Informing Consent

Giving Control Back to the Data Subject from a Behavioral Economics Perspective

by **Santiago Ramírez López***

Abstract: The development of data privacy legislation in Europe and America has been highly influenced by the idea that individuals must maintain the autonomy to take decisions regarding the general purpose and uses of their personal data; an idea that has been generally instrumentalized with the mechanism of informed consent. Recently, both companies and researchers in the field have criticized this idea, arguing that with the new advances and technological progress, consent has lost importance due to the ubiquity of the data processing and the absence of real participation of the data subjects. This article seeks to take into account both points of view, by recognizing the importance of the autonomy of individuals to determine the destination of their personal data, but also by understanding the practical implications and the impossibilities derived from obtaining an informed consent from data subjects that are generally unfamiliar with the topic. Based on the analyses regarding the difficulties of obtaining an effective and informed consent, this contribution will examine how some of the bias and impasses studied through the discipline of behavioral economics may help us to understand the current problems in relation to the way in which consent is requested and provided by the data subjects. This contribution concludes by proposing alternatives that seek to overcome these biases and impasses with an easier provision of information of the data processing and the implementation of a data management and a value-oriented model, which would benefit the data subjects.

Keywords: Behavioral economics; Data Privacy; Data Protection; General Data Protection Regulation; Informational self-determination; Informed consent

Recommended citation: Santiago Ramírez López, Informing Consent: Giving Control Back to the Data Subject from a Behavioral Economics Perspective, (2018) JIPITEC 35 para 1.

A. Introduction

1 It is safe to say that the notion of controlling the destination of one's personal information has been strongly involved in the development of the data privacy/data protection discipline.[1] The right to informational self-determination, developed in Germany during the 1980's, entails a value that is still applicable in recent history; that individuals should be able to limit the information that can be used from them.[2] The American tradition has long

* LLB (Del Rosario University - Colombia); LLM (University of Hannover / University of Oslo). IT Law Associate Professor (El Bosque University – Colombia).

1 Professor Lee A. Bygrave has a thoughtful definition of the field of data privacy law, and the meeting points and dissimilarities between different terms that compose the field, such as "data protection", "data privacy" and "data security". For conceptual purposes, this work will indistinctively use the terms "data protection" and "data privacy" to address, in the words of professor Bygrave, the regulation of "(...) all or most stages in the processing of certain kinds of data" as well as "(...) the ways in which the data is gathered, registered, stored, exploited and disseminated". See: Bygrave, L. A. (2014). *Data Privacy Law: An International Perspective*. London: Oxford University Press, pp. 1-5.

2 Schwartz, P. (1989). The Computer in German and American Constitutional Law: Towards an American Right of

recognized equivalent values, identifying the right "to be let alone" as a way to promote a non-intrusive information gathering against the media and the emerging technologies,[3] and as a right grounded in the control of the individual to determine what information can be openly communicated.[4]

2 On paper, the European legislation has included several provisions which seem to provide data subjects more control over their information. Indeed, the former Data Protection Directive[5] (from now on the "DPD") and the recently adopted General Data Protection Regulation[6] (from now on the "GDPR"), contain the basis to prevent practices that may constitute an illegitimate processing of data, and dedicate several provisions to the possibility of control of the data subject grounded on informed consent. Nevertheless, the reality of the online scenario has shown the inability of this model to provide control and to protect the data subject's right to privacy.

3 Among experts, there is a debate if whether providing more control to the data subject can be a solution applicable in the real world for the protection of the right to privacy. The critics of a control-oriented approach base their arguments on the practical, conceptual, and moral difficulties of the model,[7] but mainly on the fact that the consent, as the main mechanism of control of the data subject, has so far proved to be impractical and inefficient.[8]

4 A concise reason for the failure of a consent-oriented model is still subject to debate. Some, especially in the private sector, believe that modern society is currently suffering a transition, where the traditional concept of privacy, or privacy as a "social norm," is being dismissed with the excuse of an interconnected world.[9] Although this explanation is convenient for businesses, it also disregards the fact that society has become increasingly more suspicious of how companies are using the data and information provided by users.[10]

5 This article aims to demonstrate that, although the legal concepts of privacy between the predominant Western traditions contain discrepancies mainly in their formation, they are not so different in their outcome, as Western traditions embrace the concept of control of the data subjects as a capital guideline of data protection.

6 This paper will analyze the implications of the field of behavioral economics in the data privacy scenario. Supporting the position of other authors,[11] it will be argued that some of the bias and impasses studied in the field of behavioral economics may help to explain the issues and problems of consent as a way to provide control to the data subject based on a conscientious decision-making scenario.

7 The objective of this analysis is to restore the position of the concept of informed consent as the primary means of control for the data subject, while recognizing that to achieve such informed consent, the data subjects must be provided with more suitable conditions that allow them to overcome the biases and impasses.

8 As a conclusion, this contribution will analyze a proposal for the creation of such a suitable scenario, by implementing alternative ways to provide and manage information and by giving a tangible value to the data from the user's perspective. This proposal is composed of the following components: (i) alternative and user-friendly ways of providing the information required by Article 13 of the GDPR, resorting to existing models, such as Creative Commons; (ii) a data management system that contains unified information of the personal data circulating online of the data subject; and (iii) a model based on the value of the data in benefit of the

Informational Self-Determination. *The American Journal of Comparative Law*, 37, pp. 678-689.

3 Warren, S., & Brandeis, L. (1890, December 15). The Right to Privacy. *The Harvard Law Review*, IV(5).

4 *Ibid.*

5 The European Parliament and the Council of the European Union. Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

6 The European Parliament and the Council of the European Union. Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

7 Allen, A. L. (2000). Privacy-as-Data Control: Conceptual, Practical, and Moral Limits of the Paradigm. *Connecticut Law Review*, 32, 861-875.

8 Koops, B.-J. (2014). The Trouble with European Data Protection Law. *Tilburg Law School Legal Studies Research Paper Series*, 4, p. 3.

9 In 2010 with the rapid increase in the use of social media, Mark Zuckerberg, founder of Facebook, stated that privacy was no longer a "social norm", as social media sharing reflected a change in attitude. See: Johnson, B. (2010, 1 11). *Privacy no Longer a Social Norm, says Facebook Founder.* Retrieved 7 1, 2016, from <https://www.theguardian.com/technology/2010/jan/11/facebook-privacy>.

10 Several polls have shown the rejection of the public in relation to surveillance and data gathering. These polls will be discussed in Section B.II. See: Jourová, V. (2015). *Data Protection Eurobarometer-Factsheet*. European Commission. See also Madden, M., & Rainie, L. (2015, 5 20). *Americans' Attitudes About Privacy, Security and Surveillance*. Retrieved 7 2, 2016, from <http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/>.

11 See footnotes 54 to 56.

data subject, that recognizes the need for awareness of the users in relation to the costs and rewards of the data exchange.

9 The aim of proposing these components is not to anticipate their actual adoption - although their compatibility with the GDPR will be briefly examined - but to explore alternative ways of providing and managing information that, while not a novelty, may have useful implications in the assessment of the behavior of the data subject and in the analysis of future measures that seek to ensure a conscientious decision-making scenario in the data protection field.

10 It will be argued that this model may create awareness and responsibility in overcoming bias and impasses studied in the field of behavioral economics but, at the same time, recognizes the paramount economic and social importance of data processing in the current state of development of the technology industry.

B. Privacy in Western traditions: A story about finding and losing control

I. Privacy as control

11 An exposition of the right to privacy should start recognizing that, as Professor James Q. Whitman states, "the concept of privacy is embarrassingly difficult to define."[12] One of the probable causes for this statement is that the notion of privacy raises different connotations depending on social and legal traditions, mainly the Western traditions of Europe and North America.

12 According to Professor Whitman, the concept of privacy in the European tradition is seen as a right strongly attached to human dignity, which implies the control of information that can be disclosed about an individual.[13] In this context, the enemy of privacy is broadly understood as any person, natural or legal, that in some way acquires information and aims to disclose it. More importantly, the European concept of privacy deeply embraces the ability to control the information.

13 On the other hand, the American conception of privacy entails freedom from the intrusion of states and contains a deeper distrust of public agents.[14] Moreover, the American recognition of privacy, due to European influence, also adopted the control of the information as an important value. Arguably, the main and most influential basis for the modern conception of privacy in the United States originates from Samuel Warren and Louis Brandeis' article *The Right to Privacy.*[15] In this article, Warren and Brandeis embraced the right "to be let alone," as an extension of the inviolability of personality. But with the recognition of the right "to be let alone", Warren and Brandeis consequently embraced the need of control of the subject that creates the information:

> *"The common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others (...) the protection afforded to thoughts, sentiments, and emotions, expressed through the medium of writing or of the arts, so far as it consists in preventing publication, is merely an instance of the enforcement of the more general right of the individual to be let alone."*[16]

14 Professor Whitman notices the big influence that the European tradition and the concept of human dignity had in Warren and Brandeis, by proclaiming the dangers of losing the capacity of control over the personal information.[17]

15 In the course of the twentieth century, the dire consequences of the categorization and profiling performed by the Nazis certainly influenced the social perception of data processing in the years to come. It is considered that the strong protection of privacy in Germany, with the creation of measures such as the right to informational self-determination, has been a reaction to the Nazi and Communist eras.[18]

16 A parallel control-oriented development occurred in the United States in the second half of the twentieth century. As an example, in 1969, the famous Nader Report elaborated to examine the functioning of the Federal Trade Commission in the United States, raised several privacy concerns in relation to data mining. This report already foresees that the increase of mass data processing and the use of social-psychological analysis of potential markets affected the privacy and autonomy of the

12 Whitman, J. Q. (2004). The Two Western Cultures of Privacy: Dignity versus Liberty. *The Yale Law Journal*, 113, p. 1153.

13 *Ibid,* p. 1161.

14 *Ibid,* p. 1018.

15 Krause, H. D., & Marcus, P. (1977-1978). Privacy. *The American Journal of Comparative Law*, XXVI, 377.

16 *Op.cit.* Warren, S.; & Brandeis; L.

17 *Op.cit.* Whitman, J. Q. p. 1167.

18 Cole, D., & Fabbrini, F. (2016). *Reciprocal privacy: Towards a transatlantic agreement.* In V. C. Federico Fabbrini (Ed.), Constitutionalism Across Borders in the Struggle Against Terrorism (pp. 169-189). Cheltenham UK: Edward Elgar, p. 454.

consumers.[19] While recognizing the importance of the user's autonomy over the information, the report warns of the potential of mass processing of data for marketing practices as a form of social control, due to the possibility of creating normative patterns in the users.[20]

II. Privacy as control: Outdated or ignored?

17 The increasing technological developments and the generalized and ubiquitous flow of personal data has led some to identify a change in the social perception of privacy, in support of a more negligent view that benefits an interconnected world. In support of a new and broader concept of privacy, Facebook's CEO and founder, Mark Zuckerberg, stated in 2010 that "(p)eople have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people. That social norm is just something that has evolved over time."[21]

18 Now, it is undeniable that the concept and perception of privacy have dramatically evolved during the last decades. Nevertheless, the fact that in the past there was a broader understanding of the information that was considered important for the users, does not necessarily mean that people have dismissed the possibility and need for control and the importance of privacy and anonymity.

19 A survey carried out by the European Commission in June 2015 on 28.000 EU citizens, showed that 67% percent of the respondents were concerned about not having control over the information they provide on the internet. The survey showed that although 71% percent of the respondents accept that providing information is part of modern life, the majority of the people still feel uncomfortable about the fact that companies use this information to tailor advertisement. It is interesting to notice that, in comparison to the same survey done in 2010, there is not a substantial change in perception.[22]

20 A similar survey carried out in the United States in early 2015 showed an even higher distrust in the activity of online service providers. This survey showed that for more than 93% of adults, it was important to have control over who can get their information, and 90% considered important to have control over the type of information that can be collected. The survey also evidenced that the majority of respondents have little trust that online service providers keep the collected information private and secure, and 55% believe that people should have the ability to use the internet in a completely anonymous way.[23]

21 This information shows the contradiction between the perception and concerns of the public, with the real life application of data processing. A big part of the problem is based on the fact that, as accurately stated by Professor Lilian Edwards, "(...) users care deeply about their privacy but can't be bothered to read privacy policies."[24]

C. Current state of affairs: An unbalance between regulation and social perception

22 The proposal to modify the DPD introduced on January 25 2012 had as one of its main aims, the idea to strengthen the online privacy of the users. As stated by the EU Justice Commissioner Viviane Reding,"(m)y proposals will help build trust in online services because people will be better informed about their rights and in more control of their information."[25] It is interesting to note that the concept of control has been embraced by the European Union when drafting the original proposal for the GDPR. Nevertheless,

19 Hasty, A. (2014-2015). Treating Consumer Data like Oil. *Federal Communications Law Journal*, 67(2), pp. 307, 308.

20 Silbey, S. S. (1984). Who Speaks for the Consumer? Nader's No Access to Law and Best's When Consumers Complain. *American Bar Foundation Research Journal,* 2, p. 177.

21 Matyszczyk, C. (2010, January 10). *Zuckerberg: I know that people don't want privacy*. Retrieved 7 17, 2016, from <http://www.cnet.com/news/zuckerberg-i-know-that-people-dont-want-privacy/>.

22 European Commission. (2015). *Data Protection Eurobarometer-Factsheet.* For empirical investigations about the value of data for consumers, see: Aquisti, A. (2014), The Economics and Behavioral Economics of Privacy. In Lane, J., Stodden, V., Bender, S., Helen Nissenbaum, H., (Eds), *Privacy, Big Data, and the Public Good: Frameworks for Engagement.* Cambridge University Press. p 8 Retrieved 4 7, 2018, from: <http://wpressutexas.net/cs378h/images/b/b3/LaneEtAlPrivacyBigDataAndThePublicGood.pdf#page=55>.

23 *Op.cit.* Madden, M., & Rainie, L.

24 Edwards, L. (2013). *Privacy, Law, Code and Social Networking Sites*. In I. Brown (Ed.), Research Handbook On Governance Of The Internet (pp. 1-35). London: University of Oxford This phenomenon has been called by some authors as the "privacy paradox", in which internet users have concerns about privacy and know about the privacy terms, but they will not read these terms and will still disclose the information. For more information about the privacy paradox, see: Zuiderveen, F.J. (2014). Improving Privacy Protection in the Area of Behavioural Targeting. *University of Amsterdam Digital Academic Repository,* pp 293-296. See also: Monteleone, S. (2015). Addressing the 'Failure' of Informed Consent in Online Data Protection: Learning the Lessons from Behaviour-Aware Regulation. *Syracuse Journal of International Law and Commerce*, 43(1). p. 75.

25 European Commission. (2015). *Data Protection Eurobarometer-Factsheet*. Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses. Brussels: European Commission.

this possibility in practice does not seem to provide enough protection or control.

23 There are several lawful bases for the processing of data according to Article 6 of the GDPR, including legal obligations and the protection of the data subject's interests. Nevertheless, the consent is the main tool to legitimate data processing,[26] and the primary tool for the data subject to exercise any control.

I. Consent in the EU regulations

24 Article 4 (11) of the GDPR, defines that consent "(...) means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".

25 The concept of consent adopted in the GDPR relies on perfectly valid grounds, and contains legitimate aims, in the sense that it should be freely given and informed. Nevertheless, so far, the model of implementation of consent that provides control to the data subject and the tools for this end have been inconvenient and not appropriate for the purpose.

26 It is worth mentioning an interesting experiment that was performed by the Norwegian Consumer Council, where volunteers read the terms of use and privacy policies of the apps of an average Norwegian smartphone. The process of reading the terms of use and privacy policies of 33 apps containing around 250.000 words, lasted more than 24 hours,[27] and led the Norwegian Consumer Council to the obvious conclusion that "mobile apps' terms of use and privacy policies fail to uphold privacy obligations and users' consumer rights."[28]

27 A major part of the problem lays in the outdated nature of the current model of consent. As stated by the privacy advocate Simon Davies, "most consent mechanisms were conceived in the pre-dawn of the Internet age. They were developed at a gentler time in history – a time when it was possible to build a simple flow chart of personal data relationships."[29]

28 However, even if it is accepted that consent, as drafted in the GDPR, is a proper tool for control, other provisions further diminish the autonomy of the data subject. Indeed, Article 6 (4) of the GDPR allows the processing of data for purposes that have not been subject to the consent of the data subject, as long as the controller proves compatibility between the initial and the new purposes. The criteria to determine such compatibility (Article 6 (4) (a-e)) are conspicuously broad, with plenty of space for interpretation.

29 With reason, critics of a consent-based approach point out its lack of suitability as a practical solution.[30] Some of these critics aim to prove that the concept of consent is currently an illusion, as the users give it on a non-negotiable, non-informed, and pressurized basis.[31] In a broader way, some authors believe that the sole concept of control is an illusion, since data subjects constantly and willingly disclose their information.[32]

30 Professor Anita L. Allen for example, stresses the practical difficulties of providing control[33] on the grounds that "control over personal data appears to be neither necessary nor sufficient for states of privacy to obtain",[34] since people that may have control over their information, choose to give up this faculty.

31 The position of the author, shared by other authors in the field,[35] is that the consent is a valuable and important tool for the data subject that should not be easily disposed on the grounds of attaining to reality. On the contrary, the concept of consent should maintain its importance in the data protection field, but its direction and implementation should be reconsidered.

26 Enerstvedt, O. (2015). *Consent as a Basis for the Processing of Personal Data under the European Data Protection Directive: case study on Facebook* (Thesis). Oslo: University of Oslo. p. 1.

27 For more information about the experiment, see: The Norwegian Consumer Council. (2016). *250,000 words of app terms and conditions*. Retrieved 7 17, 2016, from <http://www.nbcnews.com/technology/ftc-says-flashlight-app-left-consumers-dark-2D11702823>.

28 The Norwegian Consumer Council. (2016). *Appfail: Threats to Consumers in Mobile Apps*. Oslo: The Norwegian Consumer Council, p. 4.

29 Davies, S. (n.d.). *Why the Idea of Consent for Data Processing is Becoming Meaningless ad Dangerous.* Retrieved 7 17, 2016, from <http://www.privacysurgeon.org/blog/incision/why-the-idea-of-consent-for-data-processing-is-becoming-meaningless-and-dangerous/>.

30 *Op.cit.* Koops, B.J, p. 3.

31 *Op. cit.* Edwards, L. p. 24.

32 *Op.cit.* Allen, A.L. p. 869.

33 *Ibid.*

34 *Ibid.* p. 867.

35 Staben, J. (2012). *"Consent under pressure and the Right to Informational Self-Determination."* Internet Policy Review, 1(4). See also: *Op.cit.* Zuiderveen, F.J. (2014). pp. 201, 236 and 237.

II. Data protection regime: The unbalance between regulation and social perception

32 The previous sections have made evident different problematic issues. One of these issues is that the concept of control of the data is still an important basis for the right to privacy in Western traditions, both from the academic and the social point of view. On the other hand, the previous sections state that consent, as a mechanism of control included in the GDPR and other legislation, has not contributed to create a better suited and rightly entitled data subject.

33 The disparity shown on the previous sections between the ideal of control and the real practice of data mining and processing is largely a result of outside pressure and economic interests.

34 It is interesting to notice how the efforts of the OECD in the elaboration of the *Guidelines on the Protection of Privacy and Transborder Data Flow*, were primarily driven by economic interests. Indeed, the effort of creating the Guidelines mainly answered to the need of establishing a set of principles that would guard against economic protectionism.[36] The influence of the OECD's instrument has been extensive and can be found in the Safe Harbor Agreement of 2000 between the European Commission and the US Department of Commerce, invalidated by the Court of Justice of the European Union,[37] and in the data privacy laws of several countries outside Europe.[38]

35 This is also true in the context of the European Union with the creation of the former DPD. Indeed, as stated by Professor Lee A. Bygrave, the European Commission, although partly motivated by the protection of human rights, was mainly aiming to eliminate barriers to the realization of the internal market.[39] The purpose of the DPD is ambivalent, as expressed in Article 1, which, at the same time seeks to protect fundamental rights and freedoms of natural persons, whilst prohibiting any restriction in the free flow of personal data.[40]

36 The value of information as a fundamental economic asset is a fact that companies have assimilated for several decades. Therefore, the influence of the private actors in the adoption of the proposal of the GDPR is not surprising. Indeed, the GDPR was one of the most lobbied legislations in Europe,[41] with 3999 amendments only by the Civil Liberties, Justice and Home Affairs Committee.[42]

37 The current American approach to the processing of data has also been subject to different pressures that diminish the control of the data subjects. Besides more direct pressure imposed by the public[43] and private[44] sectors, the American legislation, in scenarios not only limited to data protection, has been greatly influenced by economic elites and organized groups representing economic interests, while the average citizen has little to no influence in the elaboration of public policies. This phenomenon has been called an Economic-Elite Domination.[45]

D. A Behavioral Economics Perspective

38 As it has been analyzed in the previous sections, the idea of control of the data subject is not new, but it has been attached to the right to privacy since the moment that Western doctrines identified the emerging threats in an increasingly more technological world.

39 This article supports the revitalization of the concept of informed consent as an appropriate tool of control of the data subjects. Nevertheless, the analysis of

36 *Op.cit.* Bygrave, L., p. 43.

37 Case C-362/14 Maximillian Schrems v Data Protection Commissioner (2015).

38 *Op.cit.* Bygrave, L. p. 50.

39 *Ibid.* p. 55.

40 *Ibid.* p. 57.

41 European Digital Rights (EDRi). (2016, February 24). *Data Protection Lobbyotomy Part 1: Influencing the Dutch government.* Retrieved 7 17, 2016, <from https://edri.org/data-protection-lobbyotomy-part-1-influencing-the-dutch-government/>.

42 Albrecht, J. P. (2015, January 7). *EU General Data Protection Regulation: State of play and 10 main issues.* Retrieved 7 17, 2016, from <http://www.janalbrecht.eu/fileadmin/material/Dokumente/Data_protection_state_of_play_10_points_010715.pdf>.

43 Due to the attacks on 9/11, the NSA, with the help of legislative measures, created extensive networks of collaboration with telecommunication companies. The Protect America Act of 2007, reinvigorated by the FISA Amendments Act of 2008, gave immunization to private companies that voluntarily cooperated with the US intelligence, culminating in the PRISM program, which managed to create partnerships with Microsoft, Google, Yahoo, Facebook, among several others. See: Laberge, C., 2010. *To What Extent Should National Security Interests Override Privacy in a Post 9/11 World?* Victoria University of Wellington Working Paper, pp. 1-134. See also: Tucci, L., 2013. *Putting a Price on Information: The nascent field of infonomics.* [Online] Available at: <http://searchcio.techtarget.com/opinion/Putting-a-price-on-information-The-nascent-field-of-infonomics>.

44 For more information in relation to the data processing practices of private companies in the post 9/11 legal regime, see the documentary: *Terms and Conditions May Apply*. 2013. [Film] Directed by Cullen Hoback. USA: Hyrax Films.

45 Gilens, M., & Page, B. I. (2014). Testing Theories of American Politics: Elites, Interests Groups, and Average Citizens. *Perspectives on Politics*, 12(3), p. 565.

the informed consent of the previous sections shows that models that may work in theory, very often prove to be unsuccessful in practice. The previous statement does nothing different than recognizing the complexity of the human mind and the effect of such complexity in the individual behavior and social environments.

40 The field of behavioral economics relies on the idea of economy and society as complex phenomena.[46] In this sense, behavioral economics seeks to understand the behavior of individuals and its consequences, grounded on the experimental knowledge of the good or bad choices of people. In other words, it means to reorient the interest of economy from formal theoretical assumptions to psychology and real human actions.[47]

41 A behavioral economics-oriented legal approach explores the actual human behavior in connection to law[48] over purely hypothetical or ideal scenarios. In comparison with a regular legal analysis, the inclusion of the economic factor, as stated by Posner, "(...) tries to explain and predict behavior of participants in and persons regulated by the Law".[49] But also, while the standard model of economics is based on strong assumptions,[50] such as ideal decision-making scenarios, behavioral economics tests these models in real life situations, to find evidence of the actual behavior of people.

42 Indeed, one of the most important differences of the behavioral economics approach in contrast to traditional approaches is that it aims to increase the explanatory power of economy by relying on psychological foundations.[51] This means that while it is possible to rely on certain assumptions, the ultimate test of the theory must prove accurate or congruent with reality.[52] The main reason for this is that the sole idea of implementing a behavioral approach, especially in the legal field, comes from the challenges and contradictions that the experiments have shown in relation to economic assumptions that have been paradigmatic.[53] More importantly,from these experiments, new assumptions have arisen, some of which will be explained in the next sections due to their relevance in the field of data privacy.

43 This article argues that in the current state of affairs, the problematic issues presented in the data protection field, due to the lack of consideration of the data subjects' point of view are arguably creating a favorable scenario for the application of a behavioral economics-oriented analysis that takes into account both psychological and sociological factors. This position has been examined by other authors in the field who have highlighted the importance of the economics of privacy and the behavioral economics from a privacy perspective,[54] grounded on the problematic issues for the data subject due to an asymmetric access to the information.[55] Also, other authors have approach the notion of consent from a behavioral economics perspective,[56] albeit arriving to different proposals to overcome biases and impasses.[57]

I. Bounded rationality

44 The concept of bounded rationality recognizes that people have constraints in their rational capacities, which implies that very often, people use "rules of thumb" to make decisions[58] that rely more on automatic impulses than on conscious thinking.

45 A good explanation of this phenomenon is provided by the Nobel-prize winner, Daniel Kahneman. He distinguishes between two systems of the mind: in System 1, the mind operates automatically with no sense of voluntary control; while in system 2, there is effortful and demanding mental activity. What is interesting is that the effortless impressions of System 1 tend to be the source for the conscious

46 Frantz, R. (2013). Friedrich Hayek's Behavioral Economics in Historical Context. In R. Frantz, & R. Leeson (Eds.), *Hayek and Behavioral Economics* (p. 1.34). Hampshire: Palgrave Macmillan. P. 3.

47 Camerer, C. F., & Loewestein, G. (2004). Behavioral Economics: Past, Present, Future. In C. F. Camerer, G. Loewenstein, & M. Rabinn (Eds.), *Advance in Behavioral Economics* (pp. 1-51). Princeton NJ: Princeton University Press. p. 39.

48 Jolls, C., Sunstein, C. R., & Thaler, R. (1998). Behavioral Approach to Law & Economics. *Stanford Law Review*, 50, p. 1476.

49 Posner, R. A. (n.d.). Values and Consequences: An Introduction to Economic Analysis of Law. University of *Chicago Law School, Program in Law and Economics,* Working Paper 53, p. 2.

50 Cartwright, E. (2011). *Behavioral Economics* (3 ed.). London: Routledge. p. 4.

51 *Op.cit.* Camerer, C. F., & Loewestein, G. p. 3.

52 *Ibid.,* p. 4.

53 Aaken, A. v. (2014). Behavioral International Law and Economics. *Harvard International Law Journal*, 55(2), p. 422.

54 *Op.cit.* Acquisti, A. (2014).

55 Acquisti, A., Grossklags, J. (2007). What Can Behavioral Economics Teach Us About Privacy? In Acquisti, A.; Grossklags, J. (Eds), *Digital Privacy: Theory, Technologies and Practices*. Taylor and Francis Group.

56 *Op.cit.* Zuiderveen, F.J. (2014). pp. 286-298. See also: Zuiderveen, F.J. (2013). Consent to behavioural targeting in European Law: What are the policy implications of insights from behavioural economics. *University of Amsterdam Law School Research Paper No. 2013-43.* Also: *Op.cit.* Monteleone, S. (2015). Addressing the 'Failure' of Informed Consent in Online Data Protection: Learning the Lessons from Behaviour-Aware Regulation. *Syracuse Journal of International Law and Commerce*, 43(1).

57 *Op.cit.* Zuiderveen, F.J. (2014). pp. 299-342.

58 *Op.cit.* Cartwright, E. p. 10.

choices of System 2. Moreover, the choices of System 1 may also arise with a prolonged practice that creates an automatic conduct.[59]

> *"(w)hen all goes smoothly, which is most of the time, System 2 adopts the suggestions of System 1 with little or no modification. You generally believe your impressions and act on your desires, and that is fine—usually (...) When System 1 runs into difficulty, it calls on System 2 to support more detailed and specific processing that may solve the problem of the moment. System 2 is mobilized when a question arises for which System 1 does not offer an answer".*[60]

46 This categorization of decision-making systems has an important influence on the way in which consent is provided online. A vital issue with consent is that, in Kahneman's words, "we can be blind to the obvious, and we are also blind to our blindness".[61]

47 Arguably, ticking boxes of acceptance for the provision of online services on the current state of affairs seems more reflective of System 1 than System 2, and when the data subjects provide consent for countless data processing activities, they do not read such terms or understand their implications.

48 Nevertheless, it should be recognized that this situation of automatic response of online users cannot be exclusively blamed on the data subjects. The current model of data processing and the economic interests behind them provide the proper condition for this problem.

49 The generalized use of cookies gives a good example of a model that, due to its omnipresence, leads to automatic decisions (System 1) of the data subject. According to Article 5(3) of the Directive 2002/58/EC, the user must give his consent to the use of cookies. Although for some authors, the possibility of consenting the use of cookies means a positive change that represents an almost informed opt-in mechanism;[62] the problem arises with the fact that 50.1% of all websites on the internet are currently using some type of cookies, while a big part of these sites are the ones that contribute most of the traffic of the Internet, such as Youtube, Amazon, and Wikipedia, among others.[63] The fact that the majority of websites and the most important and frequently visited sites on the internet require the users to constantly provide their consent, makes the act of taking a responsible and informed decision impractical and costly. Thus, accepting the use of cookies becomes an automatic action of the System 1.

50 It is also worth mentioning that while accepting the use of cookies requires a costly and imperfect consent described above, the legislation allows the data controller to do without consent when the cookies are considered strictly necessary.[64] The fact that the controller may use cookies even without the users' consent, arguably creates a perception of futility in the action of accepting the privacy or cookies policies, further affecting the amount of effort that the data subjects will invest in accepting such terms.

51 The application of a behavioral-oriented perspective in this matter may provide valuable contributions for a different approach. According to the bounded reality concept, "one of the tasks of System 2 is to overcome the impulses of System 1. In other words, System 2 is in charge of self-control".[65] What this means is that, in a situation where there is an automatic impulse of System 1, such as providing consent for the use of cookies, System 2 can have the power to overcome said impulse, and by overcoming an automatic decision of providing consent, the user may take a better-suited decision.

52 Therefore, a mechanism that seeks to ensure the right to privacy of the users should, in its foundation, create tools that encourage conscious and mindful decision-making. The purpose of a measure in this sense is not to create unnecessary burdens for the users or to make online browsing tedious, but to properly inform the users of the nature of the data that it is being processed and the important implications that the activity of data processing may have for them. As will be exposed later in this article, the measures to overcome a bounded reality phenomenon may consist in a better provision of information of the processing and its practical implications for the data subject, as well as in the implementation of a value-oriented model that may encourage the users to be more involved in the data processing activity.

II. Loss aversion

53 Another interesting phenomenon that may be initiated relates to "loss aversion". This concept understands that people, when facing losses in a

59 Kahneman, D. (2011). *Thinking Fast and Slow.* New York: Farrar, Straus and Giroux. pp. 22-23.

60 *Ibid.,* p. 26.

61 *Ibid.*

62 Bond, R. (2012). The EU E-Privacy Directive and Consent to Cookies. *The Business Lawyer*, 68, p. 215.

63 W3Techs. (2016, 7 18). *Usage of Cookies for websites*. Retrieved 7 18, 2016, from <https://w3techs.com/technologies/details/ce-cookies/all/all>.

64 See: Article 5(3), Directive 2002/58/EC. See also: Information Commissioner's Office. (2012). *Guidance on the Rules on use of Cookies and Similar Technologies*.

65 *Op.cit.* Kahneman, D. p. 28.

certain transaction, tend to give more weight or importance to said loss than to the gains that the transactions may bring.[66] This concept is better understood when analyzed together with the "status quo bias", which states that unless there is a good reason to change, people tend to stick to what they already have, even if the alternative seems more promising.[67] People therefore have the tendency to stay on the safe side, by giving a higher value to what may be lost than to the reward or retribution of the transaction.

54 In a general way, it is safe to say that one of the main threats to the right to privacy in the activity of data processing is the ignorance of the losses that the unlimited processing of data entails for the data subject.

55 A control-based model must, therefore, tackle this issue in different ways. As with the phenomenon of bounded reality, the data subject should be informed of the consequences of providing consent for the activity of data processing. Since the loss aversion phenomenon relies on the fact that people give higher value to their "belongings" in a transaction, in order to use this tool to shape behavior, the data subject must be aware both of the losses and the gains of a data transactions.

56 However, by itself, the sole recognition of the losses and gains may not be enough when there is not a real consequence with regard to the person's interests, economic or the like. As explained in relation to the bounded reality, the users must be able to take a mindful decision on the provision of data, not inclined to automatic impulses. This situation leads to the proposal of a mechanism that relies on the attention of the data subjects by directly affecting their interests and also by benefitting them. This can be more easily tackled in a value-oriented model that will be proposed later in this paper.

III. Time inconsistency

57 The phenomenon of time inconsistency shows that people tend to grab immediate rewards at the same time that avoid immediate costs. For example, procrastination comes from the avoidance of immediate costs in performing a task, even when performing this task may have future rewards. Overeating comes from embracing immediate rewards over foreseeable problems, such as becoming overweight. In summary, this phenomenon shows that people tend to prefer present or immediate rewards over future costs, and prefer to avoid present or immediate costs, even if they carry future rewards[68].

58 The activity of acquiring a service on the internet through consent to provide personal data constitutes an immediate reward. The service, provided immediately, outweighs the negative consequences for the users of providing such data; consequences that in most cases are not clear or evident. Moreover, even if the user has the will to provide a responsible decision, the action of reading terms and conditions would be too costly in comparison to the reward.[69]

59 In order to expect responsible behavior from the users in the disposition of data, the information of the data processing must be provided in a less costly way that allows the user to easily identify the different aspects of the activity. More importantly, a less costly solution for the user must also consider a more unified way of data management, which will be exposed as a proposal in this contribution.

IV. Bargaining impasse and self-serving bias

60 Another concept that may find an interesting application is the bargaining impasse and self-serving bias. According to this behavior, there is a tendency of people to identify or to consider something as fair when the outcome represents a benefit for them.[70] Moreover, this tendency shows that people tend to believe that their notion of what it is fair is impartial, so when the other party bargains, this action is considered aggressive and unfair.[71]

61 In general terms, users are kept uninformed or misled of the outcome of a transaction that implies the processing of data.[72] In this sense, the tendency to identify fairness or unfairness in a self-serving

66 For more information about the phenomena of "loss aversion", see: Tversky, A., & Kahneman, D. (1991). Loss Aversion in Riskless Choice: A Reference-Dependent Model. Quaterly Journal of Economics, 106(4), p 1038.

67 Thaler, R. H. (2015). *The Making of Behavioral Economics: Misbehaving.* New York: W.W. Norton & Company, Inc. pp. 131 and 154.

68 O'Donoghue, T., & Rabin, M. (2004). Doing it Now or Later. In C. F. Camerer, G. Loewenstein, & M. Rabin (Eds.), *Advance in Behavioral Economics* (pp. 223-251). Princeton NJ: Princeton University Press. p 224.

69 *Op.cit.* Zuiderveen, F.J. (2014). p. 299.

70 Babcock, L., & Loewenstein, G. (2004). Explaining Bargaining Impasse: The Role of Self-Serving Biases. In C. F. Camerer, G. Loewenstein, & M. Rabin (Eds.), *Advance in Behavioral Economics* (pp. 326-343). Princeton NJ: Princeton University Press. p 236.

71 *Op.cit.*, O'Donoghue, T., & Rabin, M. pp 326-327.

72 Kerber W. (2016). Digital Markets, Data, and Privacy: Competition Law, Consumer Law, and Data Protection. *Join Discussion Paper Series in Economics*, p. 11.

bias requires knowledge of the value, as well as of the type, degree of sensibility, and final use of the data; however, this is all information that is not always easily accessible. In other words, for the users to determine the fairness of a bargain, they should be aware of both the reward (the provision of a service) and the costs and implications of this reward.

62 This bias or impasse relies on the stringent viewpoint of people when facing a bargain. It also implies that under a better-suited model, this jealous conduct that people have over their belongings may be used to create a more responsible and conscious data subject. In any case, the possibility of control that this phenomenon brings, not only demands a better provision of information, but also requires a real possibility of bargaining from the data subject, which further supports a value-oriented model and a unified system of data management.

V. Confirmatory bias

63 The confirmatory bias implies that individuals tend to positively rate new information that is consistent with their initial opinion, and negatively rate the information that contradicts said initial opinion.[73] The confirmatory bias denotes the misinterpretation of ambiguous information, as evidence that confirms an initial opinion.[74]

64 More importantly, it has been determined that an agent with a confirmatory bias habitually believes in hypotheses that are wrong, which at the same time, represents an opportunity for an observer to take advantage.[75] Very often, private and public agents use the confirmatory bias to shape or strengthen wrong ideas.

65 Thus, although people show concerns for their privacy and crave better control over their information, the extent to which people know how their privacy is being protected tends to be more limited, and it is often subject to intentionally provoked biases. Indeed, even while there is a general distrust of the public in the activities of data processing, the perception of people in this regard is frequently inaccurate.[76]

66 There are no few examples of corporate power and media coverage diminishing privacy scandals, or supporting wrong ideas by implying that technology companies are strongly protecting the privacy of their users.

67 An example of the influence of technology companies' perpetuation of inaccurate ideas about data processing is the dispute between Apple and the FBI. Apple denied the requirement made by the FBI to create a backdoor and, therefore, unlock an iPhone belonging to an alleged terrorist, arguing the defense of civil liberties and the protection of people's privacy.[77] While this refusal of Apple has been praised as a strong protection of users' privacy,[78] it should not be forgotten that it has also served as an effective advertisement for the iPhone's security and encryption.[79] Moreover, Apple's strong stand for security and privacy has signified great economic benefits for the company by providing successful access to markets like China, where people are becoming increasingly concerned about state surveillance.[80]

68 Other technology companies have crafted their media image in similar ways. Facebook's Kathy H. Chan stated: "our philosophy is that people own their information and control who they share it with".[81] In the same way, Google's Eric Schmidt stated: "(m)y interpretation is that there is concern that we might be misusing this data and we're not telling you [about it], which I assure you is not the case. We're very committed to telling you what we do".[82]

69 In this context, is it is ironic that according to the NSA, these three companies were aware and gave access to people's data in the activities of mass surveillance performed within the PRISM program.[83]

73 *Op.cit.,* Cartwright, E. p 177.

74 Rabin, M., & Schrag, J. L. (1999). First Impressions Matter: A Model of Confirmatory Bias. Quarterly Journal of Economics, p 38.

75 *Ibid.*

76 *Op.cit.,* Staben, J.

77 Kharpal, A. (2016, March 29). *Apple vs FBI: All you need to know.* Retrieved 7 18, 2016, from <http://www.cnbc.com/2016/03/29/apple-vs-fbi-all-you-need-to-know.html>.

78 MacGregor, S. (2016, February 18). *Apple isn't protecting a shooter's iPhone data – they're defending digital privacy.* Retrieved 7 18, 2016, from <https://www.theguardian.com/commentisfree/2016/feb/18/san-bernardino-shooter-iphone-apple-tim-cook-fbi-decrypt-unlock>.

79 Grossman, L. (2016, March 29). *Here's Who Really Lost in the Apple-FBI Showdown.* Retrieved 7 18, 2016, from <http://time.com/4275033/apple-fbi-iphone-case/>.

80 Benner, K. (2016, February 20). *Apple Sees Value in Its Stand to Protect Security.* Retrieved 7 18, 2016, from <http://www.nytimes.com/2016/02/21/technology/apple-sees-value-in-privacy-vow.html?_r=2>.

81 Chan, K. H. (2009, February 16). *On Facebook, People Own and Control Their Information.* Retrieved 7 18, 2016, from <https://www.facebook.com/notes/facebook/on-facebook-people-own-and-control-their-information/54434097130>.

82 Grabham, D. (2013, May 24). *Google: "we have a clear incentive to protect your privacy.* Retrieved 7 18, 2016, <from http://www.techradar.com/news/internet/google-we-have-a-clear-incentive-to-protect-your-privacy--1154069>.

83 Kleinman, A. (2016, March 20). *NSA: Tech Companies Knew*

70 Moreover, other factors that create confirmatory bias in the data processing activity have been recognized. For example, Julian Staben argues that consumers are used to having protective warranties and cancellation policies in commercial purchases, which lead them to assume that the same protection applies to privacy policies.[84]

71 A confirmatory bias may be used in a positive way in terms of empowerment of data subjects, in the sense that under appropriate conditions and with enough information, the data subjects may be more critical in their perception of the commercialization of data and, therefore, be more careful in the disposition of such data.

E. Making a responsible data subject: Applying behavioral economics to create informed consent

72 The models of behavioral economics previously mentioned are crafted after experimental results that have evidenced that certain economic models, based on ideal behavior, do not correspond to reality. Instead, the experiments have discovered that the actions of people can be more counterintuitive. In the application of these models to the data privacy field, potential conclusions and proposals arise.

73 The following sections will analyze a proposal of a model of information provision and data management from the users' perspective, composed of three components. The first component will analyze alternative methods of providing user-friendly information online, mainly using the example of Creative Commons. Since the GPDR currently suggests the provision of information in combination with standardized icons and in a concise way, it is expected that this component will form an already important aspect of the regulation.

74 The second and third components will explore alternatives of data management and data disposal that rely more heavily on the intervention and awareness of the data subjects, thus helping to overcome some of the bias and impasses of behavioral economics. Indeed, the second component considers the difficulties of having an informed data subject in a fragmentary scenario and, therefore envisages the need for creating a system that contains unified information of the data circulating online of the users. Finally, the third component, considers the need for a more involved and aware user in relation to the costs and rewards of the data exchange, thus it will analyze the possibility of implementing a model based on the value of the data to the benefit of the data subject.

75 Although these last two components are only hypothetical and are not expected to be adopted literally by any jurisdiction, this article will argue that they are not contradictory with the GDPR and therefore, do not rely on the infeasible scenario of abolishing existing data protection laws.[85] Consequently, even if the following sections envisage a proposal based on more control of the data subject, it is not the intention of this article to stop relying on the protectionist and arguably paternalistic provisions of the GDPR in relation to consent,[86] but to explore alternative ways of providing and managing information that, while not a novelty, may have relevant implications in the assessment of the behavior of the data subject and in the analysis of future measures to ensure a conscientious decision-making scenario in the data protection field.

I. Providing data processing information

76 Arguably, one of the main issues in the current model of data processing is the assumption that actual informed consent can be expected from the data subjects, in the way in which the information of the data processing is being provided.

77 According to the GDPR, there is a substantial amount of information that must be provided to the data subjects. Mainly, Article 13 contains such a requirement, which includes the identity of the controller, purpose of the processing, and the identity of the recipients, among others. Article 14 includes the information that must be provided if the data has not been obtained directly from the data subject.

78 The purpose of providing this information and obtaining consent is to properly inform the users on the basis of the principles of transparency (Article 5(1)(a) and Article 12(1) of the GDPR) and to put people in control of their personal data.[87] This condition is therefore laudable in light of this work, but the way in which this information has so far been provided is not user-friendly and, mainly, does not comply with its purpose.

About Prism the Whole Time. Retrieved 7 18, 2016, from <http://www.huffingtonpost.com/2014/03/20/nsa-prism-tech-companies_n_4999378.html>.

84 *Op.cit.,* Staben, J.

85 *Op.cit.* Zuiderveen, F.J. (2014). p. 299.

86 *Ibid.* pp. 242-247.

87 *Op.cit.* Zuiderveen, F.J. (2014) p. 201.

79 Providing information for the data processing does not have to be this costly, however. In this line of thought, an example of providing legal information to a broad public is the Human Readable layer of the Creative Commons license. This tool was crafted with the understanding that most creators of content may not have a legal background, and therefore, require more suitable information. Indeed, Creative Commons explains the purpose of the Human Readable in the following way:

> *(...) since most creators, educators, and scientists are not in fact lawyers, we also make the licenses available in a format that normal people can read — the Commons Deed (also known as the "***human readable***" version of the license).*[88]

80 Creative Commons managed to summarize difficult copyright concepts in user-friendly images. Concepts of copyright rules, such as the right to communicate, distribute or reproduce a work, the attribution of moral rights, and other legal concepts, are contained in figures that do not require specialized knowledge.

81 In terms of privacy, some efforts have been made to provide better information to the users. In Germany, Wikimarx[89] highlights the most critical or important provisions in the terms of service, although it requires diligent and concerned users.

82 It is certainly valuable to recognize that, in most cases, the receivers of legal information online, especially in the field of data privacy, are not lawyers. In this sense, it is self-evident that relying on difficult and long privacy policies to prove the informed consent of a user is not an accurate way to create control. However, the way in which the information is provided should be reconsidered, without necessarily modifying the set of information required. As the information required in Article 13 of the GPDR aims to create an entitled and informed data subject, this contribution does not challenge the importance of this information, but the costly and ineffective way in which it is delivered by the service providers.

83 It is important to notice that the GPDR already contemplates the provision of information in a user-friendly way. Recital 60 of the GDPR states that "(...) information may be provided in combination with standardized icons in order to give in an easily visible, intelligible and clearly legible manner, a meaningful overview of the intended processing". In addition, Article 13 states that the controllers must take appropriate measures to provide any information in a "(...) concise, transparent, intelligible and easily accessible form, using clear and plain language (...)". Therefore, the adoption of a user-friendly method of provision of information, such as the one used in Creative Commons, is an interesting approach that does not contradict the GDPR but, on the contrary, may help develop it.

84 On the other hand, it is relevant to consider that, as stated by Wolfgang Kerber, data subjects are intentionally kept uninformed about the data processing by service providers.[90] Therefore, it may be assumed that a simplified way of providing information without existing standardized icons or a stringent regulation - while attractive for service providers due to its simplicity - has the potential to diminish the information received by the data subjects and create confusion. In other words, a simplified way of providing information of the data processing may be used by service providers arbitrarily to create ignorance and confusion among data subjects.

85 Thus, while the use of icons in a similar way to Creative Commons may be attractive for service providers due to its simplicity, some legislation would be expected to specify the recommendation of the GDPR, but mainly to establish the guidelines of these icons and ensure that their use is indeed standardized, understandable, and effective to transmit the information required by the GDPR.

II. Unifying the information

86 The practical problems that arise from the huge amount of information, which the users are supposed to read should not be undermined. Even if the privacy terms and conditions of a service are provided in a user-friendly way, the disparities with the terms and conditions of other services, and the difficulties of understanding their differences will arguably not encourage users to take more responsible decisions. In this sense, the possibility of creating a unified system for data management may be a viable proposal to encourage control.

87 The idea of creating a unified system for the management of data is not a novelty. The FTC Commissioner Julie Brill created an interesting initiative called "Reclaim your Name," by which she encouraged data brokers to create a consumer-friendly online service that would give access to the information that data brokers have of them.[91]

88 Creative Commons. (n.d.). *Licensing Considerations: What our licenses do.* Retrieved 7 18, 2016, from <https://creativecommons.org/share-your-work/licensing-considerations//>.

89 Wikimarx. (n.d.). *Wikimarx.* Retrieved 9 8, 2016, from <http://www.wikimarx.de/>.

90 *Op.cit.* Kerber W. p. 11.

91 Brill, J. (2013, October 28). *Data Industry Must Step Up to Protect Consumer Privacy.* Retrieved 7 18, 2016, from <http://adage.com/article/guest-columnists/data-industry-step-protect-consumer-privacy/244971/>.

88 Moreover, Data Management Platforms (DMP) have emerged during the last years, offered by companies like Oracle or Adobe.[92] These platforms store data which, after a process of analysis, provide useful information for businesses, mainly profiles for targeted online ads.[93] The DMPs, although mainly used for companies in the monetization of data, can be used as models of data management for data subjects.

89 In this line of thought, startups like Datacoup have started the path of creating a value-oriented platform and marketplace for the users to sell their data for a fixed amount per month.[94] The company Citizen Me provides a similar service for consumers with the possibility of earning cash or donating data to charity.[95] Although the payment of a small amount of money in exchange for the data of all the social networks of the users is still far from an actual management and marketplace of data, the approximation to control of the data subject is certainly present, as it provides the possibility not only to manage unified sets of information but also to make this information a valuable good.

90 This contribution argues that a unified system for data management does not contradict the GDPR; on the contrary, a unified system may help develop and create an effective right of data portability (Article 20 of the GDPR). This right, that obligates controllers when requested to provide the personal data of the data subject in a structured, commonly used and machine-readable format can be, in practice, effectively exercised with the use of a unified data management system.

91 A system of this type is already attractive for companies like Adobe and Oracle and may be profitable for others. Therefore, the presence and control of the supervisory authorities would be required, especially during the examination of a data protection impact assessment (Article 35 of the GDPR). Certainly, it is expected that the eventual adoption of a unified data management system would require said assessment, where service providers must conduct an evaluation of the risks and impacts of the data processing, based on the use of what may be considered a new technology,[96] and the fact that it may imply large-scale data processing (Article 35 (b)). Also, and due to the high volume of data that a measure of this nature requires, there may be a risk of illegal and systematic profiling or monitoring of data holders, thus a tightly regulated scenario would be desirable.

92 Eventually, a better-controlled scenario of a unified data management model may include other possibilities of control different than the sole possibility of receiving and selling data. For example, in order to build trust in the user, a unified system should create standard privacy policies oriented to data processors and controllers. Eventually, a unified system may provide the user with tracking tools that identify the current controllers and processors of the data, or mechanisms that allow one to choose the frequency and type of intrusiveness of advertisement.

III. A value-oriented model of data management

93 There is a generalized idea that the most common services provided online are free of charge. In reality, these services are profiting from the data gathered from the data subjects.[97] Indeed, corporations are increasingly treating information as a commodity,[98] as there is a commercial exchange of value, where the internet service provider offers a service in exchange for data and attention,[99] and where these providers gain economic benefits based on the detailed knowledge of the data subject's preferences and behavior.[100]

94 The approximation of data as a valuable good is mostly discussed in the enterprise scenario. So far, most analyses on this matter focus on considering the benefits for big companies in the technological market to treat data as a "natural resource".[101] In this

92 More information about the Data Management Platforms of Oracle and Adobe can be found in the following links: <https://www.oracle.com/marketingcloud/products/data-management-platform/index.html>. <http://www.adobe.com/uk/marketing-cloud/data-management-platform.html>.

93 Marshall, J. (2014, January 15). *WTF is a data management platform*? Retrieved 7 18, 2016, from <http://digiday.com/platforms/what-is-a-dmp-data-management-platform/>.

94 For more information about Datacoup, see: <https://datacoup.com/>.

95 For more information about Citizen Me, see: <http://www.citizenme.com/>.

96 Article 35 of the GDPR states that "(w)here a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks".

97 *Op.cit.*, Kerber, W. p. 9.

98 Victor, J. M. (2013). The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy. *The Yale Law Journal*, p .517.

99 *Op.cit.*, Hasty, A. pp. 297, 307, 313.

100 *Op.cit.*, Acquisti, A. p. 6.

101 Deutscher, M. (2013, March 11). *IBM's CEO Says Big Data is Like Oil, Enterprises Need Help Extracting the Value*. Retrieved 7

scenario, issues, such as antitrust have been analyzed when the value of the data and the intensive and disproportionate mining of said data is comparable to charging high prices.[102] Moreover, the emergence of big data has allowed companies like Google, Apple, and Amazon to offer bank-like services, all possible due to the enormous databases and a so far unattainable understanding of the consumer's behavior.[103]

95 This enterprise-oriented approach, which conspicuously recognizes the economic importance of data, not only disregards the possibility of individuals to dispose of their data but, on the contrary, aims to provide tools to monetize the data of the users for the exclusive benefit of companies.[104] This contribution argues that this enterprise-oriented approach not only contradicts the social perception of the data subjects but almost completely excludes the users from real economic benefits.

96 Some authors in the legal field dismiss the debate of personal data as a tradable good on a market, especially under the argument of inalienability.[105] Although this approach is certainly valuable for debate and future regulations, the following analysis will not enter this discussion, but will seek to propose measures that better reflect the current economic approach and the general understanding of data as a valuable good.

97 In any case, legal requirements for a value-oriented model should not be inferior to the requirements for data processing in the current data protection regulations, specifically the GDPR. In other words, the recognition of data as a valuable good from a data subject perspective, should not substantially affect the development of the right to privacy or the extent of the informed consent; on the contrary, it should be focused on strengthening them in a way that creates awareness and seeks to overcome the biases and impasses explained by behavioral economics.

18, 2016, from <http://siliconangle.com/blog/2013/03/11/ibms-ceo-says-big-data-is-like-oil-enterprises-need-help-extracting-the-value>.

102 Cooper, J. C. (2013). Privacy and Antitrust: Underpants Gnomes, The First Amendment, and Subjectivity. *George Mason University Law and Economics Research Paper Series*. Vol. 20, 20(4), p. 1131.

103 Packin, N. G., & Lev-Aretz, Y. (2016). Big Data and Social Netbanks: Are you ready to replace your bank? Houston Law Review, 53(5), p. 1216.

104 Twogood, C. (2014, November 19). 5 *Essential Steps Toward Monetizing Your Data*. Retrieved 7 18, 2016, from <http://www.forbes.com/sites/teradata/2014/11/19/5-essential-steps-toward-monetizing-your-data/#3c8786973b85>.

105 *Op.cit.* Zuiderveen, F.J. (2014) p. 252.

1. What do we get by providing value?

98 There are several advantages in the approach of providing value to the data to the benefit of the data subjects. From a competition point of view, the value-oriented approach provides better tools for controlling the activity of data processing.[106] Indeed, Andrew Hasting notices that "a value approach may be more efficient in providing proves of deceptive practices where the agencies would be able to compare the value of the service in comparison with the 'value' of the data provided in exchange, furtherly analyzing an unfair unbalance".[107] In other words, assigning value to the data arguably creates a more objective basis to identify the abusive market behavior of technology companies.

99 In the same way, the value approach is clearly market-oriented, thus it can have beneficial situations for consumers. Companies will be encouraged to provide better and more competitive services; contrary to the current scenario, where users download products and use services without necessarily considering their quality.

100 But more importantly for the behavioral-oriented approach of this work is the awareness that the value-oriented approach may create in the data subjects. It is undeniable that for most users, there is a lack of understanding of the flow of personal data and the ways in which this flow can be controlled[108]. This phenomenon has been mainly grounded on the lack of awareness of legislation and the acquaintance of the private and public actors, but has, so far, not taken into consideration the user's perspective and actions.

101 The behavioral economics situations previously analyzed benefit from a value-oriented approach. The phenomena of bounded reality and time inconsistency, where data subjects accept privacy limitations in an automated way and expect an immediate reward, and the issue of "loss aversion," where users give more weight to the losses and, therefore, stick to their possessions, are all strongly connected. Indeed, tackling these issues as a whole may be done by relying on the awareness of the value of the data and the possibility of disposing of it, which makes the users mindful of the loss that implies a transaction, and leads them to give more weight to the loss of data than to the reward.[109]

102 In the same way, the loss aversion derives from a more protective use of the self-serving bias. The bias of considering something fair when the outcome

106 *Op.cit.*, Kerber, W. p. 16.

107 *Op.cit.*, Hasty, A. p. 318.

108 *Ibid.* p. 302.

109 *Op.cit,* Tversky, A., & Kahneman, D. p. 1038.

represents a benefit for the person,[110] requires, also, an awareness of the value of the data, and the possibility of disposing of it. Furthermore, the bargaining impasse, where users believe in the fairness of their position in a transaction, certainly requires the possibility of having something to be bargained.

2. Value vs. Property

103 Several theoretical approaches have tried to change the perspective of the data protection model to orient it toward a right to property of the data subject.[111] Indeed, Professor Lessig states that "(t)he laws of property are one such regime. If individuals can be given the rights to control their data, or more precisely, if those who would use data had first to secure the right to use it, then a negotiation could occur over whether, and how much, data should be used".[112]

104 It is interesting to note that critics of this model are based on the dangers of allowing consumers to treat their data as commodities, without being properly informed and having information disparities with the processors.[113] The current state of technological developments, with the acquaintance of legislative rules, already did the job of putting the data subjects in this situation, with or without their knowledge. Although implementing a right to property of the data seems to bring control to the data subject, the whole concept of property lays on nebulousness and theoretical difficulties marked by endless conceptual disputes (is property an interest or a dominion of a thing?).[114]

105 The classification of the type of data that may be subject to property may also present different problems. Indeed, several authors, especially in the medical field, have acknowledged the importance of certain types of data to be part of comprehensive databases for public health and safety.[115] The conceptual issues of propertize data would require a thorough classification, which may provide weak protection for certain types of data or too strong protection for other.

106 Also, the recognition of the data subject as the owner of the data may not be completely effective. As stated by Professor Barbara J. Evans, the recognition of property does not necessarily imply legal property protection, as "(l)aw recognizes that there are many situations where consensual transactions cannot be relied on as a way of ordering an owner's relations with the larger community."[116]

107 Moreover, the model of property of data, for some writers, requires the implementation of a highly regulated market,[117] which requires, at the same time, a better suited but currently inexistent online context. Issues on the like of territoriality make a model based on property impractical and hard to implement, due to the fact that, despite certain and significant convergences, legal disparities on national laws in relation to outsourcing, data mining, or information security[118] make a global implementation of policies very difficult.

F. Conclusion

108 This work has shown that the people's perception in relation to data privacy seems to maintain an ideal of control and self-determination. Nevertheless, there is resistance from maintaining a control-oriented approach since the informed consent, the most important tool for this matter, has so far proved to be ineffective in practice.

109 This situation, greatly influenced by the lobby and economic objectives of both public actors and businesses, arguably rests on the lack of consideration of other scenarios and perspectives. The proposal of this contribution is to consider some of the alternative perspectives, which may provide mechanisms that empower the data subjects.

110 The field of behavioral economics, which takes into account psychological considerations, can be a valuable tool for this purpose. More importantly, a change to a behavioral-oriented perspective has as its main objective, to shape a desired behavior on the users, in the sense of creating a truly responsible data subject that can take informed decisions over the data. This work supports the idea that a more user-friendly way to provide information can be a strong mechanism to empower the data subjects, and that initiatives such as a Creative Commons, offer interesting examples.

110 *Op.cit.,* Babcock, L., & Loewenstein, G. p. 326.

111 *Op.cit.* Kerber W. pp. 14-16.

112 Lessig, L. (1998). The Architecture of Privacy (Draft 2). Taipei: Taiwan Net 98's Conference. pp 17.

113 *Op.cit.,* Victor, J. M. p. 518.

114 *Ibid.*

115 Evans, B. J. (2011). Much Ado About Data Ownership. Harvard Journal of Law and Technology, 25(1), p. 88.

116 *Ibid.*

117 *Op.cit.*, Victor, J. M. p. 519.

118 Gunasekara, G. (2006). The "final" privacy frontier? Regulating trans-border data flows. *International Journal of Law and Information Technology*, 15(3), p. 375.

111 On the other hand, a model that allows unified data management and provides a tangible value to the data should encourage the data subject to consciously choose the purpose of such data. For this to happen, the data subject must be fully aware of the type of data, the purpose of the processing, and the retribution received for the processing.

112 The proposal of this work, although specifically focused on creating tools of control, does not aim to create a property right on the data subjects, considering that this measure, in itself, may not be enough. In other words, the approach of this proposal seeks to be practical, relying on the need of control of the data subjects, based on the privacy values that drive the data protection field, and the fact that the data acquired the characteristics of a valuable commodity.

113 In any case, the previous contribution should be understood as a proposal to change the direction in which the activities of data processing have been so far oriented. The new direction that the current online scenario demands must be oriented to the benefit of data subjects and recognizing the actual conduct and behavior of the users of the internet.