unless firms recognize consumer-specific switching costs, in which case pricing conditional on switching costs has favorable implications for consumer surplus and total welfare.

With regards to the second basis (behavioral bias), Acquisti et al (2015) provide a very good and complete overview of the state of the art. Economic literature shows that there are behavioral biases that cause imperfect decision-making in individuals. For example, consumers act myopically when trading off the short term benefits and long term costs of information revelation and privacy invasions; also, consumers seem not to act rationally when deciding on privacy. In these conditions, privacy regulation may be required, because the market equilibrium will tend not offer privacy protection to individuals.

After surveying the current state of the art for the economic theory of privacy, the following may be concluded

- There is plenty of literature about the economic theory behind a possible regulation of privacy. One part of it deals with the issue in generic terms, without considering the specific regulation under discussion. For example, Posner (1981), Stigler (1980), Varian (1996) or Noam (1997) or Shy and Stenbacka (2016).
- Another set of papers define specific models in order to study the issue. These models try to identify instances in which regulation could be welfare enhancing with respect to the free market approach, but they do not usually deal with the possible consequences of regulation. It is the case of Hermalin and Katz (2006) or Taylor (2004).
- The same happens with the papers dealing with the economics of privacy from a behavioral point of view.
- No literature has been found referring to the consequences of the current EU privacy regulation for the social welfare. Some papers, like Christensen et al (2013), throw some light on the issue, by estimating the costs that some of the

requirements of the regulation will impose on SMEs, but this is of course just a partial view of the effects on social welfare.

This paper pretends to fill the identified gap. Instead of dealing with the issue of privacy in generic terms, it focuses on the specific regulation in place in the Europe Union and try to identify concrete effects of this regulation on the market, and to ascertain if they are or not welfare enhancing. And instead of identifying market failures or behavioral issues that could justify privacy regulation, it starts from the current regulation and look for intended or unintended consequences. Moreover, the focus is on general welfare, not just on the effects on a concrete group of individuals.

In the following section, as the first step, the standard that will be used to evaluate if the EU privacy regulation is welfare enhancing or nor will be presented.

3. Theoretical framework: catallactic efficiency

The efficiency of regulation, that is, the actual increase is welfare that regulation causes, is usually measured taking as reference the model of perfect competition. Thus, if regulation is able to approach the workings of the market to the way (or the outcomes) of the model of perfect competition, this regulation is deemed to be efficient as it increases social welfare.

However, criticism to the model of perfect competition as a reference for market efficiency has come from several and prestigious sources[1]. The main problem with this model is its static nature, which makes impossible for the model to explain innovation or investment. It has also been criticized on the grounds of its feasibility and of its actual desirability for the individuals.

Because of this, we have opted for an alternative standard, that of catallactic efficiency, originally proposed by Cordato (1992). We think that this model is more complete and relevant in this case because of its dynamic nature, as will be readily shown.

[1] For a survey of these criticisms, see Soria & Herrera-González (2013).

The catallactic efficiency goes beyond the concept of economic efficiency by recognizing that the market is formed by different individuals with different rankings of goals. That is, the starting point of the catallactic efficiency is the fact that every and each individual is different and has different preferences. Each individual may be able to optimize the economic efficiency of his resources with respect to his goal (supposing he knows both resources and goals), but this economic efficiency does not say much about the efficiency of the market or the regulation.

In order to measure the market efficiency, it is necessary to acknowledge that the economic system is composed by the economies of the individuals and institutions acting in the market (what Cordato (1992) calls *catallaxy*) thus there is no overall hierarchy of ends that can be ranked on a single scale of values.

As already said, economic efficiency is confined to the question of relative appropriateness of alternative means in the pursuit of a given hierarchy of ends, but it is not enough to assess social welfare. In this case, the rankings of goals of all individuals should be taken into account. The efficiency of a catallaxy can be judged by the extent to which it promotes individual economic efficiency.

Economic efficiency involves: 1) The setting of the goals; 2) The formulation and execution of plans to accomplish those goals; and 3) The access to physical resources that allow the execution of plans. In brief, in order to accomplish their goals, individuals must be able to acquire the appropriate knowledge and the appropriate resources. An efficient market should facilitate individuals both process of acquisition.

In consequence, when we refer to the catallaxy in which all different individuals pursue their economic efficiency, the focus has to shift to the institutional setting in which individual actors operate. This institutional setting should facilitate the use and discovery of information, on the one side, and should allow individuals to gather the necessary physical resources, on the other. In the measure that individuals are able to accomplish both actions more easily, their economic efficiency will be improved.

Cordato (1992) is able then to identify the ideal institutional setting, which can be used as a benchmark against which real institutions can be judged and public policy proposals can be measured. The institutional setting is characterized in terms of two elements, as enablers of the two processes of acquisition that an individual requires in order to increase his economic efficiency:

1) Private property as the institution that allows the individual the access and control of the resources needed to accomplish the plan.

2) The price system as the most efficient device to disseminate information concerning exchange opportunities.

Cordato (1992, chapter 4) synthetizes the application of the catallactic efficiency framework into the answer to two questions: 1) Does the proposed regulation violate property rights? 2) Does the proposed regulation distort the price system? If it is the case, then the regulation decreases catallactic efficiency and reduces social welfare.

Seen from the complementary point of view, if the current institutional setting differs from the ideal (well defined property rights, undistorted price system), there is room for regulatory changes to improve the catallactic efficiency.

These criteria offer a policy benchmark against which to measure public policy proposals. Instead of comparing with an ideal set of market outcomes (perfect knowledge, homogeneity of product, several firms…), as economic efficiency does, catallactic efficiency compares institutional settings against the ideal settings described above. It can also compare one setting against another to see whether one institutional approach is better than another in respect of social welfare. Because of this, and unlike economic efficiency, it is useful for a dynamic environment, in which the competitive process is seen as an open-ended process instead of as the achievement of a state of equilibrium.

Summing up, in order to assess whether the current EU privacy legal framework is welfare enhancing, we need to analyse how it fares in terms of catallactic efficiency. And, for that, we need to ask two questions: Does this framework violate property

rights? Does it distort the price system? Answers will be provided for both questions, but before proceeding, the legal framework object of analysis has to be presented.

4. EU current legal framework for personal data exploitation/protection

Both the EU Treaty[2] and its Charter of Fundamental Rights for EU citizens[3] ensure that citizens have the right to "*to the protection of personal data concerning him or her*". The Treaty lays down the basis under which EU data protection legislation was produced. The Charter goes a little further[4]:

> "*Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.*"

This forms the basis of the so-called ARCO rights related to personal data: Access, Rectification, Cancellation and Objection, whose economic analysis is the object of this paper.

The current EU legal framework, deriving from the Treaty obligations for the protection of personal data is split into two parts; one deals with the access to and protection of personal data for the purposes of law enforcement, the other part deals with the protection of personal data in the commercial environment. In our analysis we will focus on this second set of legislation, as it is where the ARCO rights are defined.

The principal general legislative instruments are[5]:

- The 1995 Data Protection Directive[6];
- The 2016 General Data Protection Regulation (GDPR)[7].

---

[2]Treaty on the Functioning of the European Union (TFEU), Article 16(1)
[3] Charter of Fundamental Rights of the European Union, 2010/C83/02; Article 8(1)
[4] Article 8(2)
[5] In addition, there is a further layer of regulation for the transmission of data by Electronic Communication Networks,in the 2009 e-Privacy Directive.
[6] 1995/46/EC of 24 October 1995 http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=en

In order to assess the impact on the institutional setting created by these legislative instruments, we summarise the various relevant Articles of the instruments against the criteria set out by Cordato (1992).

4.1 The Data Protection Directive

Article 1 enshrines a right to privacy with respect to the processing of personal data as part of a fundamental human right ('fundamental rights and freedoms of natural persons').

Article 2 defines '*personal data*' in a legal sense as '*any information relating to an identified or identifiable natural person*'. The concept of a '*data controller*' is also defined, as a legal person which determines what should be done in relation to processing personal data. A '*processor*' can be a third party which undertakes the act of processing data for the data controller. The concept of '*the data subject's consent*' is also defined as '*any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.*'

Article 6 ensures the quality of data and also limits the scope of what can be collected and processed for '*specified, explicit and legitimate purposes*': the amount of data collected for a given purpose must not be excessive to the completion of the purpose; moreover, the quality of the data should be assured, in that it should be accurate and kept up-to-date. The data controller is responsible for data quality. Article 7 provides greater clarity as to the conditions under which personal data can be processed; with consent, in performance of a contract to which the subject is party, compliance with legal obligations and a more general '*legitimate interests*' defence which is constrained by the fundamental rights of the data subject under Article 1.

Article 8 prohibits the processing of sensitive data (race, political opinion, trade union affiliation, religious belief, health and sexual activity) except where explicit consent has

[7] Regulation (EU) 2016/679 of 27 April 2016 http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

been obtained. However, it provides for Member States to prohibit the giving of consent by the individual, allowing an absolute right to privacy to be imposed by the State notwithstanding the wishes of the individual[8].

> "*the data subject has given his explicit consent to the processing of those data , except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject's giving his consent*"

The right to privacy is removed if these data are '*manifestly made public by the data subject*'.

Articles 12 to 14 define the so-called ARCO rights of the data subject, for Access to personal data held by the data controller and rectification of any errors or deletion of the data (Article 12), and the right to objection to the processing of data (Article 14).

The right of Access is defined in paragraph (a); it encompasses access to "*confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed*" and to "*knowledge of the logic involved in any automatic processing of data concerning him*". This information should be communicated to him "*in an intelligible form of the data undergoing processing and of any available information as to their source"* and without "*constraint at reasonable intervals*" or "*excessive delay or expense*".

Rights of Rectification and Cancellation (Erasure) are granted in paragraph (b) and (c). This right may be exerted of data "*the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data".* These rights include the notification of the action to third parties to whom the data have been disclosed, "*unless this proves impossible or involves a disproportionate effort.*"

The right of Objection is defined in article 14. The user may "*object at any time on compelling legitimate grounds relating to his particular situation to the processing of*

[8] Article 8(2)a

data relating to him". This right should be granted at least in the case in which the processing of data "*is necessary for the purposes of the legitimate interests pursued by the controller*" (Article 7 (f)). If the objection is justified, the controller may no longer use that personal data in its processing. Paragraph (b) refines the right of objection for the cases of disclosure for purposes of direct marketing.

4.2 The General Data Protection Regulation (GDPR)

Since the 1995 Directive was put in place, the processing of data has moved on significantly characterised by:

- Higher levels of data aggregation and processing – so-called "Big Data"
- Extensive data transfers to third countries, requiring a less cumbersome system of oversight to efficiently achieve the stated regulatory objective; and
- Increased automation of services based on processed data, rather than storage of records, as is implicit in the 1995 Directive.

As a consequence, in 2012 the EC started a review of the 1995 Directive, which ended earlier this year with the passing of the General Data Protection Regulation (GDPR). The GDPR is quite wide-ranging, being a horizontal regulation covering all industries. We only summarise the provisions that are relevant to the rights of individuals and where they do not repeat the 1995 Directive.

Personal data is more explicitly defined than in the 1995 Directive[9]:

> ' *'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one 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;*'

[9] Article 4(1)

Article 5(1)e creates a "shelf life" for personal data stored by a data processor, in that it can be identified with the subject "*for no longer than is necessary for the purposes for which the personal data are processed*".

Article 7 further specifies and defines the concept of "consent" to the collection and processing of personal data, making it informed consent. Consent can also be withdrawn and this process should be as frictional as the process of giving consent in the first place. Article 7(4) addresses the issue of excessive data collection, in that if data is collected with consent, but that these data go beyond what is necessary for conclusion of a contract or delivery of a service, then there is a presumption that consent has not been given for processing of this "excessive" data.

> "*When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.*"

Articles 15-22 clarify and enlarge the ARCO rights of data subjects previously defined.

Regarding the right of Access, Article 15 itemizes the personal data to which the user has this right, adding an item that was not mentioned in the Data Protection Directive: "*where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period*" (1 (d)).

It also imposes the controller the obligation to provide a copy of the personal data undergoing processing. (3)

Finally, article 20 confers, in certain conditions, the right to data portability, obliging the controller to provide the user with the above data *"in a structured, commonly used and machine-readable format"*, which may be transmitted to another controller "*without hindrance from the controller to which the personal data have been provided".*

Article 16 makes explicit the right of Rectification ("*the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her*") and incorporates a sort of right for completing the personal data.

Article 17 (1) details the conditions in which the user may exert the right of Cancellation (Erasure). The possible grounds for exerting the rights are increased and also clarified with respect to the Data Protection Directive. Article 17 (2) defines the "right to be forgotten" by requiring from the controller a certain set of actions in case of the erased personal data having been made public.

Finally, with regards to the former right of Objection, Article 18 defines what could be termed as temporary objection, detailing the conditions in which this restriction of processing may be obtained.

4.3 Summary

In this section, the rights the regulatory framework confers to users in relationship to personal data have been described. It has been shown that these rights may be grouped around the rights of Access, Rectification, Cancellation and Objection. We have also detailed the evolution in the scope of these rights from the Data Protection Directive to the GDPR, to enter in force in 2018.

Some general issues with impact on the ARCO rights has also been assessed, such as the concept of "personal data", the figure of the controller, conditions for consent and purpose, and the life cycle of personal data.

We are now in conditions to assess the catallactic efficiency of the ARCO rights and thus its contribution to welfare enhancement. This will be done in the next section.

5. An assessment of the catallactic efficiency of the ARCO Rights for Personal Data

As explained in section 3, assessing the catallactic efficiency of a policy or regulation is tantamount to answering two questions about it: 1) Does it violate property rights? 2) Does it distort the price system? In this section we will try to answer both questions for above described rights for personal data.

However, in order to deal with both questions, we need first to solve an apparently easier one: who is the owner of personal data? Only with this knowledge, it is possible to ascertain if and how property rights are violated. The subsection 5.1 deals with this issue; once solved, subsection 5.2 assesses the catallactic efficiency of the ARCO rights according to the proposed interpretation.

5.1 Property rights on Personal Data[10]

The origin of property rights may be traced to the core of economic theory: scarcity of resources. Individuals have needs, whose satisfaction requires resources to be obtained from the surrounding world. Some of these resources exist in abundance; such amount that every individual can satisfy his/her needs without limiting the satisfaction of the rest of the individual, they are not scarce. It is worthwhile to note that scarcity or not of a concrete resource is dynamic and dependent of the needs of individuals in each context.

Arguably, most of the resources we require to satisfy our needs are limited. This implies a high likeliness of conflicts about their use, among those individuals willing to use them, and aware that NOT all needs will be satisfied with the available amount of the commodity. The institution of property rights provides an easy and possibly fair solution to this issue. Thus, property rights try to prevent interpersonal conflict over scarce resources. Note that it is the scarcity of the good which makes property rights necessary to prevent the conflict. Conversely, with a dynamic perspective, the very possibility of conflict over a resource renders it scarce.

The way in which property rights operate is well known: they allocate exclusive ownership of resource to specified individuals (the owners). So, it is for the owner to decide what to do with the owned resource, and not for other individuals. In this way, conflicts are prevented ex-ante. Of course, there still may be conflicts about who is the owner or about the bounds of the property rights, among many other issues.

[10] See Herrera-González & Blades (2016) for a more detailed explanation of the ideas here exposed.

To be effective, property rights should be discernible and fair[11]. Property borders have to be objective (interpersonally ascertainable) and unambiguous so that other individuals may avoid using the goods owned by others. On the other hand, property rights have to be seen as fair by those affected; otherwise, they would resort to the use of force or other means and no property rights could be said to exist.

With regards to the acquisition of property rights, it is generally accepted that the property of a good produced from other goods belongs to the owner of the later goods. Let us now turn back to the issue at hand, namely the property rights of personal data.

Personal data refers to personal pieces of information, such as name, address or age, and to information about our behavior in the Internet (websites visited, contacts, purchases, location…), but also in other areas of our life (by means, for example, of the Internet of Things). Initially, these data are in an abstract form that makes impossible its exploitation for anyone. In order for the data to be useful, they must be materialized in a concrete physical medium. Materialization of personal data requires the investment of resources such as storage space or applications, together with labour and time of the individuals that enter and maintain the data.

Now that the data is in a physical form, the question of the ownership of data becomes relevant. While the data was abstract, no property rights seemed necessary: It is clear that the use of my name, my age or the colour of my eyes by me does not exclude using those same name, age or colour by other people. The same could be said of the list of websites visited in my last connection, or of the places I went in my car last week. Nobody says he owns his name, the colour of his eyes or the itinerary of his last trip. Personal data in its abstract form is not owned in the traditional sense of the term, because as it cannot be used, has no value and there is no need of property rights for it.

However, things change once the personal data is materialized in a physical medium. Imagine that I write down on a piece of paper some personal attributes as those

[11] Hoppe (1989), p. 138.

mentioned above. This piece of paper with the data may have value for some individuals (possibly due to the data on it). As this piece of paper is a concrete good, scarce, and with clear bounds, conflicts may arise if several individuals want to use it. In consequence, to prevent this conflict, property rights should be defined for it.

In the example above, there should be no doubt that it is the owner of the piece of paper on which the data has been written who owns the asset (doubts could arise if another individual is the one who writes the data on the paper). But it is clear that the individual whose data is written has in principle no claim on the property of the materialized data: he did not provide any of the scarce resources for the venture. He may just have told the data to the individual who was writing it down, but this did not restrict him of "using" it in the future, for example, to provide it to other parties.

Summing up:

1) No property rights are required for personal data in abstract form
2) In order to obtain value, personal data has to materialize in a concrete physical medium.
3) The owner of the materialized personal data is logically the owner of the resources invested in its materialization
4) In principle, the owner of the data could do whatever he wants with his asset, included its possible interchange for other resources.

As the controller "*determines the purposes and means of the processing of personal data*" we can conclude that the controller is actually the owner of the personal data from an economic theory point of view, in light of the 3) above. Depending on the terms of his agreement, the processor could also become the owner of the personal data.

Observe that individuals ("*data subjects*" in regulatory terms) do not "own" their personal data, as counter-intuitive as it may sound. It is just not possible to own personal data while they are in an abstract form. However, each individual has power over them: he can choose to whom to reveal it and to whom not, and what kind of data or the level of detail to provide. This is a service that each individual can uniquely provide to the interested parties. In any case, once the service is provided, the

materialized data is given away and its ownership rests not with us, but with the owner of the medium in which it is kept, the same way we own the files in our hard disk.

Before going ahead, we have to deal with another important issue. It is true that the controller "*determines the purposes and means of the processing of personal data*", but in order to acquire the data subject's consent, it is required to transparent as to the current and future uses to which data is put. In a dynamic context of innovation, the whole point is that the controller needs to experiment with the personal data in order to see if it has any value and how to extract it. So, even if the controller has an initial idea on how to use the data, it may and will probably change in unexpected ways as the entrepreneurial process evolves.

So, the above requirement would be tantamount to require either the firm to know ex ante what all the uses of the data shall be going forward, or to write the contract (terms and conditions) so broadly that they catch all possible future uses.

We have not observed a catalogue of cases brought by regulators claiming that consumers are not making informed choices. We do, however, observe firms regularly updating their terms and conditions and making acceptance of such terms a condition of continued use of the service. This suggests that innovation in the use of data is taking place and that contracts are updated to reflect such innovations.

To conclude, whilst this requirement does increase costs (at least in terms of privacy lawyers) it appears not to be hindering the use that controllers may make from the acquired personal data and is not significantly impeding innovation at present. It remains to be seen whether in the future, a stricter interpretation or enforcement of the existing statute might more negatively impinge on the property rights of the controller. There is also a longer run consequence of the requirement for specific consent, if the firm no longer has a relationship with the individual it cannot seek further permissions from that customer for processing of its data then such data becomes less valuable over time as a result (relative to data useable without restriction).

5.2 Impact of ARCO rights on the catallactic efficiency

Having shown that property of materialized personal data (the only kind that may be exploited and thus be valuable) correspond to the controller/processor, and also that the related property rights do not seem to be much constrained by the requirement of transparency of purpose to attain the consent of the data subject, we can at last address the issue of the catallactic efficiency of the ARCO obligations.

After describing the content of the ARCO rights, it is clear that their possible effects concentrate on property rights. At first glimpse, they do not seem to distort the price system, at least not in a direct way. Because of that, our focus would be on the first of the questions required to assess the catallactic efficiency of regulation. In sum, we can now re-formulate the catallactic efficiency assessment into the following question: Do the ARCO rights violate the property rights on personal data acquired by the controller/processor? If it is the case, how and with what effects?

Prima facie, it is clear that ARCO rights put limitations on the use that the controller/processor can make of his property. For example, the right of access obliges him to put the data at the disposition of the individual to which it refers, something that the controller may or may not be interested in doing. The same may be said of the rest of the rights. This is nothing new: rights granted to individuals are always two sided, the other being that of the obligations arising as a consequence of those rights. If an individual is granted the "right to have a boy/girlfriend", then someone will be obliged to be his/her girl/boyfriend. In the case under analysis, the ARCO rights translate into obligations for the owners of the personal data, ie, limitations to the use of their property. Thus, ARCO rights actually reduce the catallactic efficiency of the market.

Having said that, what is important is to determine the degree to which they diminish the social welfare and, ideally, compare that diminution with the alleged profits of having those rights.

For this analysis, it is useful to distinguish personal data according to their origin, because the effects of ARCO rights may completely differ from one to the other. In the

first place, there is the data provided by the individual explicitly in the transaction to acquire services from the data controller or firm, which we will call "explicit data". In most cases, the firm will need to generate data in order to provide the service to the customer (for example, the call data records required to bill or account for a telephone call); this is the "implicit data". Finally there is a set of data that is much more prevalent today than it was at the time that the 1995 Directive was conceived – "inferred data", that is data inferred by the firm from the user's activity usually through an algorithm.

The understanding of which of these data should be considered personal, and so subject to the above referred rights, is fundamental to ascertain up to which point the property rights of the controller are affected by the regulation.

Absent regulation we find that:

- Explicit data might be provided with or without restrictions on its use, based on developing preferences amongst users with regards to the level of privacy they are willing to forego in exchange for the provision of services;
- Implicit data has always been created for services and used in the delivery of services. To the extent that it has now become a useful input for the firm beyond its primary purpose of executing the provided service, it might be stored for future analysis. However, the cost of storage will begin to place a constraint on the firm's willingness to store these data indefinitely pending a future use; and
- Inferred data seems to be the value added in the modern internet economy. Some of this added value might relate specifically to the user, with regard to their preferences, behaviour or connections. In other cases value might be found by analysing the data in aggregate from a large cohort of users to which the individual belongs. This might provide helpful information both in the abstract (e.g. by showing where traffic jams were in the city) or further enhance the firms understanding of the user (e.g. by comparing the user's travel patters to different cohorts of users with known preferences the firm may be able to more accurately refine the user's preferences).

We proceed now to analyse the effects on the property rights of each of the ARCO rights with regard to the three different categories of data we have identified.

Right of Access

The right of Access imposes costs on the controllers, obliging them to design and maintain systems and procedures for allowing the data subject to access his/her personal data.

However, controllers are very interested in the accuracy of the data they process, accuracy which in most cases will be only achieved in an efficient way by cooperating with the data subject. It should not be forgotten that, even if the individual cannot be said to own the personal data referred to him, he is still the more convenient provider of it. This cooperation will only be possible if the data subject is provided with some kind of access to the stored personal data, allowing him to browse them in order to identify eventual mistakes.

So, it seems that the conferred right of access is aligned with the controller preferences, in the sense that it is very likely that he would provide it even in the absence of regulation. Moreover, the regulatory requirements are not very exigent at this time, so it is very likely that the access system put up by the controller according to his preferences will meet them.

Regarding the categories of data to which access must be granted, it seems that most, if not all, of them would spontaneously be stored by controllers, with the possible exception of the sources of external data. Once again, there is alignment between controller preferences and the user right.

Problems may arise if the scope of personal data goes beyond what we have called "explicit data", for which the user is the most convenient source for check and eventual rectification. However, this does not necessarily happen with implicit and inferred data. Interpreting the right of Access as extending to these categories would in principle be against catallactic efficiency. Of course, there may be business models in which

controllers wish to provide access to all or some of the items under those categories (for example, to build trust in its relationship with the data subject or to provide visibility of service use), but this should be left to the competitive process.

In sum, the right of Access as it is defined in the current framework has small effect on the catallactic efficiency, in the sense of that its imposition force on the controller an action that he would likely do voluntarily. The only problems could appear if the regulatory scope of personal data was interpreted to include implicit and/or inferred data.

Of course, other ways of determining/ achieving accuracy of data could be devised and used by the firms in the market. For example, firms might prefer to refine the accuracy of data over time through cross referencing of interchanges with the individual, rather than provide a blanket right of access to all data, at any time. If this is the case, the right of Access could have a chilling effect on innovation in the market.

Regarding the right to Data Portability, included in the right of Access, it imposes extra costs on the controller which may be difficult to justify, in principle. However, in the same way as happens with number portability in the telco industry, portability also brings about benefits in that it make cheaper the acquisition of personal data from new data subjects (because data is already in a structured format and clean), this in turn making it easier for these users to switch providers. As data markets mature, the number of entirely "new" customers to a product market will likely decline relative to the number of "switching" customers. So in the longer run, the overall data capture costs of firms would likely reduce as they gain proportionately more switchers than entirely new customers.

Once again, the analysis above holds true provided that the right of Data Portability only reaches to what we have called "explicit data". Otherwise, alternative providers would be profiting from information they did not invest to collect, creating high disincentives for innovation. Fortunately, the text in Article 20 clearly states that

portable data is only that "*which he or she has provided to a controller*", which should not leave much room for interpretation.

Right of Rectification

The analysis of this right is similar to that of the right of Access, for which it is actually complementary, and the same conclusions hold. As in the above, damage to catallactic efficiency would come if the right of Rectification would be extended to implicit or inferred data. In none of these cases seems generally reasonable to allow the user to rectify information for which he is not the source. Precisely because the right of Rectification has no sense for implicit and inferred data, the same extension for the right of Access would also be harming for catallactic efficiency, due to the subsidiary nature of it respect to the right of Rectification.

GDPR modifies the right of Rectification to include the possibility of completing the personal data. Depending on how this right is interpreted, it could have important implications on catallactic efficiency. If the right of completion is assume to be enforceable only for the items defined in the data structure maintained by the controller, it would be very likely aligned with his preferences: a user record is more valuable it has more fields completed.

However, if the right of completion is interpreted as the possibility for the user to add any information he may think missing (but that the controller may find not useful), then it would impose unnecessary costs on the controller and it would be harming for catallactic efficiency.

Right of Cancellation (Erasure)

The Right of Cancellation imposes a hard limitation on the property rights of the controller: the ability of customers to request deletion of data retained about them is something that we believe would be unlikely to happen in the unregulated market and so impinges on the property rights of the firm, reducing catallactic efficiency and social welfare. In this case, it is obvious that there is a conflict between the interest of owner and the right conferred to the data subject: the former will rarely find it profitable to

delete a record from his database, because the fewer records his database has the less valuable it will be, *ceteris paribus*.

The right of Cancellation is limited to a set of scenarios defined in article 17(1) of the GDPR. Of these, two seem to be the more relevant for the catallactic efficiency: (a) and (b).

Scenario (a) empowers the data subject to request the cancellation of "*the personal data that are no longer necessary in relation to the purposes for which they were collected*". This relates to the "shelf life" defined in Article 5 GDPR.

Absent regulation, the firm is constrained by the cost of data storage at the margin. When the marginal cost of storage exceeds the expected marginal benefits it would rationally refine its data storage policy to reduce marginal costs. Whilst data that is required to fulfil the contract between the firm and the individual would still be retained, superfluous data would need to be assessed based on the new storage policy. Article 5 of the GDPR arguably removes the optionality to retain these data whilst it is still cost-effective to retain it, once services are no longer being rendered.

Still, if it remains efficient for firms to retain data obtained from customers, after the customer decides to terminate a service, then firms may try to renew consent for this this data retention. It appears that the shelf life of data can be circumvented through the use of terms and conditions at limited cost. Although this has a temporal limitation for the long run utility of that data as we highlight above.

Scenario (b) however could pose more problems from the perspective of catallactic efficiency, because it grants the data subject the possibility of deleting the concerned personal data after withdrawing his consent.

This provision somehow puts the property in the hands of the data subject, who may devaluate it just but denying consent and asking the erasure of the data. For its part, assured by the initial consent, the firms would have invested resources in storing,

refining and processing the data. This investment is subject to high uncertainty if it can be wiped out just by a future denial of consent.

Scenario (b) leaves open the possibility of arguing "*another legal ground for the processing*" to avoid the erasure in the case that the data subject denies consent. It would be possible to keep the data by showing that "*processing is necessary for the purposes of the legitimate interests pursued by the controller*" (Article 6.1 (f)).

In any case, it is clear that the right of Cancellation, even if not so harming for catallactic efficiency as would seem at first sight, carries with him an huge increase in uncertainty for the investments of the controllers, both in terms of data subject consent and in the interpretation of which may be considered as a "legitimate interest" of the controller.

Of course, nothing of the above precludes the existence of business models built on voluntary contractual agreements granting the possibility of cancellation on even better terms (for example, including the "right to be forgotten"). However, this imposes costs on firms in terms both of resources and of uncertainty. And the only way to assess if these costs are below the alleged profits, for individuals and for firms, is to let them be trialed in the market.

Right of Objection

In general, this right seems to have analogous consequences to the right of Cancelation that has just been analysed. However, its effects are marginally worse because it defines more scenarios in which the stored data may become unemployable by the controller.

Article 22 of The GDPR grants the "*right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her*".

Previous legislation has concerned itself with the use to which data is put, rather than the business decisions made based on that data. The GDPR breaks new ground by

introducing a right for individuals to challenge decisions based solely on automated processes.

Of course, this may reduce the value of the personal data, because it reduces the possibilities of its exploitation (for example, for firms whose business model is based on low cost automated decision making). But the burden is likely heavier on the development and innovation of algorithms to exploit the data, if in the end recourse to a human decision-maker has to be provided.

On the other side, this obligation for data controllers may provide exceptional opportunities to improve data accuracy in cases in which the automated decision is challenged on the basis on the input data (as opposed to the working of the algorithm).

In sum, there seems to be instances in which this recourse could be in the interest of the data controller, but it is not clear that it is always the case. The entrepreneurial process of trial and error is once again the best way to ascertain which business models are more likely to profit from this proposal, and which would not be viable due to the requirement.

5.3 Summary

In order to assess the catallactic efficiency of the ARCO rights, the first step was to stablish who is *de facto* the owner of the personal data. Only after that, would it be possible to assess how property rights are affected.

We showed that for personal data to be owned these data must materialize into some physical medium. Also, that the owner is, perhaps counter-intuitively, generally not the person it concerns, but what the legislation calls the controller (or the processor). In consequence, the property rights affected by the ARCO rights are his.

Our assessment on the effects of ARCO rights on catallactic efficiency may be summarised in the following points:

1) Rights of Access and Rectification are generally aligned with the controller preferences and would be very likely be spontaneously provided by controllers, at least for what we have called explicit personal data.

   Their main effects may be of a dynamic nature, because it precludes innovation in ways of increasing the accuracy of data by forcing all controllers to provide access to users. It may also eliminate a competitive variable.

2) Rights of Cancellation and Objection are harming for catallactic efficiency, because they increase the risks of the investment required for the storage and exploitation of personal data. However, the current framework seems to provide means for avoiding a unilateral decision by the data subject, thus allowing some protection for the assets of the controllers and in turn for catallactic efficiency.

6. Conclusion and policy recommendations

In this paper, we have provided an assessment on how the ARCO Rights of data subjects, granted in the EU Data Protection Directive, affect social welfare. Our analysis has used the standard of catallactic efficiency for this assessment.

Even if this normative is shaped in the form of Rights of the Citizens, even with the qualification of Fundamental Rights, it is relevant to be aware of the possible costs that such granting may impose on society on terms of social welfare. In fact, the granting of rights is not an objective matter, and, for example, the analysed "rights" are not acknowledged in plenty of countries, among them the USA. The granting of rights comes always at a cost, even if it is not directly carried by the holder of the right, because a right for an individual is likely to suppose an obligation to other. Moreover, as Milton Friedman wrote: "*'The role of the economist in discussions of public policy seems to me to be to prescribe what should be done in the light of what can be done, politics aside, and not to predict what is "politically feasible" and then to recommend*

it"[12]. So, we do not think it is out of bounds to analyse in economic terms this issue, even in light of its political connotations.

Catallactic efficiency requires the assessment of how property rights are affected by the policy or regulation under analysis. The more affected they are, the less efficient becomes the market, and the more suffers the social welfare.

For this, it is necessary as a first step to establish who holds property rights for personal data, from an economic point of view. We have shown that counter intuitively the firm or data controller holds the right to property over personal data in all the three relevant categories: explicit, implicit and inferred.

Being so, it is clear the ARCO rights, as they impose limitations on the use which can be made of personal data by their owner, the data controller, reduce catallactic efficiency and social welfare.

To what degree do they reduce it? Our analysis shows that the Rights of Access and Rectification are relatively innocuous for catallactic efficiency, because its provision is of interest for the controller too, at least for explicit personal data. The effects are worse if it is interpreted that both rights are also granted for implicit and inferred data. In this case, cost would increase for the controller, with no apparent profit opportunity.

On the other side, the Rights of Cancellation and Objection could be more harming for social welfare, by giving the data subject the unilateral possibility of hindering the use of personal data concerning them for which the controller has already invested some resources. Fortunately, the current regulation allows some flexibility for controllers to avoid the cancellation/objection of personal data, but still it creates some uncertainty with will surely affect investment and innovation in the market.

[12] Friedman. M. (1953). Comments on Monetary Policy. In *Essays in Positive Economics*, University of Chicago Press, p. 264.

Together with these static effects, dynamic effects (unintended consequences) should also be pointed out. For example, the rights of Access and Rectification reduce the incentives to innovate in procedures for achieving accurate data. The right of Cancellation eliminates possibilities of differentiation for competing in privacy of the personal data. These effects would be more acute should the rights were extended from explicit personal data to implicit and inferred data.

In light of the results of our analysis, the best recommendation would be of course to supress the ARCO rights and thus eliminate any interference of them with the property rights of the controller.

As this option may not seem politically feasible in the EU, and in light of the degree in which each Right seem to affect catallactic efficiency, our (next best) policy recommendation would be the following:

1) Clarify the scope of personal data, so that it is clear that ARCO rights refer only to explicit personal data, that is, the personal data that are explicitly provided by the data subject.
2) Revisit the rights of Cancellation and Objection, leaving this option to the competition between controllers. We anticipate that controllers providing these possibilities to data subjects will find easier to gather personal data than otherwise. But, still, controllers' investments should not be in the hands of data subjects.

References

[1] Acquisti, A. (2010). The Economics of Personal Data and the Economics of Privacy. *The Economics of Personal Data and Privacy: 30 Years after the OECD Privacy Guidelines,* 1 December 2010.

[2] Acquisti, A., Brandimarte, L. & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science* 347, pp. 509-514.

[3] Acquisti, A. & Varian, H. (2005). Conditioning Prices on Purchase History. *Marketing Science* 24 (3), pp. 367-381.

[4] Böhm-Bawerk, E. von (1891). The positive theory of capital. Londres: McMillan & Co (English translation by W.Smart, 1891)

[5] Calzolari, G. & Pavan, A. (2006). On the optimality of privacy in sequential contracting. *Journal of Economic Theory 130*(1), pp. 168–204.

[6] Christensen, L., Colciago, A., Etro, F. & Rafert, G. (2013). The Impact of the Data Protection Regulation in the E.U.

[7] Cordato R.E. (1992). *Welfare Economics and Externalities in an Open-Ended Universe: A Modern Austrian Alternative.* Boston: Kluwer Academic Publishers.

[8] Goldfarb, A. & C. Tucker, C. (2011). Privacy Regulation and Online Advertising. *Management Science* 57(1), pp. 57-71.

[9] Hermalin, B. & Katz, M. (2006). Privacy, Property Rights and Efficiency: The Economics of Privacy as Secrecy. *Quantitative Marketing and Economics* 4 (3), pp. 209-239.

[10] Herrera-González, F. & Blades N. (2016). "Personal Data: Whose data is it? What can we do about it?" *Regulatory Economic Brief 15-04,* Telefónica. Available at https://www.telefonica.com/en/web/about_telefonica/publications/others-publications

[11] Hui, K. & Png, I. (2006). The Economics of Privacy. In T. Hendershott (Ed.): *Economics and Information Systems*, *Handbooks in Information Systems,* vol. 1. Elsevier.

[12] Hoppe, H.H. (1989). *A Theory of Socialism and Capitalism.* Kluwer Academic Publishers..

[13] Hume, D. (1751). An Inquiry Concerning the Principles of Morals: With a Supplement: A Dialogue. New York: Liberal Arts Press.

[14] Kirzner I.M. (1985). The Perils of Regulation: A Market Process Approach. En R.M. Ebeling (1991): Austrian Economics: A Reader. Hillsdale, MI: Hillsdale College Press, p. 618-654.

[15] Larouche R., Peitz M. & Purtova N. (2016). "Consumer privacy in network industries". *CERRE Policy Report* (25th January).

[16] Noam, E. M. (1997). Privacy and self-regulation: Markets for electronic privacy. In U.S. Deptartment of Commerce, *Privacy and Self-Regulation in the Information Age*.

[17] Padilla, J. (2015). Personal Data and Competition: An economic perspective. *Competition Rebooted: Enforcement and Personal Data in Digital Markets*. Brussels, 24 September 2015

[18] Posner R.A. (1981). The economics of privacy. *American Economic Review (Papers and proceedings)*. 71(2), pp. 405-409.

[19] Shy, O. & Stenbacka. R. (2016). Customer Privacy and Competition. *Journal of Economics & Management Strategy*. 25(3), pp. 539–562.

[20] Soria B. & Herrera-Gonzalez, F. (2013). A Quantitative Approach to Include Time and Innovation in Traditional Market Analysis. Presented at *TPCR* 41, 2013.

[21] Stigler, G. J. (1980). An introduction to privacy in economics and politics. *The Journal of Legal Studies 9*(4), 623–44.

[22] Taylor, C. (2004). Consumer Privacy and the Market for Customer Information. *RAND Journal of Economics* 35 (4), pp. 631-650.

[23] Tucker, C. E. (2012). The Economics of Advertising and Privacy. *International Journal of Industrial Organization* 30 (3), pp. 326–329.

[24] Varian, H. R. (1996). Economic Aspects of Personal Privacy. *Technical report,* University of California, Berkeley.