Alma Mater Studiorum – Università di Bologna

DOTTORATO DI RICERCA IN

European Doctorate in Law and Economics

Ciclo 28°

Settore Concorsuale di afferenza: 12/A1

Settore Scientifico disciplinare: IUS/01 (diritto privato)

TITOLO TESI

Privacy Tradeoffs in Information Technology Law

Presentata da: **Ignacio Nicolas Cofone**

Coordinatore Dottorato

Prof. dr. Luigi Alberto Franzoni

_____

Relatore

Prof. dr. Klaus Heine

_____

Esame finale anno 2015

!

Privacy Tradeoffs in Information Technology Law

Privacy afwegingen op het gebied van informatietechnologie wetgeving

Proefschrift ter verkrijging van de graad van doctor aan de
Erasmus Universiteit Rotterdam op gezag van
de rector magnificus
Prof.dr. H.A.P. Pols
en volgens besluit van het College voor Promoties

De openbare verdediging zal plaatsvinden op
dinsdag 8 december 2015 om 12.00 uur
door

Ignacio Nicolás Cofone
geboren te Buenos Aires, Argentinië

Erasmus University Rotterdam

Erasmus

!

Promotiecommissie

!

Promotor: Prof.dr. K. Heine

!

Overige leden: Mr. C. van Noortwijk
Dr. S.E. Weishaar
Prof.dr. F. Weber

Co-promotor: Dr. A.M.I.B. Vandenberghe

!

!

!

This thesis was written as part of the European Doctorate in Law and Economics programme

A collaboration between

Table of Contents

List of Abbreviations

A29WP	Working Party on the Protection of Individuals with regards to the Processing of Personal Data (Article 29 Working Party)
AEPD	*Agencia Española de Protección de Datos* (Spanish Data Protection Authority)
CJEU	Court of Justice of the European Union
Cookie	Hypertext Transfer Protocol Cookie
DNT	Do-not-track
DPL	Data Protection Law
EC	European Commission
ECHR	European Court of Human Rights
ECJ	European Court of Justice
EP	European Parliament
EU	European Union
FTC	United States Federal Trade Commission
GDRP	Proposal for a Regulation on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Regulation Proposal)
HTTP	Hypertext Transfer Protocol
ICO	United Kingdom Information Commissioner's Office
IP	Internet Protocol
MS	Member State of the European Union
OPTA	*Onafhankelijke Post en Telecommunicatie Autoriteit* (Netherlands Independent Post and Telecommunications Authority)

PECR	Privacy and Electronic Communications Regulations of the United Kingdom
PET	Privacy-enhancing Technology
TFEU	Treaty on the Functioning of the European Union
UK	United Kingdom
US	United States of America
USSC	United States Supreme Court

Tables and Figures

Tables

Figures

1.!Introduction

1.1.! Motivation and scope

A text (text *A*) states that one should "please be aware that if your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party through your use of voice recognition." Another text (text *B*) states that "any sounds... above the level of a very low whisper, would be picked up by it, moreover, as long as he remained within the field of vision which the metal plaque commanded, he could be seen as well as heard. There was of course no way of knowing whether you were being watched at any given moment." There are several differences between text *A* and text *B*, such as the dramatic tone and superior pen of the latter. Text *B*, in fact, seems like a dramatic exaggeration of text *A*, phrasing a story that involves the object described in it. It turns out, however, that (as readers of Orwell will have anticipated) text *B* is an extract from *1984*, while text *A* is an extract from a *Samsung Smart TV* privacy policy.

The aim of this comparison which shows the similarity between the texts is not to generate paranoia or to encourage dystopian analogies, but to illustrate the motivation for this analysis: a concern for how technological changes modify how we deal with personal information, the risks that such modifications imply for privacy, and the need for the law to be responsive to those changes.

The central risk that a reduction in privacy due to these technologies represents stems from the argument that, when being surveilled either by the State or by their peers, people may be deterred from any choice that drifts away from social expectations.[1] A lack of privacy results in this way in a reduction in dissent and in a chilling effect on the scope of peoples' actions.[2] In those situations, people express themselves guardedly, impairing the social benefits of free

[1] See Lilian Mitrou, "The Impact of Communications Data Retention on

[2] See Christopher Slobogin, "Transaction Surveillance by the Government," *Mississippi Law Journal* 75 (2005): 139; Daniel Solove, "The First Amendment as Criminal Procedure," *NYU Law Review* 82 (2007): 112.

communication.[3] As a consequence, a society faces a reduction in the scope of viewpoints,[4] and people face a reduction of their civil liberties, particularly regarding freedom of expression.[5] Human rights treaties seem to have responded to this societal concern. Article 8 of the European Convention on Human Rights and article 8 of the Charter of Fundamental Rights of the European Union protect privacy as a fundamental right,[6] and the Treaty on the Functioning of the European Union (TFEU) in its article 16 protects privacy and recognizes data protection as a fundamental right, providing a basis for action.

On the other hand, in the same way that societies value privacy, they value other goods, and they often face a tradeoff between them.[7] In particular, an increment in privacy protection seems to reduce the amount of available information. There are significant social benefits from increasing the amount of available information, since information has public good characteristics.[8] A larger amount of information publicly available in the market generates more trade, faster scientific discoveries

---

[3] See Richard Posner, "Privacy, Surveillance, and Law," *The University of Chicago Law Review* 75, no. 1 (2008): 245. (arguing further that free communications are essential to constitute a space to form ideas.)

[4] See Daniel Solove, "'I've Got Nothing to Hide'and Other Misunderstandings of Privacy," *San Diego Law Review* 44 (2007): 745.

[5] See Robert Goodin and Frank Jackson, "Freedom from Fear," *Philosophy & Public Affairs* 35 (2007): 249; Neil Richards, "The Dangers of Surveillance," *Harvard Law Review* 126, no. 1 (2013): 1934; Yoan Hermstruwer and Stephan Dickert, "Tearing the Veil of Privacy Law: An Experiment on Chilling Effects and the Right to Be Forgotten," Preprints of the Max Planck Institute for Collective Goods (Bonn, 2013); Jonathan Zittrain, *The Future of the Internet. And How to Stop It* (New Haven: Yale University Press, 2008).
Regarding the importance of dissent, see Cass Sunstein, *Why Societies Need Dissent* (Cambridge, Mass.: Harvard University Press, 2003).

[6] The e-Privacy Directive explicitly roots data protection to the right to privacy in its Recital 24, by establishing that computers or other devices used by data subjects to access the internet belong to the sphere of privacy of those data subjects.

[7] See Amitai Etzioni, *The Limits of Privacy* (New York: Basic Books, 2008). Chapter 1.

[8] This statement is developed in section 2.3.1 below.

and a more substantial democratic empowerment.[9] This is done, namely, by linking those who need a certain good with those who offer it, by increasing available datasets for scientific discoveries, and by providing more communication channels to inform oneself and to express one's opinions, respectively.[10] Both the risks and the benefits of information flow are larger now than they were before; big data (the exponential increment in the possibilities to collect, store and disseminate data[11]) turns the balance between them to be both more difficult and more important.[12] Some have even hyperbolically talked about new technologies possibly leading to the end of asymmetric information.[13]

As this tension between the benefits of protecting privacy and the benefits of increasing information illustrates, privacy is largely about tradeoffs. For data subjects,[14] these are tradeoffs between their privacy and the use of products that require the release of information for their use; for policymakers, these are tradeoffs between protecting the right to privacy and protecting the right to access information. Tradeoffs, in turn, are the realm of economics, and in this sense privacy is to a large extent an economic problem—even when it does not have a simple monetary interpretation and agents are not always aware of the tradeoffs that they are making. Economic theory can therefore shed some light on how these tradeoffs function, and on what are the optimal choices within them.

---

[9] See Jerry Kang, "Information Privacy in Cyberspace Transactions," *Stanford Law Review* 50, no. 4 (1998): 1193. (emphasizing the availability of relevant information, increased economic efficiency, and improved security.)

[10] See Ibid.

[11] See Lokke Moerel, *Big Data Protection. How to Make the Draft EU Regulation on Data Protection Future Proof* (Tilburg: Tilburg University Press, 2014). See also Yochai Benkler, *The Wealth of Networks: How Social Production Transforms Markets and Freedom* (New Haven: Yale University Press, 2006).

[12] See Robert Sloan and Richard Warner, "Big Data and the 'New' Privacy Tradeoff," Chicago-Kent College of Law Research Paper 13-33, 2013. See also Robert Sloan and Richard Warner, *Unauthorized Access: The Crisis in Online Privacy and Security* (Boca Raton: CRC Press, 2013).

[13] See Alex Tabarrok and Tyler Cowen, "The End of Asymmetric Information," *Cato Unbound*, April 6, 2015.

[14] This is the term used by European DPL for people whom data that is being collected or processed is about. The British Data Protection Act, for example, states that "data subject means an individual who is the subject of personal data."

The analysis evaluates data protection law (DPL) from a law & economics perspective; this branch of law has evolved to cope with new interactions involving privacy between private parties, also called the horizontal right to privacy, and in this way exists in the intersection between privacy law and information technology law.[15] Chapters 2 and 3 perform this economic evaluation of DPL at an abstract level, and chapters 4 and 5 do so regarding two policy debates that can be called the most prominent regarding horizontal privacy in the last years in Europe: the right to be forgotten and online tracking.

The scope of the analysis is, therefore, the way in which European DPL deals with new interactions pertaining the right to privacy among private parties.[16] Within that scope, it seeks to make the existing tradeoffs more visible in order to allow for a more informed balance between privacy and other countervailing rights. In order to do so, it uses property rights theory in a framework of rational choice to explain the recent developments of DPL from an economic perspective; this methodology presents the advantage of making the costs and benefits of choices

---

[15] DPL is, to some extent, the branch of law that deals with the issue of privacy in the context of information technology. This differentiates it from other branches of law, where two caveats can be made. Firstly, data subjects are, in some sense, consumers, but that is not a full description given that not all interactions that pertain them are set in a consumer relationship; to the extent that the internet is not reducible to electronic commerce, data subjects are not reducible to consumers. The analysis, therefore, is not about consumer law. Secondly, the internet can be separated in its infrastructure and its content, and two related but separate branches of law—telecommunications law and information technology law, deal with those two respectively. For this reason, the analysis is not about telecommunications law.

[16] The issue of government surveillance, and the problems of privacy between private parties and their governments (or other governments) that it introduces, is another relevant problem. Although in many ways linked to the issue addressed in this analysis, the issue of surveillance has several specific elements that justifies its individual study, and although many of the conclusions of this analysis are applicable to it, I leave the scope of this for further study. For example, a relevant issue of surveillance is the determination of what is legal, and how to make States to comply with the law. See, for instance, Bruce Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* (New York: Norton & Company, 2015); James Rule, *Privacy in Peril: How We Are Sacrificing a Fundamental Right in Exchange for Security and Convenience* (New York: Oxford University Press, 2007).

regarding privacy identifiable. In this way, it builds on the traditional law & economics literature on privacy to account for more recent technological and legal developments.

The abovementioned concern for how technological changes modified how we deal with personal information has largely exceeded the intellectual spheres of academia and journalism. In Rotterdam, the *Museum Boijmans Van Beuningen* hosted in 2014 the exhibition "*Dataism*", exploring the role of the individual in the scenario of big data. One of its central pieces, "Mirror Piece",[17] captures the faces of its visitors and analyses their biometric features in order to identify them publicly, together with their (sometimes controversial) findable characteristics.

Orwell's *1984*, *Samsung TV* and the *Dataism* exhibition are examples of the same issue. That a television or a work of art would need a privacy policy is a feature that we are not used to as a society. With traditional televisions and works of art, the observer remains passive while interacting with them: only a consumer of images and sounds. With some new objects, however—particularly those that operate through the internet—,[18] the observer is a subject who engages the device actively, and inputs something about himself.[19]

In interacting with these devices, subjects face an increment in the costs of protecting their personal information, while those who want to acquire such information face reduced costs of obtaining it. For example, if upon walking into a store, an employee recorded our name, another followed us noting how much time we spend in each aisle, and another

[17] "Mirror Piece" (2010), by Marnix de Nijs.

[18] The internet can be defined as an open network of devices that communicate among each other using the same protocol.

[19] Some people consider that the subject who uses this devices turns into an object, inverting the relationship between them. See, for example, Stanley Benn, "Privacy, Freedom and Respect for Persons," in *Nomos XIII: Privacy*, ed. Ronald Pennock and John Chapman, vol. 8 (New York: Atherton Press, 1971). This idea is also behind the saying, popular in in Silicon Valley, that if a service seems free then one is the product. Conversely, one could also say that the subject who interacts with objects instead of being a mere spectator can be seen as less of an object (and more of a subject) than the subject who does not.

noted which items we bought, we would easily notice.[20] Surveillance in physical spaces is more evident than in cyberspace.[21] In addition, in order to perform this real-world surveillance, the store would have to spend a significant amount of money, while in cyberspace it can do so with an algorithm at a much lower cost. Thus, surveillance in physical spaces is more expensive than in cyberspace.[22]

While the internet's technological characteristics, to some extent, offer privacy with no precedents,[23] they also produce a loss of privacy with no precedents: our browsing patterns can be known by internet server providers and by content providers, as well as by third parties, with a wide array of technological developments such as cookies and fingerprinting. In addition, people anywhere in the world can learn personal information about us with just a few searches.

In particular, in the last years two relevant modifications took place that affect the incentives in privacy exchanges. The first relates to the phenomenon of big data, which makes surveillance significantly easier both for public and private parties.[24] The second relates to a decentralization in how the internet's content is generated. Both of them imply that the context in which privacy interactions take place has

---

[20] See Lawrence Lessig, "The Law of the Horse: What Cyberlaw Might Teach," *Harvard Law Review* 113, no. 2 (1999): 501. The USSC has utilized this idea by rejecting the analogy between surveillance by a GPS and visual surveillance between neighbors. See *US v. Maynard*, 615 F.3d 544 (DC Cir. 2010).

[21] See Ian Brown and Douwe Korff, "Technology Development and Its Effect on Privacy and Law Enforcement. Report for the UK Information Commissioner's Office" (Wilmslow: Information Commissioner's Office, 2004).

[22] See Lawrence Lessig, "The Law of the Horse: What Cyberlaw Might Teach," *Harvard Law Review* 113, no. 2 (1999): 501.

[23] In social interactions people know our face, gender, general physical characteristics, and can have a good guess at our weight and age. On the internet, on the other hand, we can access information that we would be embarrassed to look for in a library, or shop for any item that we would not like to be seen buying in a shopping mall. On the internet, fellow shoppers do not know our particular identity and potential members of our community do not know which information we are accessing.

[24] See Julie Cohen, "What Privacy Is For," *Harvard Law Review* 126 (2013): 1904; James Grimmelmann, "Big Data's Other Privacy Problem," University of Maryland Working Paper 14-7 (College Park, 2014). See also Omer Tene and Jules Polonetsky, "Privacy In The Age Of Big Data: A Time For Big Decision," *Stanford Law Review Online* 64 (2012): 63.

changed due to technology and that, consequently, its optimal scope of protection might have changed as well.

Regarding the first change, we have faced a modification in the accessibility of information with advances in search algorithms. These algorithms reduce the costs of information retrieval. Their development has been coupled with an increment in the durability of information, produced by increasing storage capacities and a significant reduction in storage costs.[25] As a result, peoples' lives can be increasingly recorded and stored in an accessible way. This makes personal information more vulnerable to third parties—both public and private—increasing the repercussions of people's actions and reducing their well-being by producing discomfort, together with potentially creating chilling effects that can interfere with personal autonomy.[26] Surveys, high profile litigations and policy debates show the high levels of concern that people have about their informational privacy in this context.[27]

Additionally, there has been a modification in the process of content-creation, which has become decentralized through technologies such as cloud computing and social networking, and the globalization of data flows. The internet evolved from the previous linear model in which there was a strong separation between content-creators and content-providers to a system which is characterized by global collaborations—sometimes called peer-to-peer technology or web 2.0.[28] An iconic moment of this trend was the apparition of Napster in the 1990s, which was the first company to mass-market the idea that files needed not to be obtained from their traditional suppliers, but they could be obtained from other users'

---

[25] The cost of storing a gigabyte of data dropped to about 1/100 of its value from 2000 to 2010. See Lilian Mitrou and Maria Karyda, "EU's Data Protection Reform and the Right to Be Forgotten: A Legal Response to a Technological Challenge?," in *Proceedings of the Fifth International Conference of Information Law and Ethics* (Corfu, 2012), 29.

[26] See Paul Schwartz, "Privacy and Democracy in Cyberspace," *Vanderbilt Law Review* 52 (1999): 1607.

[27] For a review of different surveys reaching this conclusion, see Jeff Sovern, "Opting In, Opting Out, or No Options at All: The Fight for Control of Personal Information," *Washington Law Review* 74 (1999): 1033.

[28] See Lawrence Lessig, *Code 2.0* (New York: Basic Books, 2006).

computers via a system called peer-to-peer.[29] The same mechanism was taken directly by millions of websites, such as YouTube, Wikipedia, Digg and SSRN, and more abstractly by the concept of blogs and social networks. It has also been taken by a wide array of products, such as the television and work of art used previously as examples. This mechanic of content creation, as it will be explained later on, is linked with the incentives for the generation of information.[30]

Most new technologies carry with them the creation of new risks, and one could argue that it is a feature of responsive legal systems to address the externalities implied in those risks accordingly. For the case of privacy, these technologies reduce the transaction costs of collecting, storing and disseminating information. This reduction of transaction costs had been done before by the automatic photo camera which motivated the famous article by Warren and Brandeis,[31] and was done to a more profound level by the internet. The internet forced us to rethink existing legal concepts and institutions[32] and, unlike photo cameras, the internet's architecture does not remain the same over time. This has led scholars to consider that the main risks of losing privacy come not from the State, as they traditionally did, but from other private parties.[33]

These technological changes have made privacy law more prominent in the last years.[34] In Europe, they have motivated the Data

---

[29] This phenomenon has already motivated commentaries assessing its effects in copyright law, and evaluating modifications for it. See, for example, Daniel Benoliel, "Copyright Distributive Injustice," *Yale Journal of Law & Technology* 10 (2007): 45; Niels Schaumann, "Copyright Infringement and Peer-to-Peer Technology," *William Mitchell Law Review* 28, no. 3 (2002): 1001; Raymond Ku, "The Creative Destruction of Copyright: Napster and the New Economics of Digital Technology," *University of Chicago Law Review* 69, no. 1 (2002): 263.

[30] This idea is developed in chapter 2.

[31] See Samuel Warren and Louis Brandeis, "The Right to Privacy," *Harvard Law Review* 4, no. 5 (1890): 193.

[32] See Andrej Savin, *Research Handbook on EU Internet Law* (Cheltenham: Edward Elgar, 2014). Preface.

[33] See Amitai Etzioni, *The Limits of Privacy* (New York: Basic Books, 2008). Chapter 1.

[34] See Alessandro Acquisti, Leslie John, and George Loewenstein, "What Is Privacy Worth?," *Journal of Legal Studies* 42, no. 2 (2013): 249.

Protection Directive,[35] the e-Privacy Directive,[36] and the Electronic Communications Framework Directive,[37] which together form the EU data protection framework.[38] The EU data protection framework is considered by some to be a leading paradigm in data protection,[39] having been followed by more than 30 countries that issued similar laws since its establishment.[40] These changes have also changed the legal consequences which are derived from existing legislation.[41] In Germany, for example, the Federal Constitutional Court has protected privacy with the argument that the potential storage of personal information can lead to the aforementioned conforming behavior.[42]

---

[35] Directive 1995/46/EC.
[36] Directive 2002/58/EC.
[37] Directive 2009/136/EC.
[38] The EC has based its competence to issue these directives on the single market provision of article 114 TFEU, referring also to articles 49 and 56 of the treaty (free movement of goods and services provisions). In *Docmorris* and *Gambelli*, the ECJ has accepted the use of article 114 TFEU as a basis of competence for regulating the internet. See John Dickie, *Producers and Consumers in EU E-Commerce Law* (Portland: Hart Publishing, 2005). Chapter 1. See also *Deutscher Apothekerverband eV v. DocMorris NV and Jacques Waterval*, ECJ C-322/01 (2003); *Piergiorgio Gambelli and Others*, ECJ C-243/01 (2003).
[39] See Paul Schwartz, "The EU-US Privacy Collision: A Turn to Institutions and Procedures," *Harvard Law Review* 126 (2013): 1966; Neil Robinson et al., "Review of EU Data Protection Directive. Report for the UK Information Commissioner's Office" (London, 2009).
[40] See Anu Bradford, "The Brussels Effect," *Northwestern University Law Review* 107, no. 1 (2012): 1. This is largely driven by the prohibition to companies in the EU to send data to companies in countries outside the union without guarantees that such data will receive an equivalent protection as it would have in the EU. See article 25 of the Data Protection Directive.
[41] In the US, for example, the Supreme Court has overturned a federal conviction on the basis that it rested on proof gathered by a GPS device installed in the defendant's car, and such method violated his fourth amendment guarantee to be free of unreasonable search and seizure. The USSC, in this way, uses to the fourth amendment to protect the right to privacy in the context of the US constitution, which does not have a disposition that protects it directly. See *US v. Antoine Jones*, 132 S. Ct. 945 (2012). See also Susan Brenner, "The Fourth Amendment in an Era of Ubiquitous Technology," *Mississippi Law Journal* 75 (2005): 1.
[42] See Hans Peter Bull, *Informationelle Selbstbestimmung. Vision Oder Illusion? Datenschutz Im Spannungsverhältnis von Freiheit Und Sicherheit* (Tubingen: Mohr Siebeck, 2011); Michael Ronellenfitsch, "Bull, Hans Peter, Informationelle Selbstbestimmung-Vision Oder Illusion? Datenschutz Im Spannungsverhältnis von Freiheit Und Sicherheit," *Die Verwaltung: Zeitschrift Für Verwaltungsrecht Und Verwaltungswissenschaften* 44, no. 4 (2011): 601.

The EU data protection framework, still, was established before many of these changes took place, particularly the phenomenon of big data and the de-centralized content creation scheme referred to before.[43] Motivated by them, the European Commission (EC) issued a communication to the European Parliament (EP) in 2010 stating that, maintaining the general principles of the Data Protection Directive,[44] new regulations are needed to address the impact of new technologies and to enhance the protection of personal data.[45] This led to the General Data Regulation Proposal (GDRP),[46] which confirms these concerns stating in its recital 5 that "rapid technological developments and globalization have brought new challenges for the protection of personal data" and in its recital 6 that "these developments require building a strong and more coherent data protection framework in the Union."[47]

Hereon, the remaining part of this introduction briefly reviews the history of the concept of privacy as it permeated into the law in order to see how the right of horizontal privacy emerged, together with the different conceptions of the right available in the literature after this historical evolution. It then defines which of these will be used for the analysis that follows; it argues that a functional concept, seeing privacy as an exclusion right of our personal information, can encompass most aspects of the reviewed concepts for the topic of this analysis and provide more tractable implications. This functional concept also allows for an economic analysis, which follows in the subsequent chapters.

---

[43] See Lilian Mitrou and Maria Karyda, "EU's Data Protection Reform and the Right to Be Forgotten: A Legal Response to a Technological Challenge?," in *Proceedings of the Fifth International Conference of Information Law and Ethics* (Corfu, 2012), 29.

[44] See Directive 95/46/EC.

[45] See European Commission, "A Comprehensive Approach on Personal Data Protection in the European Union," *Communication from the Commission to the European Parliament, the Council, The Economic and Social Committee and the Committee on the Regions*, November 2010.

[46] See European Commission, *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free movement of Such Data* (January 25, 2012).

[47] GDRP, recitals 5 and 6.

1.2.! Background: A Brief History of Privacy

1.2.1.! Early stages: privacy as a sphere of action

DPL emerges from the interrelation of a phenomenon that is very old and one that is new: the concept of privacy and the development of a mechanism to ensure privacy with new technologies. Having evaluated the latter, it seems fitting for an informed approach to the topic to briefly review the former.

The distinction of what is public and what is private has existed since the beginnings of modern legal thought.[48] Before that, in ancient legal-political thought, the concepts of public and private were intertwined, and law was considered to exist to make men virtuous.[49] Even after such distinction, privacy was seen as a guarantee opposable only to the State (a vertical right). It was only later, when privacy moved from a political concept to a social concept, that two changes occurred: the horizontal right to privacy appeared, allowing privacy to be a right opposable to other private parties, and informational privacy appeared, expanding privacy from a sphere of liberty of action to a sphere of liberty of thought.

The engine of the initial lack of a distinction between the private and the public is that, in Aristotelian thought, and arguably until Kelsen, law and morality share the same object of study. In a passage at the beginning of *Nicomanean Ethics*, for instance, Aristotle states that politics is about the study of happiness, and about making citizens both happy and obedient to the law, in a context where happiness is intrinsically linked with virtue.[50] Later in the book, he states that law must direct the young into a temperate and firm lifestyle.[51] In *Politics*, he states that the law guides citizens' behavior towards a certain idea of perfection that is

[48] See Jürgen Habermas, *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society* (Cambridge, Mass.: MIT Press, 1991).
[49] See Aristotle, "Politics," n.d. III.9 1280b11.
[50] See Aristotle, "Nicomanean Ethics," n.d. I.13, 1102a7-9.
[51] See Ibid. X.9 1179b34-35.

determined by it, and for such reason legislators must know about virtues and vices.[52]

As with other constructs of modern legal thought, an embryonic version of the distinction between the private and the public is proposed by the Sophists. The idea was originally proposed by Lycophron, who argues that the reason why the political community (*polis*) exists is to guarantee the enforcement of the rights that men have among each other.[53] Aristotle's idea, however, predominated, and continued virtually unopposed through ancient and medieval thought.[54]

This line of thought was set in a context where individuals did not see themselves as completely separate from their family and their community; they lived closely together and spent little time alone to develop thoughts and activities that could arise privacy interests.[55] Speculatively, one could say that there was no need to spend resources in protecting privacy in a context where information about one was inevitably known by one's close community, and for outsiders of the community accessing that information was very expensive.[56]

Aristotle's idea perpetuated into modern paternalistic thought,[57] which traditionally formulates an analogy between a ruler and a father and argues that, as a father, the State should watch over its citizens to ensure their happiness.[58] Paternalism, later on, was linked to the concept

---

[52] See Aristotle, "Politics," n.d. III.9 1280b3-5.
[53] See Robert George, *Making Men Moral* (New York: Oxford University Press, 1993). 21. See also Aristotle, "Politics," n.d. iii.5 1280b.
[54] See Robert George, *Making Men Moral* (New York: Oxford University Press, 1993). Most prominently, this idea was taken by Aquinas. See Thomas Aquinas, *Summa Theologiae*, 1917. I-II q.91 a1.
[55] Gini Graham Scott, *Mind Your Own Business: The Battle for Personal Privacy* (Cambridge, Mass.: Perseus Books, 1995).
[56] Technology, as it was seen, reduces this cost of accessing information for outsiders.
[57] See generally Santiago Legarre, "The Historical Origins of the Police Power," *University of Pennsylvania Journal of Constitutional Law* 9 (2006): 745.
[58] See Robert Filmer, *Patriarcha*, 1680.

of police power:[59] the State's legitimacy to engage in an imposition or preservation of order that leads to the aforementioned happiness.[60]

This concept of police power that was used to justify State interventions, in turn, was taken by liberal political theorists as what is public. This allowed them to formulate an opposed concept of what is private.[61]

By formulating the harm principle, Mill introduced the idea that the distinction between the public and the private sphere is the delimitation of the scope in which the State can legitimately interfere.[62] In the public realm, the State can punish its citizens for their deeds because it is the realm in which they can hurt others, and consequently social responsibilities emerge. In the private realm, on the other hand, acts are self-regarding, or they involve others only when their undeceived consent is involved—and the State's interest in such acts can only be indirect.[63]

This idea was translated into law with the Hart-Devlin debate. In 1957, a specialized committee recommended the British Parliament to remove criminal sanctions for homosexuality stating that "there must remain a realm of private morality and immorality which is, in brief and crude terms, not the law's business"[64]. It posed that a conduct is of public concern only if it can damage by itself the legitimate interest of other non-consenting parties.[65]

---

[59] See Emmerich de Vattel, *Le Droit de Gens*, 1758.
[60] See Ibid. See also Santiago Legarre, "The Historical Origins of the Police Power," *University of Pennsylvania Journal of Constitutional Law* 9 (2006): 745.
[61] Locke, in this line, defines even before Vattel what is private as the opposition to what is political. This interpretation of police power as what is public can also be found in Smith, who enumerated it as one of the objects of jurisprudence relating to the duties of the administration, and in Blackstone, who rejects the idea of a ruler as a father to distinguish between the existence of public and private spheres. See John Locke, *Two Treatises of Government*, 1689; Adam Smith, *Lectures on Jurisprudence*, 1764; William Blackstone, *Commentaries on the Laws of England*, 1769.
[62] See John Stuart Mill, *On Liberty*, 1859.
[63] See Ibid. 12, 13, 74-75.
[64] John Wolfenden, "Report of the Committee on Homosexual Offences and Prostitution" (London, 1957). Paragraph 61.
[65] See Robert George, *Making Men Moral* (New York: Oxford University Press, 1993). 51.

Thus far, privacy was not about the tension between individual rights and the collective interest, but about the limits of collective interest when no rights are involved.[66] The report provoked one of the main debates in modern jurisprudence, between Devlin[67] and Hart,[68] which established the idea that the State cannot interfere with private acts.[69] This debate and the piece of legislation that motivated it launched the contemporary critique against the State's intervention in conducts that have no victims,[70] and to that extent it established a vertical right to privacy.

This definition of the scope of the State's regulation is equivalent to the economic concept of externalities, which traces back to the methodology chosen for this analysis. In a more individualistic society than Aristotle's, with communications between private parties that with some investment could remain as such, and where individuals did not self-identify with the community, there was a desire to keep the State away from those issues that did not affect the welfare of others.

1.2.2.! The horizontal right to (informational) privacy

This idea of privacy was transformed by a more modern account that parted from the classic liberal distinction between the public and the private.[71] For this view, the individual is not only threatened by the State

---

[66] See Ibid. 19-47

[67] See Patrick Devlin, *The Enforcement of Morals: Maccabaean Lecture in Jurisprudence of the British Academy* (New York: Oxford University Press, 1959). See also Ronald Dworkin, "Lord Devlin and the Enforcement of Morals," *Yale Law Journal* 75, no. 6 (1966): 986.

[68] See Herbert Hart, "Immorality and Treason," *Listener*, July 30, 1959. Reprinted in Herbert Hart, "Immorality and Treason," in *The Philosophy of Law*, ed. Ronald Dworkin (New York: Oxford University Press, 1977). See also Herbert Hart, *Law, Liberty, and Morality* (Stanford: Stanford University Press, 1963).

[69] See Robert George, *Making Men Moral* (New York: Oxford University Press, 1993). 48. See also Simon Lee, *Law and Morals* (New York: Oxford University Press, 1986); Basil Mitchell, *Law, Morality and Religion in a Secular Society* (New York: Oxford University Press, 1968).

[70] See Thomas Grey, *The Legal Enforcement of Morality* (New York: Alfred A. Knopf, 1983).

[71] In the modern libertarian tradition of political thought privacy is one of the basic freedoms all individuals possess, and its foundation depends on the theory of value of liberties adopted within the tradition.

but also by social context and social expectations. Therefore, the public/private distinction turns insufficient, and the meaning of what is private becomes what is personal.[72]

The policy debate on postal secrecy, contemporary to the Hart-Devlin debate, reflects this change in the concept of privacy. In colonial times, people had no guarantee that government authorities would not read their letters. This led them to develop codes to encrypt correspondence, engaging in self-protection.[73] Since letters were either simply placed inside an envelope or closed with a wax seal that was not costly to open, postal offices had no way to credibly commit to the confidentiality of communications. This encryption-based self-protection mechanism was socially expensive.[74]

As from the nineteenth century, post offices started to seriously attempt to protect the secrecy of communications.[75] However, the main protection for the privacy of correspondence was not the laws that were issued in this regard, but the invention of adhesive envelopes at the mid-nineteenth century, replacing wax-sealed envelopes.[76] These gave people the opportunity to self-protect at lower costs. At the same time, since adhesive envelopes were more difficult to open without destroying the envelope itself, it gave postal offices a way to signal to the recipient of the letter that secrecy was respected. The technological change allowed for the

---

[72] See Nancy Rosenblum, *Another Liberalism: Romanticism and the Reconstruction of Liberal Thought* (Cambridge, Mass.: Harvard University Press, 1987). 59. See also Will Kymlicka, *Contemporary Political Philosophy* (New York: Oxford University Press, 2001). 394.

[73] See Robert Smith, *Ben Franklin's Web Site: Privacy and Curiosity from Plymouth Rock to the Internet* (Washington, DC: Sheridan Books, 2000). See also Susan Brenner, "The Fourth Amendment in an Era of Ubiquitous Technology," *Mississippi Law Journal* 75 (2005): 1.

[74] An analogy can be made with PETs within DPL, in which data subjects engage in self-protection similarly to people who encrypted their letters, engaging in costs that could be saved if protection was in place.

[75] See Robert Smith, *Ben Franklin's Web Site: Privacy and Curiosity from Plymouth Rock to the Internet* (Washington, DC: Sheridan Books, 2000).

[76] See Ibid.

implementation of the social idea that communications between private parties should be private.[77]

Arendt has explained, in this line of thought, that "modern privacy to its most relevant functions, to shelter the intimate, was discovered as the opposite not of the political sphere but of the social."[78] In ancient times, privacy was not a value: it meant the lack of one's involvement in the public sphere.[79] Modernity and individualism, however, turned privacy into a value, first in the political sphere (against the State) and then in the social sphere (between private parties).[80]

This view implied a break between the public/private distinction and the government/citizens distinction that was inherent in it. Privacy moved to be defined as the opposition between what is personal and what is social.[81] In this way, a horizontal right to privacy appeared, where privacy claims are not only opposable to the government to prevent its intervention when one is not harming others, but also to fellow citizens.

The horizontal right to privacy, moreover, was not only about what is confidential anymore. An eighteenth-century citizen of a western country was familiar with the concepts of secrecy and confidentiality, and would have agreed on the statements that some things are better not

---

[77] After the sealed envelope was invented, the USSC, for example, recognized the confidentiality of sealed mail based on the 4th amendment, which is the same amendment it uses now to protect privacy. In this way it ensured privacy of communications. See *Ex Parte Jackson*, 96 US 727 (1877). British courts did the same, even when this liability rule for confidential communications was not directly linked with the right to privacy. See *Prince Albert v. Strange*, 2 De G, & Sm 652 (1859). See also Roger Toulson and Charles Phipps, *Confidentiality* (London: Sweet & Maxwell, 2007); William Cornish, David Llewelyn, and Tanya Aplin, *Intellectual Property: Patents, Copyright, Trade Marks and Allied Rights* (London: Sweet & Maxwell, 2013). Chapter 8.

[78] Hannah Arendt, *The Human Condition* (New York: Anchor, 1959). 38. See also Stanley Benn and Gerald Gaus, *Public and Private in Social Life* (Kent: Croom Helm, 1983).

[79] Not being involved in the public sphere was, in ancient times and particularly in Greece, not suited for citizens but for slaves and barbarians, who were not considered to be complete because they lacked the public involvement as a realm of human development. See Hannah Arendt, *The Human Condition* (New York: Anchor, 1959).

[80] See Ibid.

[81] See Will Kymlicka, *Contemporary Political Philosophy* (New York: Oxford University Press, 2001). 388.

disclosed, but he could have had difficulties agreeing with classifying non-confidential information as private.[82] Larger societies with interactions that can have a higher level of anonymity allow for this more robust idea of privacy.

This horizontal view of privacy is central for data protection. For example, the right to be forgotten and the online tracking regulations, which are analyzed below, would not be a topic of discussion under a vertical conception of privacy. Moreover, most of the central features of DPL in general would not exist under a vertical conception of privacy, since the problematic of privacy upon new technologies would be reduced to the issue of governmental surveillance.

In this way, this horizontal aspect of privacy shapes information technology law. A purely vertical reading of privacy would restrict it, in this domain, to the limits of surveillance and the question of the extent to which the State can spy on its citizens—for security purposes or otherwise. A horizontal reading of privacy extends it to the relationship between the individual and other private parties, opening a variety of issues such as the extent to which personal information exchanges between a company and a consumer are legitimate, of which are the rights of consumers in such context, and of the scope of consent when information is automatically gathered.

At a more general level, this view of privacy is central for informational privacy, also outside the scope of DPL. While decisional privacy (as in the right to abortion or the right to have consenting adult relationships of any kind) remains mainly opposed to governmental power, it is an essential characteristic of the right to privacy as a sphere of personal information that it can be opposed both to the government and to our peers. The following concepts are a reflection of this horizontal idea of privacy.

---

[82] See Neil Richards and Daniel Solove, "Privacy's Other Path: Recovering the Law of Confidentiality," *Georgetown Law Journal* 96 (2007): 124; Daniel Solove, *The Digital Person* (New York: New York University Press, 2004).

1.3.! Analytical Underpinnings: Concepts of Horizontal Privacy

1.3.1.! Conceptualizing privacy

According to a well-respected tradition in philosophy,[83] a central task of philosophical analysis is to clarify what is meant by a certain term for it to be used subsequently in other analyses. Following such tradition, this section aims to shed light on what does privacy mean.

A widely accepted classification of the different attempts to conceptualize privacy enumerates them as: (i) privacy as the right to be left alone, (ii) privacy as autonomy or the limited access to the self, (iii) privacy as secrecy or concealment of discreditable information, (iv) privacy as control over one's personal information, (v) privacy as personhood and preservation of one's dignity, and (vi) privacy as intimacy and the promotion of relationships.[84]

Warren and Brandeis wrote in 1890 the article that is said to set the right to (informational) privacy in the common law.[85] They showed that, in American case law, the right was already recognized without being explicitly mentioned; they characterized such right as the right to be left alone.[86] Unlike previous literature that argued for enhancing privacy, this was not a reaction against State intervention, but one against the possibilities that other private parties had upon the invention of the automatic camera, which reduced the costs of taking an image of someone

---

[83] This is, analytical philosophy.

[84] The classification is taken from Daniel Solove, "Conceptualizing Privacy," *California Law Review* 90, no. 4 (2002): 1087; Daniel Solove, Marc Rotenberg, and Paul Schwartz, *Privacy, Information and Technology* (New York: Aspen Publishers, 2006). The classification seems to be widely accepted. See, for example, Richard Bruyer, "Privacy: A Review and Critique of the Literature," *Alberta Law Review* 43, no. 3 (2006): 553. Still, it is to note that some authors would fit in more than one category, while others, such as Nissenbaum's privacy as context, seem to not completely fit in any.

[85] See Samuel Warren and Louis Brandeis, "The Right to Privacy," *Harvard Law Review* 4, no. 5 (1890): 193.

[86] See Ibid.

else.[87] This was, hence, an early attempt to approach the problem of informational privacy between private parties, which led to the establishment of the privacy tort in the United States (US).[88]

From a different perspective, other scholars have argued that privacy is a necessary tool to promote the autonomy of people. The idea that one is being watched by others constrains the spectrum of thoughts and behaviors that one considers acceptable, and hence limits one's freedom to fully develop as an autonomous person.[89] Those who focus on this conception consider that privacy interests are centered on limiting one's accessibility, and that this limitation is composed by a combination of secrecy, anonymity and solitude.[90] None of the three is able to encompass privacy interests by itself,[91] they argue, since a loss in any of them can be a privacy loss without altering the other two.[92]

Posner, on the other hand, has famously argued that privacy law is mainly about concealing undesirable facts about oneself to others, chiefly to deceive them in their opinion of oneself.[93] This concealment can take place either to hide discreditable information—for instance a previous crime or misdemeanor—or to hide information that is not discreditable but

---

[87] More specifically, they argued that "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. It is like the right not to be assaulted or beaten, the right not to be imprisoned, the right not to be maliciously prosecuted, the right not to be defamed." Ibid. 205.

[88] Susan Brenner, "The Fourth Amendment in an Era of Ubiquitous Technology," *Mississippi Law Journal* 75 (2005): 1.

[89] See Julie Cohen, "Examined Lives: Informational Privacy and the Subject as Object," *Stanford Law Review* 52, no. 5 (2000): 1373. See also Stanley Benn, "Privacy, Freedom and Respect for Persons," in *Nomos XIII: Privacy*, ed. Ronald Pennock and John Chapman, vol. 8 (New York: Atherton Press, 1971).

[90] Jeffrey Reiman, "Privacy, Intimacy and Personhood," *Philosophy & Public Affairs* 6, no. 1 (1976): 26.

[91] See Ruth Gavison, "Privacy and the Limits of the Law," *Yale Law Journal* 89, no. 3 (1980): 421.

[92] See Sissela Bok, *Secrets: On the Ethics of Concealment and Revelation* (New York: Vintage, 1989); David O'Brien, *Privacy, Law, and Public Policy* (New York: Praeger Publishers, 1979); Edward Shils, "Privacy: Its Constitution and Vicissitudes," *Law and Contemporary Problems* 31, no. 2 (1966): 281.

[93] This conception, together with its economic consequences, will be developed in section 2.2.

would correct a misunderstanding that the person would rather maintain—for instance a serious health problem that a worker prefers that his employer ignores.[94] For the second, he adds that people reveal information to others selectively without strictly lying to them or deceiving (compare for example the image that one's partner has of one, with the image that one's colleagues have), and that people are always eager to disclose facts that portray them in a positive light.[95]

On a third conception, some scholars consider privacy is essentially control over personal information.[96] A refined notion of privacy, they argue, shows that privacy is not the absence of information about one in the public (like Posner considers), but the control that one has over that information. Stating that a man in a desert island is a very private man, for example, would be counterintuitive, even if no information about him is public.[97] Privacy has also been defined along these lines as the absence of undocumented personal knowledge about others.[98]

In a similar regard to those who view privacy as autonomy, the defenders of privacy as personhood argue that privacy is central for developing one's own identity.[99] Schwartz criticizes the paradigm of control over personal information as a liberal view that mistakenly takes autonomy as a given, and he argues that privacy is linked with self-

---

[94] See Richard Posner, "The Economics of Privacy," *The American Economic Review* 71, no. 2 (1981): 405; Richard Posner, "An Economic Theory of Privacy," *American Enterprise Institute Journal of Government and Society (Regulation)* 2 (1978): 19; Richard Posner, "The Right of Privacy," *Georgia Law Review* 12, no. 3 (1978): 393.

[95] See Richard Posner, "An Economic Theory of Privacy," *American Enterprise Institute Journal of Government and Society (Regulation)* 2 (1978): 19; Richard Posner, "The Economics of Privacy," *The American Economic Review* 71, no. 2 (1981): 405; Richard Posner, "The Right of Privacy," *Georgia Law Review* 12, no. 3 (1978): 393.

[96] See, for example, Randall Bezanson, "The Right to Privacy Revisited: Privacy, News and Social Change," *California Law Review* 5, no. 80 (1992): 1133.

[97] See Charles Fried, "Privacy," *Yale Law Journal* 77, no. 4 (1968): 475.

[98] See William Parent, "A New Definition of Privacy for the Law," *Law and Philosophy* 2, no. 1980 (1983): 305; William Parent, "Privacy, Morality, and the Law," *Philosophy & Public Affairs* 12, no. 4 (1983): 269.

[99] See Jeffrey Reiman, "Privacy, Intimacy and Personhood," *Philosophy & Public Affairs* 6, no. 1 (1976): 26; Joseph Bensman and Robert Lilienfeld, *Between Public and Private: The Lost Boundaries of the Self* (New York: Free Press, 1979).

determination. Agreeing to terms and conditions, for example, might technically fall within control over one's personal information but could violate privacy because the terms and conditions can contain boilerplate terms that the user does not understand.[100]

Finally, the supporters of a conception of privacy as intimacy argue that the concept of intimacy encloses all those types of information that one would rather keep private.[101] The idea is that privacy is a tool to protect people from being subject to misrepresentations that could occur when others know some pieces of information about them out of context that could lead to misunderstandings.[102] This concept is more relationship-oriented than others, aiming to avoid the confrontation between the individual and the community.[103] The function of the right to privacy is to define information territories, where it is socially acceptable to keep or to disclose information, defining the boundaries of private life and social life.[104]

1.3.2.! Limits of the concepts

One must note that these conceptions of privacy are not fully independent. Some focus on the means and some on the goals of privacy, and they are interrelated at both levels. Control over personal information, for example, can be seen as derivative of the limited access to the self. Limited access to

---

[100] See Paul Schwartz, "Privacy and Democracy in Cyberspace," *Vanderbilt Law Review* 52 (1999): 1607.

[101] See Julie Inness, *Privacy, Intimacy, and Isolation* (New York: Oxford University Press, 1996); Robert Gerstein, "Intimacy and Privacy," *Ethics* 89, no. 1 (1978): 76; Tom Gerety, "Redefining Privacy," *Harvard Civil Rights-Civil Liberties Law Review* 12 (1977): 233; James Rachels, "Why Privacy Is Important," *Philosophy & Public Affairs* 4, no. 4 (1975): 323.

[102] See Lawrence Lessig, "Privacy and Attention Span," *Georgetown Law Journal* 89 (2000): 2063; Jeffrey Rosen, *The Unwanted Gaze: The Destruction of Privacy in America* (New York: Vintage Books, 2001).

[103] See Paul Schwartz and William Treanor, "The New Privacy," *Michigan Law Review* 101 (2003): 2163.

[104] See Robert Post, "The Social Foundations of Privacy: Community and Self in the Common Law Tort," *California Law Review* 77 (1989): 957.

the self, in turn, presents similarities with the right to be left alone,[105] and the creation of the self seems to be a combination of the two.

All of them conceptualize privacy by looking for a necessary and sufficient set of elements to define it (*per genus et differentiam*), and in such way find its "essence."[106] This approach generates two difficulties.

Firstly, the approach fails to capture the fact that what is and what is not considered private does not depend on an essential characteristic but is dependent on context, and on cultural, historical and technological facts.[107] It has been argued that it is therefore extremely difficult, if not impossible, to succeed in this endeavor of defining precisely the essence of the right to privacy.[108]

In addition, most of the concepts that are equated to privacy have in themselves several different meanings, but they are used as instruments to link privacy breaches to situations that people intuitively consider to be wrong.[109] The concepts of autonomy and personhood, for example, have many facets, and are not more easily definable than the concept of privacy itself. Someone suffering from a privacy violation might complain that such violation injures his personhood or his autonomy, but such statement does not clarify what privacy in itself means. The problem of justifying any aspect of law with our intuitions of what is wrong is that, besides the fact that it is to be proved that such intuitions are generally shared, law must not necessarily prohibit everything that is morally objectionable.[110]

From the perspective of these limits of the prevailing conceptualizations, one can see that it is reasonable to find disagreement among scholars on which of the concepts of privacy which were reviewed is

---

[105] See Daniel Solove, "Conceptualizing Privacy," *California Law Review* 90, no. 4 (2002): 1087.
[106] See Ibid.
[107] See Ibid.; Helen Nissenbaum, "Privacy as Contextual Integrity," *Washington Law Review* 19 (2004): 119.
[108] See Robert Post, "Three Concepts of Privacy," *Georgetown Law Journal* 89 (2000): 2087.
[109] See James Whitman, "The Two Western Cultures of Privacy: Dignity versus Liberty," *Yale Law Journal* 113, no. 6 (2004): 1151.
[110] See Ibid.

the most complete, or the most convincing. In turn, the issue is not negligible, since the concept of privacy that one has implicitly underpins almost any argument that one makes about the functioning of the right to privacy.[111]

This shortcoming can be seen in the two policy debates that are the object of chapters 4 and 5. The right to be left alone concept, for example, cannot account for the right to be forgotten, while privacy as personhood cannot account for laws preventing online tracking. More generally, intimacy cannot account for most of the law regarding informational privacy, since most of DPL protects non-intimate information. Concealment leaves out the secondary use of information and applications of DPL aimed to protect information not considered undesirable. Autonomy leaves out any aspect of informational privacy that is not necessary for decision-making but is still protected by the law and, consequently, it ignores DPL almost as a whole.

These three difficulties (two conceptual, one explanatory) suggest that a different approach to conceptualizing horizontal privacy would be preferable as a foundation for this analysis.

1.3.3.! Privacy as excluding others from one's personal information

A possible way out of the conundrum is to attempt a functional approach to privacy that does not attempt to identify the essence of the right, but to analyze it functionally, based on the practical implications of privacy law rather than on abstract justifications.[112]

This is a less ambitious endeavor since such concept can describe privacy but cannot, by itself, explain it. However, it allows for a flexible concept that can account for a wide array of privacy problems hence taking

---

[111] See Daniel Solove, "'I've Got Nothing to Hide'and Other Misunderstandings of Privacy," *San Diego Law Review* 44 (2007): 745.

[112] In support of this conceptual approach over those which were seen, see Ibid.; Daniel Solove, "Conceptualizing Privacy," *California Law Review* 90, no. 4 (2002): 1087; Irma Van der Ploeg, "Keys to Privacy," in *The Machine-Readable Body*, ed. Irma Van der Ploeg (Maastricht: Shaker, 2005), 15.

into account the chief concerns of the different conceptions, and in that way serve as a useful basis for further explanations.

The protection of informational privacy can be described, for the purposes of this analysis, across the different concepts reviewed as a mechanism to exclude others from certain pieces of one's personal information—or, in an extreme case, of one's personal information as a whole.

Overcoming the explanatory difficulties mentioned, this conceptual basis is able to explain the central elements of the EU data protection framework, and in particular the rights that data subjects have within it. DPL in Europe has evolved by providing data subjects with entitlements over their personal information.[113] This has led to the argument that the general principles of European DPL would be compatible with establishing property rights over data,[114] that European DPL has a human rights based approach which is compatible with the establishment of property interests, and that the system is closer to the property-rights paradigm than the American system of data protection.[115] These entitlements allow data subjects to exclude others—both the State and their peers—from their personal information. The central rights of European DPL, such as the right to object, the right to erasure, the right to refuse and, as it will be seen later on, the right to be forgotten,[116] fit with this concept inasmuch as they signify that data subjects have exclusion rights over their personal

---

[113] See Nadezhda Purtova, "Illusion of Personal Data as No One's Property," *Law, Innovation and Technology* 7, no. 1 (2015): 83; Corien Prins, "The Propertization of Personal Data and Identities," *Electronic Journal of Comparative Law* 8, no. 3 (2004): 1.

[114] See Nadezhda Purtova, "Property in Personal Data: A European Perspective on the Instrumentalist Theory of Propertisation," *European Journal of Legal Studies* 2 (2010): 3; Nadezhda Purtova, *Property Rights in Personal Data: A European Perspective* (Tilburg: Proefschrift ter verkrijging van de graad van doctor aan de Universiteit van Tilburg, 2011).

[115] See Corien Prins, "When Personal Data, Behavior and Virtual Identities Become a Commodity: Would a Property Rights Approach Matter?," *SCRIPT-Ed* 3, no. 4 (2006): 270; Corien Prins, "Property and Privacy: European Perspectives and the Commodification of Our Identity," in *The Future of the Public Domain*, ed. Lucie Guibault and Bernt Hugenholtz (Alphen aan den Rijn: Kluwer Law International, 2006), 223.

[116] See articles 12 and 14 of the Data Protection Directive.

information.[117] So do the main duties of data controllers, such as the duty to have and to specify a limited and justified purpose for collecting and for processing personal data, the general requirement of consent for the secondary processing of data, the duty to provide security of processing and the duty to maintain confidentiality of communications.[118]

Furthermore, this approach presents three analytical advantages for the purposes of the analysis that follows.

First, the concept emphasizes the aspect of privacy that is relevant for information technology. New technologies change the way in which we acquire, store and disseminate information; information technology law as a mechanism to address this does not deal with privacy as the freedom to act without coercion but with informational privacy issues. While this concept might be weak for the first (decisional privacy), it is robust for the second (informational privacy).

Moreover, this functional characterization, since it abstracts from aims, seems to be overarching of the different conceptions of privacy. For this reason, using it instead of any of the concepts reviewed does not run the risk of excluding aspects of informational privacy that could be relevant for the conclusions drawn by other conceptions. By focusing in a functional aspect that is common in all conceptions, it can build on what has been said for each of them while avoiding contradictions.

Lastly, seeing informational privacy as an exclusion mechanism makes it analogous to an entitlement over a certain piece of personal information, in virtue of which the entitlement holder has the right to decide who can access it and who cannot (hence excluding others from accessing the good). This is a broad definition of entitlement, in the lines of the definition used by Calabresi and Melamed; this definition encompasses

[117] A similar trend, although less systematic, seems to be present in American law. An example of this is the *Personal Data Notification and Protection Act* of 12 January 2015, which mandates companies to notify when data has been breached.
[118] See articles 4 and 5 of the e-Privacy Directive.

that the good, in this case personal information, is owned by someone, and that such person has some rights over it.[119]

This establishment of an entitlement is analytically previous to the establishment of a property right, since first one must determine whether an entitlement is in place, to then evaluate which is the appropriate protection for such entitlement.[120] Property, in this sense, is narrower than entitlements and, accordingly, it allows to question whether a property rule, a liability rule or an inalienability rule is the best way to protect the entitlement.

In such way, this functional approach to the concept is fitting as a basis for evaluating DPL from a law & economics perspective. This leads to some open questions. Can DPL be justified from an economic perspective at a general level? Do we have reasons to believe that agents operating under DPL behave rationally? What are the policy implications of this? Do the main current policy debates in European DPL fall within this economic justification? These questions will be addressed in the following chapters.

1.4.! Overview of Chapters

Chapter 2 will ask to what extent DPL as an exclusion mechanism for personal information can be justified in the first place. In order to do so, it will explore whether, contrary to the often-depicted tradeoff between privacy and information, data protection can lead to more production of information and information flow. This counterintuitive result would stem from an analysis of *ex-ante* incentives of creating entitlements to protect personal information. Although as long as property right are defined and transaction costs are low initial allocations should be irrelevant in aggregation (as entitlements will be allocated to its highest valuer *ex-post*), these allocations matter for the generation of goods that are not already available. Some aspects of personal information could fit in this category

[119] See Guido Calabresi and A. Douglas Melamed, "Property Rules, Liability Rules, and Inalienability: One View of the Cathedral," *Harvard Law Review* 85, no. 6 (1972): 1089.
[120] See Ibid.

since, in order to place information and make it available to others within the peer-to-peer system, people face expected costs. When evaluating how to protect these entitlements, one can see that property rules increase information flow, but they introduce new problems. A liability rule, in turn, avoids those problems but it seems difficult to implement. In such way, the chapter aims to explain DPL from a law & economics perspective and, in doing so, provide a conceptual framework for the evaluation of data protection measures.

Chapter 3 will address the issue that, despite the high value that internet users place on privacy, they offer their personal information for low compensations. This behavior, known as the privacy paradox, has been explained by a stream of literature with different behavioral biases, and in particular with hyperbolic discounting. However, economics offers two reasons to discount payoffs—costs of waiting and hazard rates—which produce two possible reasons for choice reversal. The chapter shows that the second can explain the privacy paradox within a rational-choice framework in a way that fits more intuitively with consumer claims and with contemporary policy debates on privacy. This account would change the policy conclusions of the hyperbolic discounting model and would account for current trends in DPL. In particular, it would be relevant for the right to be forgotten.

The right to be forgotten, stipulated in the GDRP, is the topic of chapter 4. The right establishes that anyone could demand any information about himself to be deleted by entities that collect or process data. The chapter analyses article 17 of the proposal and explores some unintended consequences that have been neglected in the debate. Namely, how it strikes a (dis)balance between the right to privacy and the rights to freedom of expression and access to information, and what are the potential welfare impacts that it creates. Finally, it argues that due to the difficulties in its implementation it could introduce a risk compensation mechanism according to which a false feeling of safety would lead people to

engage in more risky behavior than before (Peltzman effect).[121] It also shows that the recent decision in *Google v. Spain* does not rule on the right to be forgotten, but rather on the liability of search engines under the rights and obligations established in the Data Protection Directive. It then makes a brief evaluation on the case arguing that the decision fails to offer a consistent balance between the right to privacy and the freedom of expression.

Chapter 5 deals with limitations on online tracking, which are object of a regulatory debate that has shifted to the use of default rules to enhance privacy. The European Union implemented this idea with the Electronic Communications Framework Directive.[122] The directive aims to change the default system for tracking and move to an opt-in system where data subjects must agree to it beforehand. The chapter presents a comparative overview of the implementation of the directive across member states and evaluates in particular the cases of The Netherlands and the United Kingdom (UK). These are representative examples of implementations with explicit and implicit consent, and two of the most complete regulations on the topic. It then draws from the behavioral economics literature on default rules to evaluate these regulations and to consider whether it is possible to implement the policy in a way that avoids some of the problems that they faced.

In such way, the analysis that follows addresses the tradeoff between privacy and access to information and between privacy and freedom of expression. Making the dynamics of such tradeoff more visible can be helpful in determining at which point of its sliding scale a society might want to stand, and it can also be helpful to answer whether there is any point of such sliding scale in which one can reasonably have both.

---

[121] See Sam Peltzman, "The Effects of Automobile Safety Regulation," *Journal of Political Economy* 83, no. 4 (1975): 677.
[122] Directive 2009/136/EC.

2.!Privacy Entitlements, Property Rules and Liability Rules

2.1. Identifying Tradeoffs

In writings about privacy legislation, both by lawyers and by economists, there is often an implicit idea that there is a tradeoff between data protection and the amount of information available to reach other social goals, such as research that will in turn lead to innovation.[123] This idea is sometimes depicted as a tradeoff between rights and efficiency,[124] prioritizing one or the other depending on the normative views one could have, and it is sometimes left unstated, proposing a balance between the right to privacy and the right to freedom of expression or to the access of information. This idea determines the extent to which the normative arguments that either implicitly or explicitly incorporate it will recommend the protection of privacy.

Contrasting with this idea, there is an argument to be made for a certain level of data protection leading to more production of information, and hence to more information flow, which would in turn increase the scope of the same rights to which privacy is sometimes balanced against. To illustrate this point, one must evaluate the *ex-ante* incentives generated by the creation of entitlements to protect, or to abstain from protecting, personal information.

In a low transaction-cost scenario where property rights are clearly defined, to whom an entitlement is given should not affect total welfare, since costless bargaining will lead to its *ex-post* allocation to its highest valuer. However, there is a caveat to this principle for goods that do not exist yet in the market. Some instantiations of personal data are included in this caveat since they do not fulfill the characteristics of a good until the information is disclosed and it is made available for others to use it. In those cases, to whom the entitlement will be given is relevant to determine levels of investment, and hence the amount of the good that will be

[123] See, for example, Amitai Etzioni, *The Limits of Privacy* (New York: Basic Books, 2008). See also World Economic Forum, "Personal Data: The Emergence of a New Asset Class. Report for the 'Rethinking Personal Data' Project" (Geneva, 2011).

[124] As a partial disagreement, one should note that rights are important for most conceptions of efficiency.

available in the future. In order to disclose personal information and make it available to others within the peer-to-peer system, people face expected costs which, if left uncompensated, would lead to a lower level of disclosure. This argument is strengthened further when paired with the public good characteristics of information, which provide an additional reason for the relevance of these levels of investment; if personal information has positive spillovers, that is a further reason why it would be underproduced if these are not internalized.

For these reasons, there is some degree of data protection that, from a dynamic point of view, increases the amount of personal information available for exchanges. The question would then not be whether to grant data protection at all in order to allow for access to information, but how much of it to grant. No protection at all, similarly to a maximum level of protection, would lead to a low amount of available information.

If this is true for personal data, one should expect the good to either not be produced or to be visibly under-produced under a common property regime where anyone can access it. However, one can observe that even when data protection is low, there is some degree of personal information sharing. A possible explanation for this outcome is taking the production of such information within a process where personal information is an unwilling by-product of another activity, such as browsing websites or using a social network.

In such way, one can explain DPL from a law & economics perspective and, in doing so, have a simplified framework for the evaluation of data protection measures.

Section 2.2 reviews the economic justifications that were made so far for privacy law. The following section evaluates the economic characteristics that personal information has in the technological context described: a public good (section 2.3.1), a good that can be traded in a low transaction-cost scenario (section 2.3.2), a good that does not yet exist in the market (section 2.3.3), a good whose production can be incentivized with data protection (section 2.3.4) and a good that is produced as a by-

product of an activity (section 2.3.5). Section 2.4 approaches property rules and liability rules as alternatives with which an entitlement over personal information can be protected, concluding that the optimal choice would be to have a combination of both. Section 2.5 examines DPL as a way to design this combination, considering its relevant analogies with copyright law. Section 2.6 concludes the chapter

2.2.! The Economics of Privacy

2.2.1.! Concealment and asymmetric information

As it was mentioned,[125] for Posner, the term "privacy" means concealment of information—in particular, concealment of information in an instrumental way. For a first economic evaluation of privacy measures, he argues, this is the concept that has the most interesting economic implications.[126] Privacy as concealment has a direct link with the economics of information, where a person wants to screen a certain characteristic and another would like to conceal it (for example the job market, or even the marriage market), impeding efficient allocations.[127]

His argument is that many privacy concerns are instrumental: hiding information from someone else to obtain something. There are individuals with bad traits and individuals with good traits, and the individuals with bad traits want to hide them (privacy) while the individuals with good traits want to show them. From this point of view, privacy is an intermediate good with costs of protection and costs of

[125] See section 1.3.1.
[126] See Richard Posner, "The Economics of Privacy," *The American Economic Review* 71, no. 2 (1981): 405; Richard Posner, "The Right of Privacy," *Georgia Law Review* 12, no. 3 (1978): 393; Richard Posner, "An Economic Theory of Privacy," *American Enterprise Institute Journal of Government and Society (Regulation)* 2 (1978): 19; Richard Posner, "Privacy," ed. Peter Newman, *The New Palgrave Dictionary of Economics and the Law* (New York: Macmillan, 1998).
[127] Posner develops here the idea that privacy is a tool of concealment of the devious, originally formulated by Arndt. See Heinz Arndt, "The Cult of Privacy," *Australian Quarterly* 21 (1949): 69.

discovery.[128] Privacy then creates an information asymmetry regarding those traits towards the buyers in the market (for example, employers, or potential spouses), therefore distributing wealth and creating inefficiencies.[129] In this way, privacy in the sense of concealment of information reduces the information with which the market allocates resources.[130]

Stigler continues to develop this concept of privacy by referring to it as a restriction on the collection of knowledge or information about someone (including both people and corporations). He refers to information as the property of someone, but a good with the characteristics of a public good: once I tell person *A* certain information, I cannot know if he will tell it to person *B*, which means that the costs of exclusion of information are high. A privacy statute reduces the amount of information about someone that is available for everyone else. Then, people who want information about someone that is protected by a privacy statue will use other less precise (and usually less intrusive and more costly) substitutes, which should work as a proxy for the information that they want to acquire. For

---

[128] See Richard Posner, "The Right of Privacy," *Georgia Law Review* 12, no. 3 (1978): 393.

[129] See Richard Posner, "The Economics of Privacy," *The American Economic Review* 71, no. 2 (1981): 405. For a different argument, stating that information about others is necessarily incomplete, and a lack of privacy rule can lead to hasty judgments about others that are often mistaken, see Daniel Solove, "The Virtues of Knowing Less: Justifying Privacy Protections against Disclosure," *Duke Law Journal* 53, no. 3 (2003): 967. For the argument that the internet is prone to disseminating false rumors, see Cass Sunstein, "Believing False Rumors," in *The Offensive Internet*, ed. Saul Levmore and Martha Nussbaum (Cambridge, Mass.: Harvard University Press, 2010), 91.

[130] Still, Posner argues that the US privacy tort is efficient. The tort covers four aspects: preventing the use of one's picture and name without one's consent for advertising purposes, preventing facts about one being portrayed under a "false light", preventing people from obtaining information by intrusive means, and preventing the publication of intimate facts about oneself. Posner argues that the first three increase the flow of information and that the prevention of publication of intimate facts is rarely enforced. See Richard Posner, "The Economics of Privacy," *The American Economic Review* 71, no. 2 (1981): 405; Richard Posner, "The Right of Privacy," *Georgia Law Review* 12, no. 3 (1978): 393.
In Europe, absent Warren and Brandeis' influence, there tends to be no autonomous privacy tort prior to DPL that is independent from the confidentiality of communications. For the UK, which is probably the jurisdiction that is the most explicit about this, see *Home Office v Wainwright*, EWCA Civ. 2081 (2001).

example, if an employer cannot access the work history of a potential employee, he will establish a trial period in which he will monitor the new employee.[131] A similar principle can be applicable to the internet: if the same employer cannot access criminal records because of a privacy rule, he will estimate the likelihood of that employee having a criminal record based on the information that he has available.

The second step in the argument is an application of the Coase theorem.[132] With clearly defined property rights and low transaction costs, goods will end up in the hands of those who value them the most, independently of their initial allocation, since under those conditions the party that values a good the most can buy it from the other if the initial allocation was granted to him. It was argued, in these lines, that if one applies this argument to personal information, then as long as transaction costs remain low, it is irrelevant for the final allocation of the information whether there is a privacy rule that allocates it to the person to whom that information refers, or there is no privacy rule, which allocates the information to whoever finds it.[133] Privacy law would have then a distributional effect but would not have a welfare effect. For that reason, it is not justifiable to introduce disturbances in the market such as information asymmetries, which would be welfare-decreasing. [134]

---

[131] See George Stigler, "An Introduction to Privacy in Economics and Politics," *Journal of Legal Studies* 9, no. 4 (1980): 623. In these contexts, not disclosing information can sometimes also be informative for the other party: if people with good traits can reveal them, but people without them cannot do so fraudulently, then the lack of disclosure will be informative of the lack of good traits.

[132] See Ronald Coase, "The Problem of Social Cost," *Journal of Law and Economics* 3, no. 1 (1960): 1.

[133] See Richard Posner, "The Right of Privacy," *Georgia Law Review* 12, no. 3 (1978): 393; Richard Posner, "The Economics of Privacy," *The American Economic Review* 71, no. 2 (1981): 405; George Stigler, "An Introduction to Privacy in Economics and Politics," *Journal of Legal Studies* 9, no. 4 (1980): 623. 981

[134] See Richard Posner, "The Right of Privacy," *Georgia Law Review* 12, no. 3 (1978): 393; Richard Posner, "The Economics of Privacy," *The American Economic Review* 71, no. 2 (1981): 405; George Stigler, "An Introduction to Privacy in Economics and Politics," *Journal of Legal Studies* 9, no. 4 (1980): 623. 981

2.2.2.! Property rights over personal information

A property rule over personal information can be portrayed as a non-disclosure default (unless consent is given). If the individual owns the property right, he can control the dissemination of his own personal information. On the other hand, if data collectors own the property right, then the default rule is disclosure.[135] The non-disclosure default rule (a privacy rule) has been argued to be welfare-increasing for three reasons.

The first reason is that technologies have drastically decreased the transaction costs of acquiring people's personal information.[136] These transaction costs are not symmetric, and the difference in transaction costs for consumers and companies makes property rights over personal information efficient. If property rights are given to data collectors, the costs for individuals of knowing what personal information about them was disseminated or is going to be disseminated in order to engage in negotiations is high, while these costs would be low for data collectors.[137]

In a scenario where companies have the property rights over information, individuals would face a collective action problem.[138] Moreover, under a regime with no privacy companies lack incentives to make it easy for internet users to have an augmented control over their personal information.[139] The presence of property rights over such information would force a negotiation that would alter this; for instance, by developing more privacy-enhancing technologies (PETs).[140] Market-

---

[135] See Richard Murphy, "Property Rights in Personal Information: An Economic Defense of Privacy," *Georgetown Law Journal* 84, no. 1 (1995): 2381.
[136] This statement is further explored in section 2.3.2 below.
[137] See Jerry Kang, "Information Privacy in Cyberspace Transactions," *Stanford Law Review* 50, no. 4 (1998): 1193.
[138] See Ibid.
[139] See Lawrence Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books, 1999); Lawrence Lessig, *Code 2.0* (New York: Basic Books, 2006).
[140] See Lawrence Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books, 1999); Lawrence Lessig, *Code 2.0* (New York: Basic Books, 2006); Julie Cohen, "Examined Lives: Informational Privacy and the Subject as Object," *Stanford Law Review* 52, no. 5 (2000): 1373.
For PETs, see generally GW van Blarkom, John Borking, and Jacobus Olk, *Handbook of Privacy and Privacy-Enhancing Technologies* (The Hague: College bescherming persoonsgegevens, 2003). Chapter 3. The European Commission has

based mechanisms that assure a higher level of control over one's personal information are said to be thus desirable order to ensure a proper protection of privacy in the face of new technologies.[141]

The second reason is that the concealment approach, which considered that privacy is socially welfare-decreasing, did not take into account the non-instrumental value of privacy.[142] The rule where individuals own a property right over information is argued to be welfare-enhancing because of pure privacy preferences that form part of data subjects' utility functions.[143] This preference encompasses the taste for privacy in contexts where the individual wants to keep information private for reasons that are different from deceiving others.[144]

Surveys have shown that people disagree with the view that those who are concerned about their privacy have immoral or illegal behaviors that are trying to hide,[145] idea that is confirmed by psychological literature on the topic.[146] People seem to have "pure privacy preferences" which are independent from considerations of reputation or deceit;[147] these are likely to be motivated by reasons such as the improvement of the consumption experience, the elimination of interference by disapproving peers, and the

---

defined them as "a coherent system of ICT measures that protects privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal fata, all without losing the functionality of the information system." See COM(2007) 228 final. Typical PETs include encryption tools and IP masks.

141 See Kenneth Laudon, "Markets and Privacy," *Communications of the Association for Computing Machinery* 39, no. 9 (1996): 92.

142 See Ibid.

143 Posner also recognizes the relevance of pure privacy preferences in later work regarding governmental surveillance. See Richard Posner, "Privacy, Surveillance, and Law," *The University of Chicago Law Review* 75, no. 1 (2008): 245.

144 See Kenneth Laudon, "Markets and Privacy," *Communications of the Association for Computing Machinery* 39, no. 9 (1996): 92.

145 See Priscilla Regan, *Legislating Privacy: Technology, Social Values, and Public Policy* (University of North Carolina Press, 1995). P. 48.

146 See Cathy Goodwin, "A Conceptualization of Motives to Seek Privacy for Nondeviant Consumption," *Journal of Consumer Psychology* 1, no. 3 (1992): 261.

147 See Sasha Romanosky and Alessandro Acquisti, "Privacy Costs and Personal Data Protection: Economic and Legal Perspectives," *Berkeley Technology Law Journal* 24, no. 3 (2009): 1061.

relief from self-discrepancies.[148] Due to the presence of these preferences, there is no evidence to believe that the utility gain for the acquirers of data subjects' information is always larger than their utility loss in the interactions that are not mediated by consent. If one establishes a property right over personal information, however, those preferences can be reflected in the market and balanced with the amount of information available.[149]

The third reason is that externalities are present in data processing. There is a privacy interest implicated every time information about someone is collected or used without his consent, potentially imposing an externality on him. The private cost of collecting personal information is then lower than the social cost. Therefore, there is more collection of personal information than what is socially efficient.[150] As long as ownership of personal information is given to the collector and not to the data subject, people do not receive a compensation for the use of their personal information and the price of such information is low because it fails to reflect the social cost of privacy invasions.[151]

The secondary use of information also poses externalities to data subjects, which comes in the form of annoyances, such as junk emails, which consume their time and attention.[152] Defining property rights in

---

[148] See Cathy Goodwin, "A Conceptualization of Motives to Seek Privacy for Nondeviant Consumption," *Journal of Consumer Psychology* 1, no. 3 (1992): 261.

[149] See Richard Murphy, "Property Rights in Personal Information: An Economic Defense of Privacy," *Georgetown Law Journal* 84, no. 1 (1995): 2381; James Rule and Lawrence Hunter, "Towards Property Rights in Personal Data," in *Visions of Privacy: Policy Choices for the Digital Age*, ed. Colin Bennett and Rebecca Grant (Toronto: University of Toronto Press, 1999), 168.

[150] See Kenneth Laudon, "Markets and Privacy," *Communications of the Association for Computing Machinery* 39, no. 9 (1996): 92.

[151] See Kenneth Laudon, "Extensions to the Theory of Markets and Privacy: Mechanics of Pricing Information," Stern School of Business Working Paper 97-04 (New York, 1997).

[152] If someone gives his telephone number to a company so they can fix his cable, and then the company gives it to someone else that calls him at dinnertime to sell him an insurance, that is a cost (in the form of attention and time that is taken from him) that is externally imposed from the transaction between the cable company and the insurance company. See Hal Varian, "Economic Aspects of Personal Privacy," in *Cyber Policy and Economics in an Internet Age. Topics in*

private information in a way that allows consumers to retain control of how much information about them is used, since their agreement is needed for further trade, would internalize these externalities.[153]

The use of encryption has been suggested as a way to approximate the property protection standard "from below" in the absence of legislation which establishes it.[154] Encryption allows excluding others from a certain piece of information, and hence should allow for bargaining and redistribute wealth to consumers.[155] This approach is similar to the one taken before the establishment of postal secrecy.[156] The inconvenient that this approach presents is that it can be costly for data subjects to engage in it and, even if they do, the aggregated costs of self-protection would be socially wasteful.

2.2.3.! The economic rationale of privacy law, or lack thereof

The literature on the economics of privacy seems to show that there is so far little economic justification for the right to privacy. Posner and Stigler's reluctance to protect privacy has been attacked mainly on the basis that it departs from (and depends on) the narrow conception of privacy as concealment,[157] but no alternative economic justifications have been offered from more ample concepts, with the exception of the literature arguing for propertization.

In turn, the propertization of personal information that was proposed as an alternative presents its own difficulties. For example, it has been argued that, given that the good protected is intangible, establishing

---

Regulatory Economics and Policy Series., ed. William Lehr and Lorenzo Pupillo (Norwell: Springer, 2002), 127.

[153] See Ibid.

[154] See Eli Noam, "Privacy and Self-Regulation: Markets for Electronic Privacy," in *Privacy and Self-Regulation in the Information Age*, ed. Barbara Wellbery (Washington, DC: National Telecommunications and Information Administration, 1997), 21.

[155] See Ibid.

[156] See section 1.2.2.

[157] See Edward Bloustein, "Privacy Is Dear at Any Price: A Response to Professor Posner's Economic Theory," *Georgia Law Review* 12 (1978): 429.

a property right over personal information would mean, in essence, creating a new intellectual property right, but this right would generate an incompatibility between the reasons to protect information with intellectual property law and the reasons to protect personal information.[158]

Moreover, the strongest defenders of privacy rules who suggest that they should be protected by property rights leave a central issue unanswered. If it is true that transaction costs are low, then as long as the property rights are clearly defined, to whom the property right is allocated should be irrelevant in aggregation, as the allocation will not change who will be the right holder *ex-post*. In addition, the reason why each agent values the good in which amount, and whether there are any externalities, should also be irrelevant, as low transaction costs allow for a bargaining process that can lead them to be internalized by the market.[159]

Privacy, in fact, is usually justified on deontic grounds, which are able to support a wide privacy right as long as one considers that people have a fundamental right to privacy. It seems that efficiency, if at all, would support a narrower concept of privacy than the one proposed in the human rights literature. From this one can take two messages about the economics of privacy. First, that efficiency considerations are not the best tool to attack privacy in a certain area where it is being debated, since it will always be the perspective with the narrowest view about it. Second, that when efficiency considerations actually support a defense of privacy in a certain domain, they constitute a good argument for its establishment.

The following sections portray a scenario in which efficiency considerations, in fact, can support a defense of privacy within the domain of DPL.

---

[158] See Pamela Samuelson, "Privacy as Intellectual Property?," *Stanford Law Review* 52, no. 5 (1999): 1125.

[159] See Ronald Coase, "The Problem of Social Cost," *Journal of Law and Economics* 3, no. 1 (1960): 1.

2.3.! Special Characteristics of Informational Privacy in the Web

2.3.1.! Personal information as a public good

A central characteristic of information is that people can make use of it without leaving less for others, and for the case of digitalized information, it is very easy to reproduce. Information, for this reason, has public good characteristics: once it is released, it can be reproduced at a marginal cost close to zero (non-excludability) and the use of information does not reduce the amount which is left available for others (non-rivalry).[160]

Due its public good characteristics, the generation of information produces positive spillovers to others than its creators. These positive spillovers, or positive externalities, imply that not all of the social benefits from the generation of the information are internalized by the creator, and for that reason he might have suboptimal incentives to produce it. As a consequence, he might generate less information than what is socially desirable. For this reason, it might be socially welfare-increasing in the long run to incentivize its production.[161]

Classic literature has addressed works of authorship as suffering both from the problems of non-excludability and non-rivalry due to the characteristics of information[162] even before Samuelson's seminal work on public goods.[163] Shortly after, information was identified as a quasi-public

---

[160] See George Stigler, "An Introduction to Privacy in Economics and Politics," *Journal of Legal Studies* 9, no. 4 (1980): 623; Paul Schwartz, "Property, Privacy, and Personal Data," *Harvard Law Review* 117, no. 7 (2004): 2056.

[161] For an analysis along these lines in the form of a prisoners' dilemma where agents choose whether to produce or reproduce information in the context of intellectual property, see Wendy Gordon, "Asymmetric Market Failure and Prisioner's Dilemma in Intellectual Property," *University of Dayton Law Review* 17 (1992): 853.

[162] See Arnold Plant, "The Economic Aspects of Copyright in Books," *Economica* 1 (1934): 167; Arnold Plant, *The New Commerce in Ideas and Intellectual Property* (London: Athlone Press, 1953).

[163] See Paul Samuelson, "The Pure Theory of Public Expenditure," *Review of Economics and Statistics* 36 (1954): 387.

good that suffers both from the problems of non-excludability and non-rivalry.[164]

Personal information as a sub-type of information shares these characteristics. As such, given that information has a cumulative nature (the uses that are given to it are not independent but they build upon each other),[165] it behaves as a capital good that can foster innovation.[166] As innovation presents most of its benefits in the future, it is difficult to grasp the effects that different kinds of information, or even information in general, will have, unless one takes into account its dynamic aspects. Inasmuch as it presents the characteristics of a public good, it could be socially desirable to incentivize the generation of new information, as well as information flow. The next subsections explore how data protection relates to it, and therefore to innovation.

2.3.2.! Low transaction costs of personal information exchanges

Independent of which concept of privacy one finds the most convincing,[167] it was seen that the protection of informational privacy can be described across them as a mechanism to exclude others from one's information.[168] Seeing informational privacy as an exclusion mechanism makes it analogous to an entitlement over a certain piece of personal information, in virtue of which the entitlement holder has the right to decide who can

---

[164] See Robert Hurt and Robert Shuchman, "The Economic Rationale of Copyright," *American Economic Review* 56, no. 1 (1966): 421; Stephen Breyer, "The Uneasy Case for Copyright: A Study of Copyright in Books, Photocopies and Computer Programs," *Harvard Law Review* 84, no. 2 (1970): 281.

[165] See William Landes and Richard Posner, "An Economic Analysis of Copyright Law," *Journal of Legal Studies* 18, no. 2 (1989): 325.

[166] From this perspective, information is socially valuable in a way that is difficult to quantify. Determining how far in the future one wants to look and what discount rate one wants to apply are only the first obstacles to specify its social benefits. This is also the case, for example, of environmental goods.

[167] See Daniel Solove, "Conceptualizing Privacy," *California Law Review* 90, no. 4 (2002): 1087; Daniel Solove, Marc Rotenberg, and Paul Schwartz, *Privacy, Information and Technology* (New York: Aspen Publishers, 2006). See also section 1.3.2.

[168] See section 1.3.3.

access it and who cannot. In particular, it makes it analogous to an entitlement of data subjects to exclude anyone from their personal information. This is analytically previous to the establishment of a property right, since one must first determine whether an entitlement is in place, to then evaluate which is the appropriate protection for such entitlement.[169] But why should one place entitlements over personal information at all?

In an interaction between a data subject (*A*), an information intermediary (*B*) and a third party interested in the information (*C*) regarding a certain piece of personal information that relates to *A*, a policymaker has three options with respect to the entitlement of such information. He could entitle *A* with a right to exclude the others (*B* and *C*) from the piece of information, he could entitle *B* to exclude the others (*A* and *C*) from that information, or he could grant no one the exclusion right, allowing anyone to obtain and use the information.[170]

It was seen above how technological changes have reduced the transaction costs for gathering, storing and disseminating information, and in addition that in the peer-to-peer system data subjects voluntarily give personal information.[171] These technological characteristics reduce the costs of copying and distributing information, making the marginal cost of information gathering close to zero.[172] In the context of information technology, personal information exchanges have reduced costs of communication among parties and, hence, have low transaction costs.[173]

---

[169] See Guido Calabresi and A. Douglas Melamed, "Property Rules, Liability Rules, and Inalienability: One View of the Cathedral," *Harvard Law Review* 85, no. 6 (1972): 1089.

[170] Under a property regime, this would be analogous to leaving the information as common property, where everyone has a right to access and no one has a right to exclude.

[171] See section 1.1.

[172] See Raymond Ku, "The Creative Destruction of Copyright: Napster and the New Economics of Digital Technology," *University of Chicago Law Review* 69, no. 1 (2002): 263.

[173] See Trotter Hardy, "Property (and Copyright) in Cyberspace," *University of Chicago Legal Forum* 1 (1996): 217.

In the traditional market for personal information, the acquirer incurs into certain costs to acquire such information. These are, for example, chasing a celebrity in the street to take pictures of him, eavesdropping on a conversation behind a door to know about its content, or wiretapping a telephone line and listening to what is being said. The market for personal information online, on the other hand, does not necessarily follow this pattern due to its different technological characteristics: reduced costs and the peer-to-peer system.

Many ways of acquiring information about other people online, such as setting up a virus attack or looking for their information in search engines, follow a similar structure to the traditional market for personal information but present much lower transaction costs. In them, the person who desires the information must engage in some degree of search costs in order to acquire it, even though the costs of doing so are often much lower than those of traditional privacy invasions. Looking for someone's details in a search engine, for example, is easier and less costly than going through his correspondence, wiretapping his telephone or asking questions to his friends.

Moreover, in some markets for personal information online, in particular in social networks and cloud computing, where online profiling is used,[174] it is the producer of the personal information (the data subject) who directly puts it in the hands of the acquirer, seemingly for free.[175] This mechanism, described as the peer-to-peer technology or Web 2.0,[176] implies that the acquisition of such information has not only a reduced marginal cost compared to the traditional privacy scenario, but a marginal cost of zero. This can take place in two different ways: though the creation of active digital footprints and passive digital footprints.

---

[174] Profiling is the assembling of personal information from different sources to generate a complete database of a data subject. See Roger Clarke, "Profiling: A Hidden Challenge to the Regulation of Data Surveillance," *Journal of Law, Information and Science* 4 (1993): 403.

[175] Alessandro Acquisti, Laura Brandimarte, and George Loewenstein, "Privacy and Human Behavior in the Age of Information," *Science* 347, no. 6221 (2015): 509.

[176] See Lawrence Lessig, *Code 2.0* (New York: Basic Books, 2006).

Firstly, social network companies do not need to incur into additional costs in order to discover personal information about their users because, by utilizing the social network, they provide that information to them by themselves.[177] Other users of the social networks, similarly, do not need to ask their friends and acquaintances for their recent pictures and updates because they often send them through the social networks. Cloud computing companies, in the same line, do not need to inquire about which kind of files their users manage because, by using the cloud computing service, they show that information to them voluntarily.

Secondly, there are technologies in the internet such as http cookies that, when used, create data trails without a need for the user to actively attempt to do so—and they can do this either with or without his knowledge. Even for the cases of these technologies in which—unlike social networks—they are not specifically designed to create data trails, they generate user-metadata associated with the places where the user places his attention, and therefore also encourage the generation of personal data.

The counterpart of this reduction on the costs of collecting and disseminating information is that there are increased costs of protecting one's personal information. Surveillance in cyberspace, as it was mentioned, is more difficult to detect than in physical spaces,[178] which means that preventing such surveillance is more costly.

Protecting one's privacy on the internet requires technical skills that not all data subjects possess, and that for the ones that do possess those skills this protection can be costly. The tradeoff between data disclosure and expected privacy costs is opposed to another tradeoff between privacy and convenience. For example, browsing through anonymity networks such as TOR, which is one of the most effective means of self-protection, leads to a reduction in usability (by having the need to retype all registration data on each access) and to a decrease in browsing

[177] These companies have to build an infrastructure that represents fixed costs, while the marginal costs of acquiring information from data subjects is close to zero.
[178] See section 1.1.

speed. Moreover, monitoring one's personal information after disclosure is rarely possible and, when so, it is costly. There is yet no equivalent for the internet to the sealed envelopes mentioned in the introduction for postal secrecy.[179]

2.3.3.! Personal information as good that does not yet exist

This low-transaction cost scenario implies that, whatever the allocation of the entitlement is, as long as this allocation is clear, *ex-post* bargaining can lead to its efficient allocation. For this reason, it would seem that it is not interesting for policymaking to determine who is the highest valuer of the right over the information or if there are any externalities, as due to the low transaction costs described above these can be internalized by the market.

A caveat to this principle is that to whom an entitlement is allocated has distributional effects. If the information intermediary *B* values the good more than the data subject *A*, and an entitlement over the information is given to *A*, then *B* will obtain the entitlement as a result of a bargaining process with *A*. However, although irrelevant in aggregation, it is relevant both for *A* and for *B* who had the entitlement initially. The information intermediary *B* had to give something to *A* to obtain the good over which *A* had the entitlement, which means that if *B* had been given the entitlement in the first place, he would have been wealthier at the end of the transaction.

These distributional effects, in turn, are relevant for goods that do not exist in the market at the moment of the definition of the entitlements. If data subject *A* had to produce the good to trade with *B*, and (in the opposite case as the one in the previous paragraph) the entitlement was *ex-ante* given to *B*, then *A* would lack incentives to produce it, since the

[179] See Susan Brenner, "The Fourth Amendment in an Era of Ubiquitous Technology," *Mississippi Law Journal* 75 (2005): 1.

distributional effect of the entitlement would be eliminated.[180] The allocation of entitlements determines the incentives for *ex-ante* investment in the generation of the good in question because it determines who will get paid in the trade that will take it to its highest valuer. Hence, it affects the *ex-ante* production mechanism of the good.[181]

The mechanisms for generating information either actively or passively that were described in the last subsection (peer-to-peer system or surveillance, respectively) illustrate the fact that the amount of personal information available is not static. A significant portion of it is produced by users of these services depending on how much (and how many) of these services they consume. This data, in turn, would not fulfill the characteristics of a good until it is disclosed to others, since before the disclosure takes place, they are not readily available to be used and therefore not able to satisfy other people's needs.[182] For this reason, personal information which is handed-in voluntarily is included in the caveat regarding the impact of distributional effects.

In turn, the disclosure of information by data subjects requires investment levels in the form of expected privacy costs, which depend on the information disclosed. The more personal information that is disclosed by a data subjects in the use of these products, the higher the risk that he faces harm in the form of a privacy breach. Data subjects face expected costs of privacy breach both in their initial production of information, and subsequently in the information trade between data collectors,

---

[180] This is analogous to the reason why most legal systems establish protections in the form of entitlements for intellectual property, as it is evaluated in section 2.5.2. below.

[181] See Oliver Hart and John Moore, "Property Rights and the Nature of the Firm" 98, no. 6 (1990): 1119; Thomas Merrill and Henry Smith, "What Happened to Property in Law and Economics," *Yale Law Journal* 111, no. 2 (2001): 357; Thomas Merrill and Henry Smith, "Making Coasean Property More Coasean," *Journal of Law and Economics* 54, no. 4 (2011): 77.

[182] Goods have been defined as materials that can readily satisfy human wants, and in such way increase utility. See Murray Milgate, "Goods and Commodities," ed. Lawrence Blume and Steven Durlauf, *The New Palgrave Dictionary of Economics* (New York: Macmillan, 2008).

intermediaries and advertisers.[183] Data processing poses the problem that the company that carries it out obtains the full benefits of the processing, via marketing gains or fee gains with the sale of such information, while it does not suffer the expected losses produced by such disclosure of personal information, hence having incentives to overuse personal information.[184] In other words, data trades imply externalities for data subjects.[185]

This often leads data subjects, in the absence of regulatory protection, to engage in socially costly self-protection. The failure of engaging in it can lead, in the worse cases, to identity fraud or identity theft. An example of these materializing that became famous due to its magnitude is the Sony scandal of 2011, where data from 100 million users were stolen from the Sony Online Entertainment databases. Many of those data subjects had not used the device that uploaded information to the database but their information was nonetheless in it because it had been replicated or moved. The stolen information included names, addresses, birth dates, and debit and credit card information, which were later used for a wide array of frauds.[186]

A relevant factor to take into account when establishing data protection rules, for these reasons, is that one is not simply defining an entitlement over an already available good over which there could be a dispute. When establishing data protection rules one is also defining entitlements over goods that do not yet exist, and whose generation implies expected costs for the data subjects that must generate them.

---

[183] See John Hagel and Jeffrey Rayport, "The Coming Battle for Consumer Information," *Harvard Business Review* 75, no. 1 (1997): 53. See also section 3.4.2 below.

[184] See Peter Swire and Robert Litan, *None of Your Business: World Data Flows, Electronic Commerce and the European Privacy Directive* (Washington, DC: Brookings Institution Press, 1998)., p. 8.

[185] See Kenneth Laudon, "Markets and Privacy," *Communications of the Association for Computing Machinery* 39, no. 9 (1996): 92; Hal Varian, "Economic Aspects of Personal Privacy," in *Cyber Policy and Economics in an Internet Age. Topics in Regulatory Economics and Policy Series.*, ed. William Lehr and Lorenzo Pupillo (Norwell: Springer, 2002), 127. For a development of this argument, see section 3.4.2 below.

[186] See Sony Online Entretainment Press Release, "Sony Online Entretainment Announces Theft of Data from Its Systems," 2011.

2.3.4.! The effects of data protection over information flow

From a static point of view, information flow is a counteracting value to privacy: the less data protection, the fewer rights of exclusion that people will have over different pieces of information, and the more personal information that will be available on the market. This has been, as it was explained, the underlying idea in the first-generation economics of privacy literature.[187]

From a dynamic point of view, however, based on the characteristics of being a good that is costly to produce and does not exist yet, the allocation of the entitlement through data protection becomes relevant. The reason is that the disclosure of personal information largely depends on the allocation of the entitlement. In this way, some degree of data protection incentivizes the generation of information and, consequently, an increment in information flow, since data protection allows for exchanges over pieces of information that would have not been generated had it not been in place.[188]

An example of this effect is the number of people that, under the current data protection regime, abstain from using social networks because of privacy concerns. If a higher level of data protection was in place, these concerns would not rise and those users would not need to abstain from using the social network because of them. This means that they would produce, in their use, information that under the current regime is not being generated.

While the static and the dynamic effect work in opposite directions, it is possible that, up to a certain level of protection, the second overcomes

---

[187] See section 2.2.

[188] There is some tension between an increment in data protection, which generates more personal information, and the innovations that this increase in the amount of personal information can produce, which translated into the incentive/access tradeoff. Personal information tends to induce innovation when innovators can access and use it—particularly when they can do so for free. This means that personal information especially leads to innovation where it is not protected. This tension reflects the differences between information production and information flow.

the first in the long run. This would be a similar mechanism to the exclusion of some people for the use of products protected under copyright law, which is compensated in the long run by the amount of people that can access those creations which take place due to the incentives set by these laws.[189]

Under an extreme regime with no data protection at all, there would be a low level of information production (long-term effect) but a high level of information flow of the data that is produced (short-term effect). Under a regime on the other end of the scale, where disclosure of information would be directly forbidden, personal information as a good would have a system analogous to public ownership; although people would have the right (and obligation) to exclude others, they would not have the right to exchange.[190] This would produce the opposite result, of a high level of information production (long-term effect) but a low level of information flow (short-term effect). In the middle of both regimes there are several options. A property rule, as proposed by a section of the literature,[191] and a liability rule, would be two possibilities within that scope.

Due to the static effect, an extremely high data protection regime would lead to little information flow because nothing would be able to be disclosed.[192] Due to the dynamic effect, on the other hand, a very low data protection would lead to a low level of information production because data subjects would be under-incentivized to place such information in the market.

Due to this interrelation between the short-term effects of information flow and the long-term effects of generation of information, it

---

[189] A closer evaluation of the common elements between DPL and copyright is done in section 2.5.2 below.

[190] Regarding the characteristics of public ownership, see Armen Alchian, "Some Economics of Property Rights," *Il Politico* 30 (1965): 816.

[191] See section 2.2.2.

[192] This would be a more extreme system than that of PETs, which seek to allow for a high privacy preservation while allowing the sharing of high-value data for socially valuable aims such as research. A PET-based system, in the ideal types identified here, also lies in the middle of both extreme regimes.

seems that the relationship between data protection and the amount of personal information presents a concave function ($f' > 0, f'' < 0$). In order to maximize the amount of personal information in the market, a policymaker would have to set a level of exclusion high enough to incentivize information production, but not too high as to stop information flow. This dynamic is illustrated in figure 1.

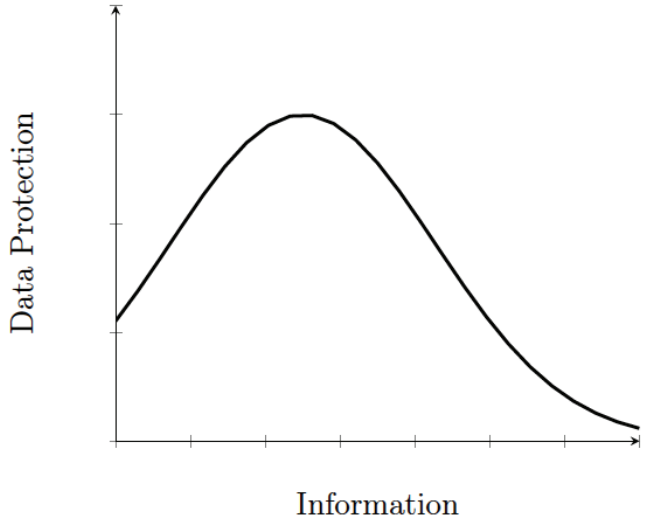

Figure 1. Illustrates the relationship between levels of data protection and amount of information available.

In sum, the traditional arguments of the economics of privacy supporting full disclosure have limitations in the context of DPL and online privacy due to the technological characteristics that underpin these. These arguments are applicable to this context from a static point of view. However, from a dynamic point of view, a certain level of data protection increases the supply of information. It could still be reasonable to not establish such exclusion rights when transaction costs are high; independently of the effects on production, such allocation might impair the entitlement to end in the hands of the highest valuer under high transaction costs. However, as it was stated by the literature surveyed, and again due to the technological characteristics which are involved in

DPL, transaction costs are low in this context on average.[193] As transaction costs are low, the right is likely to go to the higher valuer in any case, especially when the acquirers of such data (data collection companies) are likely to have less liquidity constrains than the other party (data subjects). However, to whom one allocates the entitlement is still relevant for the production of information.

2.3.5.! Personal information as a by-product

A possible concern to the argument presented is that personal information was still produced to some degree before the apparition of DPL, and it is likely that some degree of personal information production would take place even in the absence of DPL. This concern was reflected in figure 1, where the curve intersects with the *y* axis above zero. This section addresses this issue by explaining that personal information, besides being a public good, is produced as a by-product of an activity.[194]

Mill had already noticed that "it sometimes happens that two different commodities have what may be termed a joint cost of production (…) both produced from the same material, and by the same operation."[195] Unlike standard goods such as bread, beer or cereal, no one decides to produce personal information and does so deliberately in order to sell it to others. For example, companies do not ask people directly where they are at each moment of the day, but offer them a product to check their daily distances and calorie expenditure, which records their location data.

The process in which personal information is produced, therefore, is analogous the processes of other products, such as gas (by-product of coal) or manure (by-product of animal breeding). This is, a process in which two goods are produced simultaneously by a certain production process using a common input where (i) both products are desirable goods, such as gasoline

---

[193] See section 2.3.2.

[194] On by-products in joint production, see generally Richard Cornes and Todd Sandler, "Easy Riders, Joint Production and Public Goods," *Economic Journal* 94, no. 375 (1984): 580.

[195] John Stuart Mill, *Principles of Political Economy: With Some of Their Applications to Social Philosophy* (Longmans, Green, 1865).

and kerosene, or (ii) one of them is a desirable good while the other is an undesirable good, such as the different cases of pollution.

Data subjects consume a certain good deliberately; this good can be, for instance, interaction or time spent at a certain website. They trade their time at the website to someone who desires it because he can profit from that time or attention span—for example, to sell advertisements. This exchange is how ad-supported websites are traditionally financed.[196] Blogs and news websites, for example, compete for data subjects' attention because it allows them to have more expensive advertisements that provide them with revenue.

In cases of online profiling, such as in social networks and in cloud computing, the consumption of the good (for example, time at the website) produces simultaneously another good (personal information): the more one does on Facebook the more Facebook knows about one, and the more files one uploads to Dropbox the more Dropbox knows about one. This personal information is useful to the producers of the web service. Now they not only can show advertisements to the user, but they can also personalize their content, increasing relevance and sales.

From this perspective, personal information can be seen as produced in a process of joint production, where it is a by-product of the activity of using a product. Unlike gasoline and kerosene, personal information is a by-product not of the production of another good but of the consumption of other goods. Under this framework, consumption of the social network, which is desirable for the data subject, is tied to production of his private information. This functions differently than traditional exchanges. People do not say "I need to generate more personal information in order to buy more time at Facebook" but just know that the more they use the product the more personal information about them that will be in the market. The production of personal information and its

---

[196] See Lokke Moerel, *Big Data Protection. How to Make the Draft EU Regulation on Data Protection Future Proof* (Tilburg: Tilburg University Press, 2014). Chapter 1. See also Alexander Furnas, "It's Not All about You: What Privacy Advocates Don't Get about Data Tracking on the Web," *The Atlantic*, March 15, 2012.

placement in the market is, from this point of view, unintended, even if it can be conscious.

In standard joint production, there is one marginal cost curve and two demand curves for the different products. If the proportions of the products are fixed, then one of them will be produced in an amount that is different from the efficient amount.[197] Another type of joint production is the scenario where the good is a by-product of an activity, which is prominent in environmental issues. In environmental economics there is often a different case of joint production, where the production of a good also gives as an outcome a by-product that is (collectively) harmful.[198] While in the first case the agent in the market produces two "sellable" goods and optimizes the production of one, either overproducing or underproducing the other, in the second case the agent focuses on the production of one particular good that he can sell, and the other is a by-product that does not alter his utility function.[199]

The production of personal information by social network users seems to resemble more the second case. When users generate personal information with the use of the product, they do not deliberately produce an extra good to sell—such as with the case of oil and wood processing. While they are consuming the web service, they unwillingly produce personal information, which is a good for the service provider. Instead, the generation of this product has an expected (private) cost, which is the increased risk of a privacy breach together with the disutility of sharing personal information from pure privacy preferences. These users—unlike the case of environmental production—do not directly impose negative externalities on others with their by-product. The dissemination of

---

[197] Unless the unlikely case takes place where the ratio between the two demand curves is equal to the ratio of the production quantities.

[198] See Heinz Kurz, "Goods and Bads: Sundry Observations on Joint Production, Waste Disposal, and Renewable and Exhaustible Resources," *Progress in Industrial Ecology* 3, no. 4 (2006): 280.

[199] See Heinz Kurz, "Classical and Early Neoclassical Economists on Joint Production," *Metroeconomica* 38 (1986): 1; David Bradford, "Joint Products, Collective Goods, and External Effects: Comment," *Journal of Political Economy* 79, no. 5 (1971): 1119.

personal information, as it increases the probabilities of a privacy breach, should create in rational users an expected cost function for the production of personal information which, when it gets too high, should stop them from continuing to use the product.

What differences does this present with a standard buy and sell scenario where the user sells his personal information in exchange for a product? The main difference is that, due to the reasons explained before,[200] a data protection statute in this context does not have the same effects as those produced in the context of traditional privacy exchanges which were described by the first-generation economics of privacy. This by-product characteristic is able to explain why personal information is produced even in the absence of exclusion rights, and at the same time why there are limits posed on its production.

Picture an agent that consumes a website where his consumption is measured by x (extent of the use of the service). While the agent consumes x he produces y as a by-product, where y is the personal information shared. The good x cannot be consumed separately from y, since information is a by-product of consuming the website: if the internet user spends time in the network, personal information about him will be available to the service providers.

Suppose the ratio between the consumption and the production of the by-product is $y = \alpha x$, where α is constant and $\alpha > 0$. The production of y, in turn, has the costs to the agent $C(y)$ of expected privacy breach and disutility from sharing, where the more information shared, the higher the risk of a privacy breach ($C'(y) > 0$). The data subject's utility from consuming of the web service is $v(x)$, *where* $v'(x) > 0$ and $v''(x) < 0$. Hence, his expected utility function is $U(x, y) = v(x) - C(y = \alpha x)$.

Maximizing the data subject's utility function, $dU/dx = 0$ results in $v'(x) = C'(\alpha x)$. This means that he will limit x (his consumption of the website) to the point where his marginal benefit of consuming the website intersects with his marginal cost of producing information ($v'(x) =$

[200] See sections 2.3.1 to 2.3.4.

$C'(y)$).[201] After this point, the cost of producing y is too high for him. Since x cannot be consumed without producing y, the data subject stops consuming x. Thus, the consumption of the website is determined by the production costs of personal information.[202]

This mechanism is seen, for example, with people that do not have a social network account because of privacy concerns (while they otherwise would like to have one), while the social network could profit from them, and they could profit from using the social network if there was a way for them to use the product without revealing personal information—and receiving non-personalized advertisements.

This scenario is the result of an asymmetric information problem which prevents these users from accessing the product because the service provider does not know the exact privacy sensitivity of its consumers. This problem prevents them from perfectly discriminating their users based on how privacy sensitive they are: they cannot discriminate between consumers based on the shape of their $c(y)$, allowing only some of them to consume the product while producing a smaller amount of personal information ($\alpha_1 > \alpha_2$).

However, social networks are able to partially discriminate data subjects according to their sensitivity by offering them different menus to choose from, which can function as a signaling device. These are different combinations of privacy settings ($\alpha_1 \dots \alpha_i$) and functionality of the website ($x_1 \dots x_i$). This choice allows data subjects to have different degrees of privacy preferences in the product, choosing from the available combinations the one that best satisfies their preferences:

---

[201] A special case would be one in which the marginal cost curve always lays above the marginal utility curve, and hence the two curves do not intersect. This would be the case of people with high pure privacy preferences, who do not share personal information.

[202] This is often the case with environmental economics, with the difference that, in such cases, the by-product is often a bad instead of a good. See Heinz Kurz, "Goods and Bads: Sundry Observations on Joint Production, Waste Disposal, and Renewable and Exhaustible Resources," *Progress in Industrial Ecology* 3, no. 4 (2006): 280.

$\{(x_1, \alpha_1) \dots (x_i, \alpha_1)\}$.[203] Hence, data subjects can choose the combination that gives them the highest utility, creating a separating equilibrium based on their privacy sensitivity.[204]

A very high level of data protection would disallow data subjects to produce some levels of y and, in such way, would restrict the scope of choices of the menu. This would thereby restrict the business model of the web service and reduce data subjects' utility.[205] From this perspective, it is welfare-enhancing for DPL to adopt an approach closer to contract law and focus in enforcing the voluntary choices of the users and the network. An entitlement-based DPL that allows data subjects to trade and in such way gives them freedom of choice regarding privacy preferences, such as the one in place in the EU, accomplishes this task.

2.4.! Alternatives for Protecting the Entitlement

2.4.1.! Protecting privacy with property

Calabresi and Melamed explain that, if law is analyzed from the point of view of efficiency,[206] one can distinguish between three types of protection over entitlements: property, liability, and inalienability.[207] One can ask, under this framework, which of these three is at an abstract level an

[203] For example, Google and Microsoft do this for their email services, and Facebook does so for its social network.
[204] If personal information is not seen as a by-product, then services such as social networks would only have incentives to offer this kind of product differentiation due to the pressure of competition. See Ruben Rodrigues, "Privacy on Social Networks," in *The Offensive Internet*, ed. Saul Levmore and Martha Nussbaum (Cambridge, Mass.: Harvard University Press, 2010), 237.
[205] This high level of protection can be identified with an inalienability rule. This presents another reason to consider that, as it was seen in the last subsection, such a high level of protection reduces the amount of available information.
[206] Although efficiency can only portray one side of law, in the same way that Monet, as excellent as a painter as he was, could only portray one side of the Rouen cathedral. See Guido Calabresi and A. Douglas Melamed, "Property Rules, Liability Rules, and Inalienability: One View of the Cathedral," *Harvard Law Review* 85, no. 6 (1972): 1089.
[207] See Ibid.

efficient mechanism to protect the privacy entitlement in favor of which the previous section argued.

Entitlements protected by a property rule are transmitted only with the consent of the title-holder and in exchange of a price to be determined at the time of bargaining. Those protected by a liability rule, on the other hand, are transmitted without the will of the title-holder and in exchange of a collectively determined price, mainly due to high transaction costs or an actual impossibility of *ex-ante* bargaining. Entitlements protected by an inalienability rule are not subject to transfer, and if the transfer takes place then it should be set back (nullified) if it can, while there should be compensation to the title-holder if it cannot.[208]

The possibility to establish the first of these mechanisms, a property rule, takes us back to the debate described where property was proposed as a protection mechanism that could forbid extracting information from data subjects without their consent,[209] hence protecting their privacy.[210]

In addition, according to what was seen in the last section, this rule would incentivize information production since it would internalize *ex-ante* the externalities of data processing. A property system would allow for a market for personal information in which each data subject can negotiate with firms regarding what uses they are willing to submit their personal information for and for which compensations.[211] By being owners of their

---

[208] See Ibid.

[209] The Data Protection Directive defines consent of a data subject 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." See Directive 1995/46/EC, article 2(h).

[210] See section 2.2.2.

[211] See Kenneth Laudon, "Markets and Privacy," *Communications of the Association for Computing Machinery* 39, no. 9 (1996): 92; Richard Murphy, "Property Rights in Personal Information: An Economic Defense of Privacy," *Georgetown Law Journal* 84, no. 1 (1995): 2381; Lawrence Lessig, "The Architecture of Privacy," *Vanderbilt Journal of Entretainment Law and Practice* 1 (1999): 56; Patricia Mell, "Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness," *Berkeley Technology Law Journal* 11, no. 1 (1996): 26; Lawrence Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books, 1999). pp. 85-90,

personal information, data subjects would be able to extract a larger pay for its release, and would have a larger compensation for the expected privacy costs faced by each information release.

Moreover, the rule would allow for subsequent sells once information is acquired—as with any product where when one buys an item then one can sell it.[212] In such way, it would keep transaction costs low.[213] If companies would have to ask data subjects for permission each time that such information is traded, as an inalienability rule would do, transactions costs would be too high, which would decrease information flow. The ability to protect privacy while not interfering with subsequent sells is therefore a desirable attribute of the property rule.

2.4.2.! Problems of a pure property rule for DPL

However, a pure property rule could also generate new problems in the interaction between data subjects and data collectors and processors: ineffectiveness due to bargaining positions, under-protection of information obtained through data mining, and a moral hazard problem.

First, due to the type of interactions in which privacy policies are typically involved, where data subjects have a take-it-or-leave-it option, it is not clear to what extent a property rule would improve their situation.[214] Under the new regime, they could as well face a take-it-or-leave-it option of using the product and giving their personal information (for which they have a property right) for free, or not using the product at all. In addition, it might be difficult for the average data subject to properly assess the

---

[212] Pamela Samuelson, "Privacy as Intellectual Property?," *Stanford Law Review* 52, no. 5 (1999): 1125.

[213] On the importance of keeping these transaction costs low, see Eli Noam, "Privacy and Self-Regulation: Markets for Electronic Privacy," in *Privacy and Self-Regulation in the Information Age*, ed. Barbara Wellbery (Washington, DC: National Telecommunications and Information Administration, 1997), 21.

[214] In the US, it must be clarified, privacy policies have generally been held not to be contracts in the formal sense. Still, the interaction with privacy policies presents analogies to that of standard form contracts, to the extent that companies present to consumers a take-it-or-leave-it option that is not subject to negotiations.

risks of selling the property right over his personal data.[215] Data subjects generally face difficulties to assess the risks of disclosing, while the need to assess the risks of selling such property rights over information altogether would be even higher.[216]

For these reasons, even if property rules are in abstract a strong protection, they might after all not change the situation for data subjects in a significant way. This derives from the fact that a property rule is a static concept; unlike liability rules, which can impose costs at all moments of the decision-making process, a property rule is satisfied only at the start, allowing the acquirer to forget about potential externalities later on.[217]

Second, information gathered by data mining, which compiles different types of information provided by the data subject to different companies at different times, would not be protected under a property rule. The data subject would have, in the best case, an *ex-ante* compensation for each piece of information released to each data collector, but he would not have an *ex-ante* compensation for the aggregation of the information, which is more valuable and, more importantly for the incentives to generate information, is more potentially harmful.

Taken individually, these pieces of data might not be valuable enough to induce companies and data subjects to bargain over them. For instance, it is possible to buy marketing lists of about a thousand data subjects with information such as their email and whether they are interested in a particular sport, for values around fifty dollars. At the same time, the net worth of Europeans' aggregated personal data has been estimated at 315 billion euros.[218] Data subjects would not incur in risks to

---

[215] See Pamela Samuelson, "Privacy as Intellectual Property?," *Stanford Law Review* 52, no. 5 (1999): 1125.

[216] See Ibid. (adding that. while most objects that are sold can be replaced, one cannot replace personal information once it is disclosed.)

[217] This element has been considered a drawback of property rules, for example, in environmental law for the calculations of carbon dioxide emissions.

[218] See Viviane Reding, "Data Protection Reform: Restoring Trust and Building the Digital Age Single Market," *Speech 13/720 at the Fourth Annual European Data Protection Conference* (Brussels, September 17, 2013).

disclose pieces of their personal data if they are paid very little for each of them while they face a high expected cost for them in aggregate.[219]

Lastly, property rights over personal data could introduce a moral hazard problem. If a data collector gives a data subject a price for his personal information, and that data subject is therefore already compensated, then the data collecting company would have no incentives to incur in costs of care or to moderate levels of activity (data processing) in order to avoid data breaches. Given the externalities of data processing, the data collector would act as an agent of the data subject, with full control over the management of the information—which affects the welfare of the data subject—and incentives to over-process information and under-invest in care, increasing the risk of data breaches *ex-post*.

Moreover, if data subjects are rational, they would anticipate this increase in risk and, consequently, increase the price that they would demand for their personal information in accordance to those increased risks provoked by the moral hazard problem. Even if the market does not unravel, this increment in the value of information produced by the property rule would not necessarily be desirable for the aim of incentivizing it: the increment in price would, in turn, reduce the demand for such information in equilibrium, which would reduce the supply of information to meet that demand. The property rule as a protection mechanism, in this way, would be rendered useless.

If property rules are traditionally suggested for scenarios with low transaction costs, and cyberspace reduces the costs of communications (and therefore the costs of transacting), one could ask why a property rule does not accomplish its goals in this context.

The answer lies in recalling that, for the case of disclosure of personal information, the costs of generating the good are not, as with most goods, material costs of production. Data subjects produce personal information as a by-product, often unwillingly so.[220] The costs of

---

[219] See Amy Kapczynski, "The Cost of Price: Why and How to Get Beyond Intellectual Property Internalism," *UCLA Law Review* 59, no. 4 (2012): 970.
[220] See section 2.3.5.

generating personal information in this context represent the expected cost of a data breach that can derive from such disclosure: the more personal information released, the higher the expected cost of a privacy breach. From this perspective, a strict liability rule makes it easier to define expectations than a property rule.[221] A property rule implies that the data subject has to know the expected value of the data breach in order to ask for an equivalent price and find himself compensated *ex-ante*. On the other hand, under a strict liability rule, in case of a breach the data subject would be compensated *ex-post* with an amount that is able to place him back on his indifference curve.

Privacy breaches, like automobile accidents, involve several potential parties who are unidentifiable ahead of time, often also *ex-post*. For this reason, the costs of protecting one's data are high, even when those of communications are low.[222] In turn, as stated previously, the disincentives for investment in the generation of personal information are dependent on the expected costs of breach—not material costs of the production process itself.[223] For this reason, the transaction costs of protection are more relevant than the transaction costs of communications to set a rule to protect the entitlement. This leads one to consider the possibility to protect data with a liability rule instead.

2.4.3.! Protecting privacy with (strict) liability

A liability rule for personal information, similar to the US privacy tort, would represent a lower level of exclusion than a property rule. Under this rule, consent would not be a previous requirement for the transfer and data subjects would be unable to prevent a company from selling their

[221] It has been argued that liability rules are more efficient than property rules, even without prohibitively high transaction costs, when those transactions costs stem mainly from imperfect information. See Ian Ayres and Eric Talley, "Distinguishing between Consensual and Nonconsensual Advantages of Liability Rules," *Yale Law Journal* 105, no. 1 (1995): 235; Ian Ayres and Eric Talley, "Solomonic Bargaining: Dividing a Legal Entitlement to Facilitate Coasean Trade," *Yale Law Journal* 104, no. 5 (1995): 1027.
[222] See section 2.3.3.
[223] See section 2.3.3.

personal information to others, or even to collect their personal information. Still, they would be compensated if any collection or processing results in harm, for example by leading to identity theft or to the dissemination of embarrassing information. Although this differs from the type of rules that most privacy advocates defend, it is a rule that, if effective, could leave data subjects equally well-off in the event of a privacy breach and in the event of no privacy breach; this is a relevant fact to take into account if one wants to preserve their welfare, and if one wants to establish incentives for them to disclose information.

A liability rule would, first of all, maintain the freedom for subsequent sales which the pure property rule features, thus keeping transaction costs low—this was one of the main attractive features of the property rule. The rule would also avoid the main problems identified for pure property: the ineffectiveness of the rule due to bargaining positions would be solved by the fact that prices in liability rules are defined collectively, the under-protection of information obtained through data mining would be solved by fixing damages in accordance to harm, and the moral hazard problem would be solved by featuring a lower level of exclusion than the property rule. Finally, the rule would present two additional advantages.

One additional advantage is that, in privacy issues, one often has no disutility unless one is aware of the information leak. In those cases in which people consider privacy as a valuable in itself rather than to deceive others (when they have a "pure privacy preference"), then their utility is not reduced until they are aware of the knowledge of such information by other people. Two examples might clarify this point.

On the one hand, one might not want one's insurance company to learn information about one, such as a disease that one might have, because that could raise the premium, and one might not want one's employer to learn about one's traits that make one a less desirable employee, such as a preference for mid-afternoon naps. In those cases one would suffer harm when the insurance company and the employer learn about the information even if one does not know that they learned it. On

the other hand, one might not want one's friends to know about the romantic comedy that one saw last evening, or about role-playing games forums that one frequents online, because one considers these to be embarrassing. In those cases one would not suffer harm if one's friends find out about these activities and one does not know that they did. The reason for this is that harm based on a pure privacy preferences is subjective harm: it refers to a psychological state rather than to factual circumstances that inconvenience. Although this harm should also be taken into account, it does not materialize unless the data subjects is aware of the breach.

This characteristic of privacy disutilities points to liability rules as a well-suited compensation mechanism, as in these cases there would be no cases in which there is a welfare reduction without the knowledge of the entitlement holder that would justify the need for an *ex-ante* compensation mechanism.

The second additional advantage is that, if data subjects are more risk averse than data trading companies—which is likely to happen—then liability rules could be in the interest of both players in the interaction even abstracting from their ability to solve the moral hazard problem.

For data subjects, an *ex-ante* compensation such as the one featured by a property rule would in principle be composed solely by the expected value of the damage, and would not take into account the disutility that a risk-averse data subject would face for the risk. Therefore, a full *ex-post* compensation taking place in the occurrence of an eventuality that leads to damage would be more valuable for them than an *ex-ante* compensation for the expected damage.

In turn, if the compensation is higher than the expected damage to account for the disutility of risk—leaving data subjects indifferent between *ex-ante* and an *ex-post* compensation—then a liability rule would be cheaper for data collectors than a property rule, since the expected cost of the liability rule would equal the expected cost of harm under the most-expensive case of strict liability. This principle would be maintained even if the liability rule leads to levels of overcompensation, as long as such

compensation is, in expectation, lower than the equilibrium price of the property rule determined by the data collector's willingness to pay for the information and the data subjects' willingness to accept—which is likely to happen as long as data subjects are risk averse.

Lastly, one can ask which type of liability rule is the most appropriate for cases of data protection. These cases represent unilateral accidents, where the potential tortfeasors (data collectors and data processors) have an incidence over the probability of an accident (data breach) almost exclusively. The protection mechanisms in which data subjects can engage after the information is disclosed have a negligible influence on the probability of data breaches compared to the security measures which data processors can implement. After the information is disclosed, it leaves the sphere of control of the data subject, rendering him unable to control it. In addition, in these cases both the care and activity levels of the potential tortfeasors are relevant for the probability of the accident. The level of database security (care level) and the number of data transfers performed by data collectors and data processors (activity levels) directly affect the probability of data breaches. Therefore, it seems that, among the different possible liability rules, a strict liability rule would induce most efficiently appropriate levels of care and activity.[224]

2.4.4.! Approaching causal uncertainty

The central drawback of this liability rule is the high level of information costs that it would present, which might turn it inapplicable independently

[224] For a proposal along these lines suggesting strict liability for identity theft, see Chris Jay Hoofnagle, "Internalizing Identity Theft," *UCLA Journal of Law and Technology* 13 (2009): 1. Similarly, the application of a negligence rule to databases for personal information leakage has been attacked on the basis that there would be uncertainty surrounding the level of due care, leading databases to overinvest in care. See Danielle Citron, "Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age," *Southern California Law Review* 80 (2007): 241. However, it should be noted that a negligence rule with an ambiguous standard would lead potential plaintiffs to overinvest in care only up to the investment level that they would have under a strict liability rule. This is a socially efficient level of care, particularly for unilateral accidents, since it fully internalizes the externalities imposed.

of its theoretical desirability. If a data subject faces harm due to a privacy breach (for example, his identity is stolen by someone else) it might not be clear which company or which group of companies that held his personal information suffered a data breach which, in turn, led to such outcome. Causality could be costly, if not impossible, to prove. This leads to the question of whether this difficulty could be solved by using a model of causal uncertainty with multiple tortfeasors, as it is sometimes done with cases of environmental harm where responsibility is apportioned inversely to levels of caution.

Causal uncertainty is a challenge for the inclusion of several new types of responsibility within tort law in which it is difficult to determine the source of damage, such as environmental harm and medical malpractice.[225] To some degree, one could find data protection to be analogous to these categories. In this context, there are two types of causal uncertainty problems. The first is whether any of the defendants was the cause of the plaintiff's harm, and the second (conditional on the first) is who among them hurt the plaintiff and by how much.[226]

When the first question is solved, and the causal uncertainty present appears for the second, then the uncertainty is reduced to matching each victim with his tortfeasor.[227] In these cases, market-share liability serves as a solution under the assumption that the marginal increase in the risk of harm created by each defendant is proportional to its presence in the market. Under this assumption, the marginal increase of risk received by the potential victims will be equal to the market share of the firm. For the assumption to be verified, it will be necessary that potential tortfeasors have similar care levels and that they have levels of activity proportional to their market share—or that these variables compensate each other.

---

[225] See Marcel Kahan, "Causation and Incentives to Take Care Under the Negligence Rule," *Journal of Legal Studies* 18, no. 2 (1989): 427.
[226] See David Rosenberg, "The Causal Connection in Mass Exposure Cases: A 'Public Law' Vision of the Tort System," *Harvard Law Review* 97, no. 4 (1984): 849.
[227] See Saul Levmore, "Probabilistic Recoveries, Restitution, and Recurring Wrongs," *Journal of Legal Studies* 19, no. 2 (1990): 691.

This assumption seems to have underlied the leading case *Sindell v. Abbott Laboratories*, which established market share liability.[228] In the case, market share liability alleviated the victims from the burden of proving who among the producers of the drug (who harmed them in aggregation) harmed each of them individually. This also seems to be an underlying assumption in cases of recurring harms between parties.[229] Even though these cases present some degree of uncertainty on the identity of the tortfeasor for each victim, the uncertainty of tortfeasors in aggregation is low since the marginal increase on the risk of damage on the entire set of plaintiffs is considered to be proportional to market-share:[230] the more DES a company sells, the more women it harms with it.

This assumption, however, is not always valid for companies collecting and processing personal data. We know that consuming DES has a negative impact on women's health, and that this effect does not present a large variance. On the other hand, it is not always the case that the trade of personal data has a negative impact on data subjects' well-being. The trade of information is sometimes harmless and, when it is not, the possibility that it presents of creating harm largely depends on care levels.

This illustrates that the type of uncertainty problem which often appears in the context of information technology is not the second but the first. The problem has been addresses by laws requiring companies to notify data subjects in cases of data breach, such as the one recently passed in the US,[231] which marginally reduce the information problem. Still, it is sometimes the case that upon fraud or identity theft the victims

---

[228] In the case, pregnant mothers used a diethylstilbestrol-based drug (DES) to prevent miscarriage, which caused their daughters (later on known as "the DES daughters") to develop cancer twenty years later. In the DES cases this assumption is reasonable because all defendants engaged in an identical activity. See Glen Robinson, "Multiple Causation in Tort Law: Reflections on the DES Cases," *Virginia Law Review* 68, no. 4 (1982): 713.

[229] See Saul Levmore, "Probabilistic Recoveries, Restitution, and Recurring Wrongs," *Journal of Legal Studies* 19, no. 2 (1990): 691.

[230] See William Landes and Richard Posner, "Multiple Tortfeasors: An Economic Analysis," *Journal of Legal Studies* 9, no. 3 (1980): 517; William Kruskal, "Terms of Reference: Singular Confusion about Multiple Causation," *Journal of Legal Studies* 15, no. 2 (1986): 427.

[231] See *Personal Data Notification and Protection Act*, passed on 12 January 2015.

cannot know how their data were leaked, and by whom. What is more, it can be that the set of necessary data were not leaked from one single place but that elements of that set were mined from different sources, making an efficient apportioning of responsibility increasingly difficult.[232]

Additionally, in the context of information technology there are several companies that have sizeable datasets and few assets. This obstacle could point to the inapplicability of market share liability while potentially leaving some scope for another proxy to be used for apportionment, such as the amount of data collected or data traded. This alternative, however, would lead to frequent solvency problems: there are several websites that have an extremely small market share compared to data giants, but they still process personal data and would be unable to fully compensate people for their losses absent insurance. These companies could be judgment-proof.

From a legal point of view, there is also the obstacle that one is generally not considered responsible for the criminal actions of third parties. If the problem was caused by a criminal who stole data from a data collector, or a criminal who tricked a data processor (such as a credit card company) into obtaining a victim's personal information (such as his credit card details), the company would argue that data collection, even if it eventually resulted in identity theft, did not cause that identity theft—the thief did. For these reasons, it seems that a pure liability rule is also not the optimal solution to protect the entitlement.

2.5.! A Proposal for Explaining DPL

2.5.1.! Setting an intermediate level of protection

The central lesson that one can draw from the previous section is that DPL should set a level of exclusion larger than a liability rule, but lower than a property rule—and that an inalienability rule. The three traditional rules

[232] See Chris Jay Hoofnagle, "Internalizing Identity Theft," *UCLA Journal of Law and Technology* 13 (2009): 1.

in their pure forms would present either theoretical or practical problems that could render them useless as a protection mechanism. This leads to the discussion of which aspects of these rules to maintain in DPL.

The rationale of incentivizing disclosure is used canonically in areas of law such as professional secrecy. Most societies want to ensure that people are able to convey as much information as possible to their lawyers, psychologists and priests in order to allow them to perform their jobs appropriately. For that reason, they enact rules stating that the members of these professions cannot share with others the information that is shared to them in such context, thus guaranteeing trust.[233] A rule analogous to absolute data protection, for example stating that the members of these professions cannot learn the information in the first place, would be too protective and would impair the aim that the rule has. In turn, a rule that allows them to disclose everything their clients say, analogous to no data protection, would make their clients disclose less, if anything at all.

This has been the justification behind the attorney-client privilege, particularly in the US.[234] The privilege is not considered to be a right of the attorney but one of the client, who can decide whether to raise it or waive it, and it has been explicitly called in occasions a rule of privacy.[235] The extent of the privilege is that attorneys cannot disclose without the permission of their client, in a narrow interpretation,[236] any information that a client conveyed in confidence with the purpose of seeking legal advice and, in a broad interpretation,[237] any communication between them and their clients. Its justification is that an attorney can only give adequate legal advice if he has learned of all relevant information, and the

---

[233] See Ronald Allen et al., "A Positive Theory of the Attorney-Client Privilege and the Work Product Doctrine," *Journal of Legal Studies* 19, no. 2 (1990): 359.
[234] The original justification appears in Wigmore's leading book on evidence. See John Wigmore, *Wigmore on Evidence*, 1940. §2292, and cited case law.
[235] See Geoffrey Hazard, "A Historical Perspective on the Attorney-Client Privilege," *California Law Review* 66, no. 5 (1978): 1061.
[236] See US Federal Rules of Evidence. Rule 501.
[237] See American Bar Association, *Model Rules of Professional Conduct* (Chicago: American Bar Association, 2006). Rule 1.6.

client might withheld that information if the privilege did not exist.[238] Although without a direct instrumental justification, the privilege exists with equal prevalence in Europe, having a particularly wide scope in Germany and France.[239]

The attorney-client privilege, although analogous in the sense that it aims to stimulate disclosure, might not be tailored enough to apply directly to DPL. It does not present the problematic of the future use of the information, and particularly of the secondary use of information and of data transfers, which are essential to the public good characteristic of personal information.

More prominently, one of the main branches of law that displays this kind of combination between property rules and liability rules is copyright.[240] Copyright law, simultaneously, tackles the public good characteristics of information and its secondary use; it responds to the non-excludability characteristic of information and to the need to foster it with the creation of an entitlement to exclude others from certain uses, while at the same time it attempts to maintain low transaction costs for the transfer and future use of the information.[241]

Concretely, copyright law reserves for authors some rights of the bundle of rights which full property represent, mainly the right to copy.[242] DPL, from the economic perspective in which it was presented, has

---

[238] See Ronald Allen et al., "A Positive Theory of the Attorney-Client Privilege and the Work Product Doctrine," *Journal of Legal Studies* 19, no. 2 (1990): 359. See also Edna Epstein, *The Attorney Client Privilege and the Work Product Doctrine* (Chicago: American Bar Association, 2001).

[239] See Edward Imwinkelried, "The New Wigmore: An Essay on Rethinking the Foundation of Evidentiary Privileges," *Boston University Law Review* 83 (2003): 315.

[240] See Trotter Hardy, "Property (and Copyright) in Cyberspace," *University of Chicago Legal Forum* 1 (1996): 217.

[241] See Stanley Besen and Leo Raskind, "An Introduction to the Law and Economics of Intellectual Property," *Journal of Economic Perspectives* 5, no. 1 (1991): 3.

[242] See Ibid. As manifestations of copying, copyright law traditionally grants five rights: (i) the right to reproduce, (ii) the right to prepare derivative works, (iii) the right to distribute copies, (iv) the right to perform, and (v) the right to display it publicly. For example, in the US this is contemplated in title 17, section 106 of the US Code.

relevant analogies with copyright inasmuch as they both present some level of exclusion but not a pure property rule.[243]

2.5.2.! DPL and Copyright: common grounds

Copyright traditionally serves two interests: creation and dissemination of content; the tradeoff between these two has been called the incentive-access paradigm.[244] Establishing a price which is higher than the marginal cost of distribution (which in case of digitalized information is zero) generates the static effect of suboptimal dissemination; this, as it was seen, is also the case for DPL.[245] The static effect is weighted, in turn, against the dynamic effect of incentivizing the generation of new products.[246] The protection for authors is mainly given by the property characteristics of copyright, which imply a compensation, while the attempt to maintain dissemination leads to the (scarce) liability characteristics of copyright. It seems possible, from this perspective, to take applicable lessons from copyright to DPL.

From the perspective proposed in the previous section where DPL is an instrument for incentivizing the creation of information, copyright law and DPL have a similar justification. Moreover, both branches of law have a similar system of combining elements from property rules and liability rules. Neither copyright law nor DPL traditionally include inalienability rules.[247] Evaluating the common aspects with copyright law can aid, from

---

[243] See Trotter Hardy, "Property (and Copyright) in Cyberspace," *University of Chicago Legal Forum* 1 (1996): 217.

[244] See Joseph Liu, "Copyright and Time: A Proposal," *Michigan Law Review* 101, no. 2 (2002): 409; Alireza Naghavi and Günther Schulze, "Bootlegging in the Music Industry: A Note," *European Journal of Law and Economics* 12, no. 1 (2001): 57; Glynn Lunney, "Reexamining Copyright's Incentives-Access Paradigm," *Vanderbilt Law Review* 49 (1996): 483.

[245] See section 2.3.4.

[246] See Stanley Besen and Leo Raskind, "An Introduction to the Law and Economics of Intellectual Property," *Journal of Economic Perspectives* 5, no. 1 (1991): 3.

[247] The only provision of the Data Protection Directive that allows for an inalienability rule its article 8(2)(a), which states that MS can forbid the processing of sensitive data even if the data subject gave his consent.

this perspective, in understanding how DPL sets its intermediate level of exclusion.

Regarding the property characteristics of copyright law, authors holding copyrighted work are entitled to exclude others from copying their work. Simultaneously, they are able to issue licenses for the use of their work, partially alienating their exclusion right, or to request injunctions for the breach of such exclusion.[248]

Copyright holders can either transfer copyright in its entirety or, more frequently, grant a license for any of these rights in exchange for a royalty. Under full property, when an entitlement is transferred the new owner can do with it what he desires; under copyright, on the other hand, one usually gives permission for a particular use.

In this regard, licenses under copyright law are analogous to the purpose limitation principle under DPL. Both of them specify the objective for which the information can be used, and forbid its use for other purposes; they are an element of a property rule within the system, where the owner of the entitlement has the right to exclude others from uses different than the one specified.

A second common ground is that both under copyright (or, more generally, in intellectual property law) and DPL, each generation of information should ideally have a different protection in order to incentivize it without overprotecting it, but it is not possible for the law to account for all the nuances. An ideal intellectual property law in a world with perfect information would feature a different scope and breath for each creation, but as this is not possible, the law has only some categories that aim to be functional on average. Namely, a standard protection for patents and a standard protection for copyrighted works.

DPL, in this regard, faces the same issue, where the externalities for data subjects are different in each case, and therefore the expected cost of disclosing information is different for each case. Although it would be

[248] See William Cornish, David Llewelyn, and Tanya Aplin, *Intellectual Property: Patents, Copyright, Trade Marks and Allied Rights* (London: Sweet & Maxwell, 2013). Chapter 9.

desirable to completely de-homogenize information and issue individual rules, this is not possible, so DPL features few distinctions that aim to work on average, such as the distinction between sensitive and non-sensitive information.

Regarding the liability characteristics, authors sometimes face compulsory licenses, and have to accept fair use.[249] While compulsory licenses tend to be specific and limited, fair use is a central trait of copyright law.[250] As such, while it could marginally reduce the number of inventions being made, it represents an advantage for the dissemination of copyrighted works, balancing the incentive objective and the access objective mentioned.[251]

Like liability rules under the Calabresi-Melamed framework, fair use is traditionally justified based on high transaction costs. Specifically, fair use is motivated by the high transaction costs which would be otherwise implied in negotiating and monitoring the uses that it protects.[252] For example, one can quote a scientific work literally without asking the author for permission, because doing so each time that one wants to quote a published work would produce high transaction costs, and such citation does not harm the economic interest of the author since it does not reduce the expected amount of copies sold. If the quotation is large enough to cover the whole work, on the other hand, it would harm his economic interest, and the law requires permission to do so.[253] It would be

---

[249] See Trotter Hardy, "Property (and Copyright) in Cyberspace," *University of Chicago Legal Forum* 1 (1996): 217.

[250] This is particularly so in the United States. See title 17, section 107 of the United States Code.

[251] See Pierre Leval, "Toward a Fair Use Standard," *Harvard Law Review* 103, no. 5 (1990): 1105; Glynn Lunney, "Fair Use and Market Failure: Sony Revisited," *Boston University Law Review* 82 (2002): 975.

[252] See Wendy Gordon, "Fair Use as Market Failure: A Structural and Economic Analysis of the' Betamax' Case and Its Predecessors," *Columbia Law Review* 82, no. 8 (1982): 1600.

[253] Fair use finds its scope defined in the uses of the product that do not significantly affect the economic interests of the owner, in order to not deter creation exceedingly. See Leo Raskind, "A Functional Interpretation of Fair Use: The Fourteenth Donald C. Brace Memorial Lecture," *Journal of the Copyright Society* 31 (1983): 601; Richard Posner, "When Is Parody Fair Use?," *Journal of Legal Studies* 21, no. 1 (1992): 67.

unjustified from an economic perspective to ban the use of the product in those contexts where such ban would not induce a negotiation, and so the ban would generate a loss by leaving the author uncompensated and the user without using the good. Fair use, in this sense, is a tool for enhancing the diffusion aspect of copyright law.[254]

The mirror argument can be made for DPL. Demanding individual authorizations from the data subject for each secondary use of the information would significantly elevate transaction costs, especially given that personal information is valuable in aggregate and that there is a high number of data subjects that are involved in most cases of data processing. In order to avoid this consequence, DPL presents some features of a liability rule within the scope of the purpose limitation principle, by not requiring consent for every interaction.[255]

2.5.3.! DPL and Copyright: structural differences

Simultaneously, there are structural differences between copyright law and DPL that justify differences in their regulatory approaches from an economic perspective.

One of these differences is that the cost of creating a copyrighted product does not depend on its use *ex-post*, while the cost of disclosing personal information fully depends on the use that it is given after the exchange, since this use changes the expected costs of harm from disclosure. For most—although not all—copyrighted works, there are two costs involved in the artistic creation: the cost of creating the work and the cost of creating copies.[256] For disclosing personal information under DPL, however, the only cost is the expected cost of harm that people have when releasing information (instrumental value of privacy), together with the disutility of the information release in itself (pure privacy preference).

---

[254] See Wendy Gordon, "Fair Use as Market Failure: A Structural and Economic Analysis of the' Betamax' Case and Its Predecessors," *Columbia Law Review* 82, no. 8 (1982): 1600.
[255] See article 7(b) to 7(f) of Directive 1995/46/EC.
[256] See William Landes and Richard Posner, "An Economic Analysis of Copyright Law," *Journal of Legal Studies* 18, no. 2 (1989): 325.

While for both cases, for the good to be produced the expected return must exceed the expected cost, only for one of them (DPL) such cost is dependent on the *ex-post* incentives to adjust levels of care and levels of activity. This justifies a stronger incidence of liability rules in DPL than in copyright, since these rules maintain *ex-post* incentives better than property rules.

A second relevant difference between copyright and DPL from this perspective is the difference on how the value of the information changes over time. The limited duration of copyright responds to its decreasing marginal utility (prospective authors who the law wants to incentivize will discount payoffs to present value) paired to its increasing marginal cost (mainly due to tracing the origins of old copyrighted works).[257] Since old information under DPL tends to be less harmful for data subjects than new information, DPL seems to present the characteristic of decreasing marginal utility of information for the creator. However, regarding marginal costs, unlike copyrighted work personal information would turn less valuable over time also for others. In the case of DPL, the value of personal information decreases at a slow rate for data subjects, while it quickly decreases in value its commercial uses as it becomes outdated.[258] Moreover, due to the higher incidence of liability rules in DPL compared to copyright, there is no need to trace the information to allow for secondary use once it is transferred.

This can explain the different extension of the time limit under both branches of law. Policy debates in DPL have gone in the opposite direction of suggesting time limits for rights, proposing increased rights for old information.[259] However, although not explicitly, DPL also contains a time limit for its entitlements: the death of the data subject, since data protection rights, unlike copyright, are not inheritable.[260] After the death

---

[257] See Ibid.

[258] For an example of this, see Costeja's claim in *Google v. Spain*, in section 4.3.1 below.

[259] An example of this is the right to forget, described in section 4.1 below.

[260] See Edina Harbinja, "Does the EU Data Protection Regime Protect Post-Mortem Privacy and What Could Be the Potential Alternatives?," *SCRIPT-Ed* 10, no. 1 (2013): 19. (arguing that establishing a post-mortem protection would be compatible with the current system.)

of the data subject, personal information has little value for his inheritors on average, which justifies its non-inheritability even within the tendency of giving further protection to older information.

Based on these considerations, it seems that the objection that protecting personal information with an analogous system to copyright would ignore that both fields are based on different justifications is, to some extent, unjustified.[261] Simultaneously, the branches of law do present some structural differences from an economic perspective that can explain why DPL is not directly subsumed under copyright law.

These considerations point to an economic justification of having within DPL a similar system to copyright with a weakened property rule, where not all rights from the bundle (as property is often characterized) are reserved, but only some of them are. In the same direction as creative commons, which has proposed a successful model of protecting information in the form of creative inventions with a lower level of exclusion than traditional copyright law, one can discuss which rights from the bundle are worth keeping to protect information in the form of personal data.

2.5.4.! Relevant technological characteristics to shape DPL

The technological characteristics of data exchanges have elements that, if taken into account, can inform policymakers into designing better regulations from an economic perspective. From them, one can draw additional considerations to aid in determining such intermediate level of exclusion. The elements for these purposes are three: on the supply side, the generation of the information, and on the demand side, its use and the externalities that can derive from it.

On the supply side, in order to incentivize information one should distinguish how it is created. Copyright's property characteristics, it was seen, attempt to prevent free-riding of the authors' expression, hence

[261] For a representative version of the claim, see Pamela Samuelson, "Privacy as Intellectual Property?," *Stanford Law Review* 52, no. 5 (1999): 1125.

internalizing the positive spillovers.[262] If the same rationale is applied to DPL, then some types of data need to be protected more than others.

Concretely, a higher level of protection is justifiable, from this perspective, for information that had consent as a basis for processing.[263] This is analogous to the economic rationale of copyright law of protecting expression but not ideas, because (i) ideas expressed by others is information which had a high input from someone else and (ii) protection of ideas would be too wide, and it would likely compensate creators beyond their costs and (iii) this would elevate transaction costs.[264] Only information which had consent as a basis for processing fits within the peer-to-peer system under which data subjects produce it according to the degree in which their expected costs of doing so are compensated; therefore, only this type of information falls under the argument that it should be given a higher level of protection in order to incentivize its generation.[265]

For example, Google Earth has significant marginal costs of gathering information—by taking pictures across the planet—while Google+ and other social networks do not, since they form part of the peer-to-peer system where people surrender information voluntarily. Both products fall within the same rules under European DPL, but Google Earth's methods of gathering information are more analogous of those that are dealt with in traditional privacy law; they are closer to the automatic photo camera that motivated Warren and Brandeis' article than to those of the Web 2.0 that motivated the GDRP. Then, if one wants to incentivize information generation, data subjects' privacy should have a higher level of protection for Google+ than for Google Earth.

From this perspective, the under-protection of privacy issues related to data mining which was mentioned as a drawback of the property rule could, after all, have welfare-enhancing elements. Data mining

---

[262] See William Landes and Richard Posner, "An Economic Analysis of Copyright Law," *Journal of Legal Studies* 18, no. 2 (1989): 325.
[263] See article 7(a) of Directive 1995/46/EC.
[264] See Ibid.
[265] See sections 2.3.3 and 2.3.4.

implies costs of assembly for the data miner, who after such process generates new information through the synergies of the pieces of information used. If personal information obtained with data mining was granted a lower level of protection than personal information acquired in its entirety, then DPL would be incentivizing the generation of new information via data mining as well.

This leads to the more general question of who owns, under the property elements of DPL, information that was generated by someone but refers to someone else. Under current DPL, to the extent that it features property characteristics, the initial owner of the information is always the data subject: the person whom the information is about. In order to generate incentives for the creation of information, however, some property interests should be granted to the creator of the information also under the scenarios where that person is not the same as the person to whom the information refers. This person would have a different cost function than data subjects who disclose information (for him, personal information would not be a by-product, and the costs associated with it would not be related to expected privacy breach) but, inasmuch as DPL serves the interest of incentivizing information, the costs of generating such information should be compensated in order to incentivize its disclosure as well.[266]

Parallels could be made in this regard to how intellectual property assigns interests. For instance, rights over photographs are assigned to the author (the collector of information) as opposed to the person photographed, and he is entitled to make use of it within the limits of fair use (in civil law countries, within the exceptions and limitations of copyright) without the consent of the person who was photographed. This rule incentivizes the generation of photographs (which are one kind of information) because it allocates the entitlement to he who needs to make the larger marginal investments for the photograph to be generated.

[266] This property interests would be relevant, for example, for journalism. At a more general level, this principle would play a role in maintaining freedom of expression within DPL.

From the demand side, one should distinguish what uses can be made with the information, since not all types information have equal social weight. There are differences in the social utility which is derived from information than can be solely used for marketing (and might represent, individually, a low benefit for the company) and information that can be used for research regarding public health or the prevention of crime.

Clearly, it would be impossible for DPL to individually assess each unit of information to provide a tailored level of protection. However, a plausible heuristic to approximate the social value of the use of each unit of information could be whether its use is for a public good or for a private interest. A centralized rule such as a liability rule might perform poorly at making these distinctions, while a property rule might be able to do so since it determines the price in a decentralized manner. European DPL, in turn, takes this distinction into account to some degree, incorporating exceptions for freedom of expression,[267] research,[268] and healthcare,[269] where the data subject has a lower level of protection.

Regarding externalities, the basis of disclosure turns again relevant; from the point of view of revealed preferences, it is arguably the case that information that is not revealed by data subjects is likely to present larger externalities for them. There could be, from this perspective, a self-selection of information where information that is not disclosed when it could have presents higher risks due to pure privacy preferences. However, given that personal information is a by-product it seems that this is not always the case: there could also be pieces of information that a data subject did not have incentives to disclose, but that do not imply for him particularly high externalities. In the example given before, maybe he does not care about disclosing his location data, but he takes no utility from fitness applications.

[267] See article 9 of Directive 1995/46/EC.
[268] See articles 6(1)(b), 6(1)(e), 11(2), 13(2), and 32(3) of Directive 1995/46/EC.
[269] See article 8(3) of Directive 1995/46/EC.

A better indicator than the basis for processing to determine the level of externalities is the type of information disclosed. There are differences in terms of privacy risks between sensitive information and non-sensitive information, and between online information and offline information. From this perspective, it would be reasonable to set a presumption that non-disclosed sensitive information belongs to the self-selection mechanism and is therefore potentially harmful, while non-disclosed non-sensitive information could not have been disclosed yet for lack of incentives to do so.

Both of these elements, and to some extent the final presumption regarding the differences between undisclosed sensitive and non-sensitive information, are present in the European data protection framework. DPL gives a special protection to sensitive information, which mainly consists in the rule that, unlike other kinds of information, it can only be processed with the basis of consent.[270] Non-disclosed sensitive information, in this way, has a protection which is closer to a property rule.

2.6.! Fostering Information with Data Protection

This chapter has shown that, as with professional secrecy for lawyers, psychologists and clerics, and as the case of copyright law, a certain level of data protection can induce more disclosure, meaning more generation of information. More concretely, the relationship between data protection and amount of information available seems to form a concave function, where either no data protection at all or maximum data protection reduce the amount of information available. Hence, from a total-welfare perspective, irrespective of human rights considerations, a right to privacy within information technology law can be seen as desirable inasmuch as it increases information disclosure.

Given the argument of the chapter, one might ask why one sees information exchanges also without the proposed protection. The answer to that doubt lies in seeing personal information traded in the context of data

[270] See article 8 of Directive 1995/46/EC.

mining and social networks as a good which is a by-product of a consumption activity, hence having a certain level of production also absent direct incentives to produce.

This leads to the question of which rule can protect this entitlement an efficient way. The article has argued that an efficient data protection system should present a higher level of exclusion than a liability rule and a lower level of exclusion than a property rule. Moreover, evaluating the similarities and differences between DPL and copyright, it becomes apparent that the level of exclusion or propertization for DPL should be lower than for copyright law.

The exact level of exclusion desirable is, ultimately, a value judgment.[271] However, some precisions can be made. From an economic perspective, DPL should take into account (i) who incurred in costs to generate the information, (ii) the social benefits that can derive from the use of such information, and (iii) the size of the expected externalities of its use for data subjects due to the type of information involved.

This considerations allow to evaluate whether DPL, at a general level, is efficient. The rationale of European DPL, in accordance with the considerations made, gives data subjects a certain level of exclusion, but it is not based on an idea of full property, and it would be problematic to assert that these rights constitute a full property right.[272] DPL creates segments of proprietary legal entitlements without creating a full property right. DPL seems to have evolved by enhancing data subjects' entitlements over their personal information, it presents large similarities with the protection system for copyrighted works, and where it presents a difference

---

[271] Similarly, it has been said for copyright that, due to the social values that are involved, "economic analysis can tell us what would happen if we make certain policy decisions. It cannot tell us what policy decisions we should make." Stan Liebowitz, "Is Efficient Copyright a Reasonable Goal?," *George Washington Law Review* 79, no. 6 (2011): 1692.

[272] See Vera Bergelson, "It's Personal But Is It Mine? Toward Property Rights in Personal Information," *UC Davis Law Review* 37 (2003): 379; Randolph Sergent, "A Fourth Amendment Model for Data Networks and Computer Privacy," *Vanderbilt Law Review* 81 (1995): 1181. See also Pamela Samuelson, "Privacy as Intellectual Property?," *Stanford Law Review* 52, no. 5 (1999): 1125. 1131 (together with cited case law).

it finds an explanation either in the different incentives or due to the technological imperative of DPL. In this way, European DPL seems justifiable from an economic perspective.

In addition, these considerations allow to formulate general policy suggestions to shape this branch of law. Current European DPL seems to incorporate the considerations made regarding the social use and the expected externalities of information, while it does not incorporate differences regarding the source of information. If it did, one should expect from the arguments exposed here that it would generate a higher degree of information flow.

3.!Informational Privacy within Rational Choice Theory

3.1.! The Value of Privacy

In agreements that internet users conclude with some websites and service providers—normally called "privacy agreements" or "privacy policies"—, they are allowed to use a certain product and, as a side-product,[273] they allow the company in exchange to profit from the personal information collected through the use of that product, which is utilized for targeted advertising. While technically the use of the product is free, from an economic perspective the price they pay for it is the aspect of their privacy they relinquish.

Social networks are a good example of this. Facebook users, for instance, receive a free account that they use to communicate with their peers or for leisure, and while doing so they reveal personal information about themselves. This information ranges from basic information such as their gender and age up to very personal information such as whom they are currently dating, where they travel and what movies they like to watch. With 850 million users that provide this information periodically the company is worth around 100 billion dollars because of the possibilities it presents for behavioral advertisers.

A first approximation to this interaction would suggest that these consumers (hereafter data subjects) will disclose the amount of information for which their marginal cost of disclosure equals their marginal benefit for the use of the product. In such way—one could conclude by applying the first stream of literature in the economics of privacy—the market would allocate data subjects' personal information to their highest valuer.[274]

With the rise of these products, however, a series of complaints have been made both by consumers and consumer associations that state

---

[273] See section 2.3.5.

[274] See Richard Posner, "The Right of Privacy," *Georgia Law Review* 12, no. 3 (1978): 393; Richard Posner, "The Economics of Privacy," *The American Economic Review* 71, no. 2 (1981): 405; George Stigler, "An Introduction to Privacy in Economics and Politics," *Journal of Legal Studies* 9, no. 4 (1980): 623; Jack Hirshleifer, "Privacy. Its Origin, Function and Future," *Journal of Legal Studies* 9, no. 4 (1980): 649.

that their privacy is not being properly protected in the online domain.[275] Similarly, people have declared in surveys that they place a very high value on their privacy, while in incentivized experiments they disclose their personal information for little compensation. This behavior is known as the "privacy paradox."

The privacy paradox is a phenomenon that indicates that there is in fact a different incentive structure between internet data collection and processing and the traditional privacy problems long addressed by law. This new incentive structure could justify a different regulation for the former.[276] As it is clear, however, an answer on which type of regulation is appropriate stems not from the paradox itself but from the explanation of its incentive structure.

The main explanation provided so far for the privacy paradox is that data subjects have cognitive biases,[277] and in particular they display self-control problems and thus they hyperbolically discount.[278] This chapter argues that the privacy paradox, when examined closely, might after all be not an amalgam of behavioral biases but instead an uncertainty problem. The question it asks is then: is it possible to provide an explanation for the privacy paradox within a rational-choice framework?

The next section reviews the experimental findings that confirm the existence of a paradox in data subject's behavior. Section 3.3 then provides the standard explanation for this paradox together with an alternative explanation. Section 3.4 discusses their robustness to explain the paradox.

---

[275] See Patricia Norberg, Daniel Horne, and David Horne, "The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors," *Journal of Consumer Affairs* 41, no. 1 (2007): 100.

[276] For example, the much-debated right to be forgotten. It will be seen in section 3.4 that the privacy paradox is mainly a flexibility problem, and section 3.5.1 will explain that the right to be forgotten increases flexibility for data subjects.

[277] See Alessandro Acquisti, Leslie John, and George Loewenstein, "What Is Privacy Worth?," *Journal of Legal Studies* 42, no. 2 (2013): 249.

[278] See Alessandro Acquisti, "Privacy in Electronic Commerce and the Economics of Immediate Gratification," in *Proceedings of the Fifth Association for Computing Machinery Conference on Electronic Commerce*, ed. Jack Breese, Joan Feigenbaum, and Margo Seltzer (New York: Association for Computing Machinery Press, 2004), 21.

Section 3.5 introduces the normative implications of this argument. Section 3.6 concludes the chapter.

3.2.! The Privacy Paradox

3.2.1.! Inconsistencies in privacy valuations

Part of the experimental literature on the topic addresses the question of how much data subjects really value their privacy in view of the mentioned paradox.

The earliest studies in the topic show the inconsistency between data subjects' declared concern for privacy and their actual behavior online.[279] The study grouped participants according to their own declared privacy concern and discovered that, when participating in an online shopping simulation, there was no significant difference between the groups regarding the amount of personal information revealed.[280]

The same finding can be found in other experiments, which show that privacy concerns announced by subjects prior to the experiment are inconsistent with shopping behavior during the experiment.[281] It was also shown that privacy concerns of experimental subjects are a weak predictor of membership and of the amount of information disclosed through social networks.[282] In an experiment where almost 90% of respondents of a survey declared that they have a high concern about their own privacy,

---

[279] See Sarah Spiekermann, Jens Grossklags, and Bettina Berendt, "E-Privacy in 2nd Generation E-Commerce: Privacy Preferences versus Actual Behavior," in *Proceedings of the Third Association for Computing Machinery Conference on Electronic Commerce*, ed. Michael Wellman and Yoav Shoham (New York: Association for Computing Machinery Press, 2001), 38.

[280] This included information such as: in which occasions the subject takes photos, what he does with his pictures, what are his motivations for taking pictures, how photogenic he is, and how conceited he is. See Ibid.

[281] See Bettina Berendt, Oliver Günther, and Sarah Spiekermann, "Privacy in E-Commerce," *Communications of the Association for Computing Machinery* 48, no. 4 (2005): 101.

[282] See Alessandro Acquisti and Ralph Gross, "Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook," in *Proceedings of the Sixth Workshop on Privacy Enhancing Technologies* (Cambridge: Robinson College of Cambridge University, 2006), 1.

again almost 90% of these respondents accepted to put full name and home address under risk of disclosure in exchange for a loyalty card.[283]

Still, data subjects have been shown to respond to monetary incentives regarding privacy, and particularly regarding the avoidance of secondary use, improper access, and error, even if the willingness to pay was low.[284] In addition to their willingness to pay, data subjects have been shown to respond to privacy concerns by avoiding behaviors that deviate from social norms, which have been shown to be more privacy-sensitive.[285]

In more recent studies, data subjects' valuations also display a gap between willingness to pay to protect information and willingness to accept a certain proposal to sell information.[286] In a survey, most participants under a first treatment were not willing to pay one dollar to prevent behavioral advertising, while under a second treatment most participants were not willing to accept one dollar to allow for behavioral advertising.[287] In an experiment, subjects were either asked how much money they were willing to pay to protect their otherwise public personal information, or how much they would be willing to accept to allow that information to become public. The average willingness to accept was five times higher

---

[283] See Alessandro Acquisti and Jens Grossklags, "Privacy and Rationality in Individual Decision Making," *Institute of Electrical and Electronics Engineers Security and Privacy Magazine* 3, no. 1 (2005): 26.

[284] See Il-Horn Hann et al., "Overcoming Online Information Privacy Concerns: An Information-Processing Theory Approach," *Journal of Management Information Systems* 24, no. 2 (2007): 13. Willingness to pay was shown to vary between $30.49 and $44.62 for US subjects.

[285] See Yoan Hermstruwer and Stephan Dickert, "Tearing the Veil of Privacy Law: An Experiment on Chilling Effects and the Right to Be Forgotten," Preprints of the Max Planck Institute for Collective Goods (Bonn, 2013).

[286] Some studies suggest that, counter intuitively, the offer of a reward for the information actually reduces self-disclosure, intensifying concern against rational-choice based predictions. See Eduardo Andrade, Velitchka Kaltcheva, and Barton Weitz, "Self-Disclosure on the Web: The Impact of Privacy Policy, Reward, and Company Reputation," *Advances in Consumer Research* 29 (2002): 350. Other research, however, contradicts those findings. See Kai-Lung Hui, Hock Hai Teo, and Sang-Yong Lee, "The Value of Privacy Assurance: An Exploratory Field Experiment," *Management Information Systems Quarterly* 31, no. 1 (2007): 19.

[287] See Aleecia McDonald and Lorrie Faith Cranor, "Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising," in *Proceedings of the 38th Research Conference on Communication, Information and Internet Policy* (Arlington, 2010).

than the willingness to pay (WTA:WTP ratio of 5.47) which almost doubles average ratio for other goods (2.92).[288]

Other related research has explored the impact —or lack thereof— of privacy policies in websites,[289] together with other elements such as the mention of a protecting regulation,[290] privacy seals,[291] the way in which information requests are presented,[292] how much other data subjects disclose,[293] and promises of data breach notifications.[294]

3.2.2.! Differing valuations

Other research focuses on whether these valuations vary and whether certain types of personal information are valued more or less than others.

Data subjects value their offline information, which is composed by facts related directly to their person that enters the online domain such as their birth date or health status, differently than their online information, composed by their browsing patterns. In average, they seem to value offline information three times as much as their browsing behavior.[295]

---

[288] See Alessandro Acquisti, Leslie John, and George Loewenstein, "What Is Privacy Worth?," *Journal of Legal Studies* 42, no. 2 (2013): 249.

[289] See Eduardo Andrade, Velitchka Kaltcheva, and Barton Weitz, "Self-Disclosure on the Web: The Impact of Privacy Policy, Reward, and Company Reputation," *Advances in Consumer Research* 29 (2002): 350; Kai-Lung Hui, Hock Hai Teo, and Sang-Yong Lee, "The Value of Privacy Assurance: An Exploratory Field Experiment," *Management Information Systems Quarterly* 31, no. 1 (2007): 19.

[290] See Sarah Spiekermann, Jens Grossklags, and Bettina Berendt, "E-Privacy in 2nd Generation E-Commerce: Privacy Preferences versus Actual Behavior," in *Proceedings of the Third Association for Computing Machinery Conference on Electronic Commerce*, ed. Michael Wellman and Yoav Shoham (New York: Association for Computing Machinery Press, 2001), 38.

[291] See Kai-Lung Hui, Hock Hai Teo, and Sang-Yong Lee, "The Value of Privacy Assurance: An Exploratory Field Experiment," *Management Information Systems Quarterly* 31, no. 1 (2007): 19.

[292] See Alessandro Acquisti, Leslie John, and George Loewenstein, "The Impact of Relative Standards on the Propensity to Disclose," *Journal of Marketing Research* 49 (2012): 160.

[293] See Ibid.

[294] See Francesco Feri, Caterina Giannetti, and Nicola Jentzsch, "Disclosure of Personal Information Under Risk of Privacy Shocks," University of Bologna School of Economics Working Paper 875 (Bologna, 2013).

[295] See Juan Pablo Carrascal et al., "Your Browsing Behavior for a Big Mac: Economics of Personal Information Online," in *Proceedings of the 22nd International Conference on World Wide Web* (Geneva, 2013).

Regarding offline information in particular, it has been shown that—as it is intuitive—data subjects do not value all of its types in the same way. An inverse linear relationship has been shown between the desirability of their personal traits and the value they place on them; people ask for more money in order to reveal their undesirable traits with no direct financial or identity-theft repercussions, such as weight and age.[296]

More specifically, some research has indicated that data subjects place different values over different types of offline personal information. For instance, they seem to place a high value on information related to their medical and financial status and information about their families, and to have less trouble disclosing information about product consumption and brand consumption, as well as media usage.[297]

This line of research suggests that there are relevant differences between the types of information data subjects choose to disclose—offline and online, sensitive and non-sensitive—, and if personal information is treated as fungible units then experimental results might not be entirely accurate. Since not all types of personal information impact data subjects' utility in the same way, it is questionable to treat personal information as fungible units when analyzing transactions.[298]

3.2.3.! Context and accessibility

Other papers explore the importance of context and accessibility of information at the moment of disclosure, which data subjects seem to respond to. They suggest that consumer behavior is less random than one might think based on the findings reviewed above.

---

[296] See Bernardo Huberman, Eytan Adar, and Leslie Fine, "Valuating Privacy," *Institute of Electrical and Electronics Engineers Security and Privacy Magazine* 3 (2005): 22.

[297] See Daniel Horne and David Horne, "Domains of Privacy: Toward an Understanding of Underlying Factors," in *Direct Marketing Educators' Conference* (San Francisco, 1998).

[298] See Luc Wathieu and Allan Friedman, "An Empirical Approach to Understanding Privacy Valuation," Harvard Business School Working Paper 07-75 (Boston, 2007).

When taking the context of disclosure into account, there is some evidence in favor of agents that behave rationally when facing simple privacy issues.[299] Data subjects' privacy concerns seem to be sensitive not only to direct harms—defined as an immediate perceived harm provoked by an information release such as fear of fraud or spam—but also to the indirect consequences of the transmission of information—such as fear of ending up being the object of price discrimination. Data subjects seem mainly concerned about the use that is given to their information—even more than about its transfer.[300] An increment in control over the publication of data subjects' personal data decreases their concerns over their privacy and hence increases their willingness to disclose sensitive information.[301]

Data subject's ability to act in their own self-interest when dealing with privacy issues changes when these issues become complex—there does not seem to be a generalized inability to deal with them.[302]

Other studies have shown that when information about security is made visible, for instance available on browsers themselves, data subjects respond to it.[303] One of them shows that, when information about privacy is available directly on search engines, data subjects do prefer websites that offer a higher protection for their privacy, in particular regarding purchases that involve the disclosure of sensitive information.[304] Another,

---

[299] See Ibid.
[300] See Ibid.
[301] See Leslie John, Alessandro Acquisti, and George Loewenstein, "Strangers on a Plane: Context-Dependent Willingness to Divulge Sensitive Information," *Journal of Consumer Research* 37, no. 5 (2011): 858.
[302] See Ibid.
[303] See Julia Gideon et al., "Power Strips, Prophylactics , and Privacy, Oh My!," in *Proceedings of the Second Symposium on Usable Privacy and Security* (New York, 2006), 133; Janice Tsai et al., "The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study," *Information Systems Research* 22, no. 2 (2011): 254; Nicola Jentzsch, Sören Preibusch, and Andreas Harasser, "Study on Monetising Privacy: An Economic Model for Pricing Personal Information. Report for the European Network and Information Security Agency" (Heraklion, 2012).
[304] See Julia Gideon et al., "Power Strips, Prophylactics , and Privacy, Oh My!," in *Proceedings of the Second Symposium on Usable Privacy and Security* (New York, 2006), 133.

explores whether a different display of privacy policies induces data subjects to incorporate better privacy considerations. It shows that when information is available and salient, data subjects prefer to purchase from retailers that protect their privacy better and are even willing to pay a premium to do so.[305]

Conversely, it has been shown that when information about privacy is not salient, data subjects display a low willingness to pay for their personal information. Participants were shown two otherwise identical stores that differed only in the requested information; one store asked for sensitive information and the other for non-sensitive information. When prices between the stores differed, subjects chose to buy from the cheapest store—even if it required more disclosure—and when the prices of the stores were equal, they were indifferent between the stores.[306]

Finally, while the level of comprehension of privacy policies is very low, and while an accessible link to the privacy policy in websites does not significantly affect levels of disclosure, other more "visceral" notices—such as anthropomorphic elements, self-focused attention mechanisms and a high level of formality in web design—do achieve higher levels of comprehension on data subjects and have an effect on their levels of disclosure.[307]

---

[305] See Janice Tsai et al., "The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study," *Information Systems Research* 22, no. 2 (2011): 254.

[306] See Alastair Beresford, Dorothea Kübler, and Sören Preibusch, "Unwillingness to Pay for Privacy: A Field Experiment," *Economics Letters* 117, no. 1 (2012): 25. For an extension of this experiment to an unraveling market, and showing that to some extent data subjects react to privacy costs, see Volker Benndorf, Dorothea Kuebler, and Hans-Theo Normann, "Privacy Concerns, Voluntary Disclosure of Information, and Unraveling: An Experiment," *Forthcoming in European Economic Review*, 2015.

[307] See Victoria Groom and Ryan Calo, "Reversing the Privacy Paradox: An Experimental Study," in *Proceedings of the 39th Telecommunications Policy Research Conference* (Schertz, 2011).

3.3.! Competing Explanations

3.3.1.! Hyperbolic discounting

In a first approximation to explain the privacy paradox, an explanation that has been offered for it pictures data subjects within a model of self-control problems with agents who hyperbolically discount.[308]

A two-fold explanation has been offered for this. First, if data subjects declare that they value their privacy highly, but then they act disregarding it by offering it for low compensations, this behavior can be interpreted as setting a certain plan of action or consumption pattern (they possess a good which they value highly so they should only sell it for a high price) and then deviating from it (they offer the good for a low compensation). Second, this behavior is consistent with the literature that suggests that people in many situations discount the distant future at lower rates than the near future.[309]

It has been argued that based on the available data from experimental findings it is unrealistic to expect rationality from data subjects. Behavioral economics has shown individuals display in many occasions hyperbolic discounting, under insurance, self-control problems, and immediate gratification, all of which alter people's ability to make decisions. From this perspective, it was argued that the privacy paradox is an example of these biases driving behavior.[310]

---

[308] Hyperbolic discounting is an increasing rate of time preference over time so that the distant future is more heavily discounted than the near future.

[309] See Richard Thaler, "Some Empirical Evidence on Dynamic Inconsistency," *Economics Letters* 8 (1981): 201.

[310] See Alessandro Acquisti, "Privacy in Electronic Commerce and the Economics of Immediate Gratification," in *Proceedings of the Fifth Association for Computing Machinery Conference on Electronic Commerce*, ed. Jack Breese, Joan Feigenbaum, and Margo Seltzer (New York: Association for Computing Machinery Press, 2004), 21; Alessandro Acquisti and Jens Grossklags, "Privacy Attitudes and Privacy Behavior," in *The Economics of Information Security*, ed. Jean Camp and Stephen Lewis (Dordrecht: Kluwer, 2004); Alessandro Acquisti, Leslie John, and George Loewenstein, "What Is Privacy Worth?," *Journal of Legal Studies* 42, no. 2 (2013): 249.

Based on this line of reasoning, models of self-control problems have been offered as an explanation for the experimental data. Data subjects' behavior has been then explained based on a model of immediate gratification where agents hyperbolically discount when facing decisions involving different delays,[311] as a response to the consideration that it is unrealistic to assume knowable probabilities or complete beliefs.[312]

It has also been mentioned that data subjects face uncertainty about the possible outcomes, the magnitude of their consequences, the possible measures to protect themselves, the actions taken by those who desire their information, and the existence of some unforeseeable events, between others.[313] Exploring further the role of uncertainty could thus shed light in data subjects' behavior.

In economics there are two possible reasons to discount payoffs—costs of waiting and hazard rates—which produce two different reasons for choice reversal. The first, hyperbolic discounting, relies on assumptions on the agents, while the second, a decreasing or uncertain hazard rate, relies on assumptions on the context.

The second stage of the explanation given to data subjects' behavior can be reevaluated. To do this the literature that reconciles non-constant discounting with dynamic consistency can be used to offer a feasible explanation to the observed consumer behavior within rational-choice theory.

---

311 See Ted O'Donoghue and Matthew Rabin, "Choice and Procrastination," *Quarterly Journal of Economics* 116, no. 1 (2001): 121.

312 See Alessandro Acquisti and Jens Grossklags, "What Can Behavioral Economics Teach Us About Privacy?," in *Digital Privacy: Theory, Technologies and Practices*, ed. Alessandro Acquisti et al. (Boca Raton: Auerbach Publications, 2007), 363; Alessandro Acquisti and Jens Grossklags, "Privacy and Rationality in Individual Decision Making," *Institute of Electrical and Electronics Engineers Security and Privacy Magazine* 3, no. 1 (2005): 26.

313 See Ibid.; Yoan Hermstruwer and Stephan Dickert, "Tearing the Veil of Privacy Law: An Experiment on Chilling Effects and the Right to Be Forgotten," Preprints of the Max Planck Institute for Collective Goods (Bonn, 2013); Alessandro Acquisti, Laura Brandimarte, and George Loewenstein, "Privacy and Human Behavior in the Age of Information," *Science* 347, no. 6221 (2015): 509.

3.3.2.! Discounting based on a declining hazard rate

Time discounting means that people care less about future consequences than about present consequences, for any possible reason. A relevant reason to discount is that waiting is costly. Another relevant reason is that, over time, payoffs have the risk of depreciating or disappearing; payoffs have a certain hazard rate.

Imagine an agent who has two choices. The first one is a choice between a certain payoff V (100 Euros) at time T (now) or a bigger payoff V' (150 Euros) at further time T' (a year from now). The second one is between the same payoffs (V and V') at times $T + t$ (3 months from now) and $T' + t$ (a year and 3 months from now).[314]

If the hazard rate that payoffs have is independent of time (in the example, there is a constant chance of the promisor of the 150 euros going bankrupt), then the discount rate of a rational agent should be constant. If the agent has a choice between a payoff V at time T or a bigger payoff V' at further time T' with a constant hazard rate (λ), then the expected payoff he compares with V should be $e^{-\lambda T'}V'$.[315] The same applies to the second choice.

On the other hand, if the hazard rate (λ) is not independent but dependent on time (T), such that $\lambda = \lambda(T)$ in a way that λ decreases in T ($\lambda' < 0$), then closer payoffs would be discounted at a higher rate than distant payoffs (each month there is a lower chance of the promisor going bankrupt, because he handles his business better).[316] This increases the discount rate as hyperbolic discounting.[317]

This equivalence between the hyperbolic discounting function and the discount function based on a hazard rate, it should be noted, does not

---

[314] See Peter Sozou, "On Hyperbolic Discounting and Uncertain Hazard Rates," *Proceedings of the Royal Society of Biological Sciences* 265, no. 1409 (1998): 2015.
[315] See Partha Dasgupta and Eric Maskin, "Uncertainty and Hyperbolic Discounting," *The American Economic Review* 95, no. 4 (2005): 1290.
[316] See Ibid.
[317] See Shane Frederick, George Loewenstein, and Ted O'Donoghue, "Time Discounting and Time Preference: A Critical Review," *Journal of Economic Literature* 40, no. 2 (2002): 351.

happen with any kind of risk, but only in those cases in which the hazard rate decreases over time. Due to the declining hazard rate the agent is more afraid of the payoff disappearing in the first period, and therefore discounts the first choice and the second choice in a different way. This could happen, for instance, with college students, who have a decreasing hazard rate of dropping out, and start-up firms, which have a decreasing hazard rate of going bankrupt, or the unfortunate promisor of the example.

Using a different example, the following table illustrates this procedure.

Delay	*Probability of survival* (s)	*Hazard rate*	*Expected value of cake* ($s.v_c$)	*Expected value of wine* ($s.v_w$)
No delay	1	0%	2	3
1 month	$\frac{1}{2}$	50%	1	$\frac{3}{2}$
2 months	$\frac{1}{3}$	27%	$\frac{2}{3}$	1
3 months	$\frac{1}{4}$	8%	$\frac{1}{2}$	$\frac{3}{4}$
Intrinsic value of cake $v_c = 2$ Intrinsic value of wine $v_w = 3$				

Table 1. Illustrates choice reversal over a hypothetical choice between cake and wine. A cake now is preferred over wine in one month, but wine in 3 months is preferred over cake in 2 months. Based on the table in Sozou (1998). The hazard rate is added for clarity using the probabilities available in the original table.

In the table, the agent has the choice between cake and wine in different time periods. If he has to choose between cake and wine now, he prefers wine ($2 < 3$). If he has to choose between cake now and wine in a month, he would rather take the cake ($2 > \frac{3}{2}$), since the promise of wine has a probability of 50% to materialize itself in a month ($3 * \frac{1}{2} = \frac{3}{2}$). However,

even when fully rational and absent of behavioral biases, if he has to choose between cake in two months and wine in three months, he would rather choose wine ($\frac{1}{2} < \frac{3}{4}$). His choice between the options shifts because the hazard rate of cake and wine (their marginal probability of disappearing) is decreasing over time. This example illustrates how a rational agent would reverse his choices when placed in a particular context.

3.3.3.! Discounting based on an unknown hazard rate

If one assumes that the hazard rate is not declining but it is unknown to the agent, then a rational agent will approach the new situation in a similar way. The first choice he has is only relevant in a conditional way to the payoffs surviving after the first period of time T (in the example, now), while his second choice is only relevant conditional to the payoffs surviving after the first period of time $T + t$ (in the example, 3 months).

Since the agent faces uncertainty over the hazard rate in each scenario, he will again be afraid of the payoff disappearing in the first period and will use a discount rate that is lower for the second case. So the (rational) agent will behave less patiently in the first choice, even without a declining hazard rate.[318] [319] In the example, if he cannot get the prize that was promised to him at time T (now) anyhow, and he must face the unknown risk (he does not know how well the promisor handles his own business), he would rather wait longer ($T + t$, 3 months) and get a larger reward.

---

[318] See Peter Sozou, "On Hyperbolic Discounting and Uncertain Hazard Rates," *Proceedings of the Royal Society of Biological Sciences* 265, no. 1409 (1998): 2015; Yoram Halevy, "Strotz Meets Allais: Diminishing Impatience and the Certainty Effect," *The American Economic Review* 98, no. 3 (2008): 1145; Omar Azfar, "Rationalizing Hyperbolic Discounting," *Journal of Economic Behavior & Organization* 38 (1999): 245.

[319] There are also accounts for the change in discounting based on the effect of intervals. See Daniel Read, "Is Time-Discounting Hyperbolic or Subadditive?," *Journal of Risk and Uncertainty* 23, no. 1 (2001): 5; Daniel Read and Peter Roelofsma, "Subadditive versus Hyperbolic Discounting: A Comparison of Choice and Matching," *Organizational Behavior and Human Decision Processes* 91, no. 2 (2003): 140.

Rational agents with no strict time preferences that include in their analysis unknown risks such as their own mortality have been shown to display diminishing impatience while maintaining time-consistent choices,[320] even when the unknown hazard rate is increasing.[321] Non-expected utility models can be the result of rational behavior when faced with uncertainty in the future, which means that preference reversals do not imply impatience when risk is present.[322]

This idea has been supported by experimental evidence, where it was found that when uncertainty for the present increased from 0 to 0.5, subjects choosing immediate rewards in standard choice reversal problems decreased from 82% to 39% (present bias is reduced when the present is also risky).[323] A procedure to test for hyperbolic discounting while controlling for uncertainty has also been presented.[324][325] Other studies

---

[320] See Peter Sozou, "On Hyperbolic Discounting and Uncertain Hazard Rates," *Proceedings of the Royal Society of Biological Sciences* 265, no. 1409 (1998): 2015; Omar Azfar, "Rationalizing Hyperbolic Discounting," *Journal of Economic Behavior & Organization* 38 (1999): 245.

[321] See Yoram Halevy, "Diminishing Impatience: Disentangling Time Preference from Uncertain Lifetime," University of British Columbia Department of Economics Working Paper 05-17 (Vancouver, 2005).

[322] See Yoram Halevy, "Strotz Meets Allais: Diminishing Impatience and the Certainty Effect," *The American Economic Review* 98, no. 3 (2008): 1145.

[323] See Gideon Keren and Peter Roelofsma, "Immediacy and Certainty in Intertemporal Choice," *Organizational Behavior and Human Decision Processes* 63, no. 3 (1995): 287; Bethany Weber and Gretchen Chapman, "The Combined Effects of Risk and Time on Choice: Does Uncertainty Eliminate the Immediacy Effect? Does Delay Eliminate the Certainty Effect?," *Organizational Behavior and Human Decision Processes* 96, no. 2 (2005): 104.

[324] See Jesus Fernandez-Villaverde and Arijit Mukherji, "Can We Really Observe Hyperbolic Discounting?," Penn Institute for Economic Research Working Paper 02-08 (Philadelphia, 2006); Gregory Besharov and Bentley Coffey, "Reconsidering the Experimental Evidence for Quasi-Hyperbolic Discounting," Duke Department of Economics Working Paper 03-03 (Durham, 2003).

[325] Agents in an experiment have consumption choices involving immediate and delayed consumption, and receive shocks in their preferences before each choice. Agents receiving different shocks initially make different decisions regarding those choices, while as the time horizon is moved forward shocks become irrelevant. The demand for pre-commitment devices during the whole experiment is very low.

indicate that this is also the case for uncertain delays.[326] This implies incurring in fewer assumptions than an uncertain hazard rate since in such case the prize (or penalty) is certain but only its moment of execution is uncertain.

This is how a rational agent facing two equivalent choices with different delays—even without a declining hazard rate—might have delay-dependent discounting and exhibit choice reversal when the hazard rate is uncertain.[327]

A way of discriminating between preference-based (dynamically inconsistent) diminishing impatience and uncertainty-based (dynamically consistent) diminishing impatience is checking for preferences towards pre-commitment or flexibility.[328] While sophisticated agents who discount due to self-control problems should be willing to pay to pre-commit—since that would maximize their long-term utility—sophisticated agents discounting due to uncertainty should be willing to pay for flexibility—since their utility is increased by the ability to adjust to new information.[329]

Agents facing a temptation problem who are aware of that problem would be willing to pay for a mechanism to bind oneself in order to avoid changing a certain decision in the future, and hence resist temptation. Some common examples of this mechanism are not having alcohol or unhealthy food at home, or taking a limited amount of money—and no credit cards—to the casino. Agents facing an uncertainty problem and who

---

[326] See Joseph McGuire and Joseph Kable, "Decision Makers Calibrate Behavioral Persistence on the Basis of Time-Interval Experience.," *Cognition* 124, no. 2 (2012): 216; Joseph McGuire and Joseph Kable, "Rational Temporal Predictions Can Underlie Apparent Failures to Delay Gratification.," *Psychological Review* 120, no. 2 (2013): 395.

[327] A mathematical explanation of this can be found in the appendix to this chapter, showing how the uncertainty-based discount function can take the same shape as a hyperbolic discount function.

[328] See Marco Casari, "Pre-Commitment and Flexibility in a Time Decision Experiment," *Journal of Risk and Uncertainty* 38, no. 2 (2009): 117.

[329] Sophisticated agents are defined as those who are aware of the reason for the diminishing impatience, while naïve agents are defined as those who are not. Naïve agents, of course, are not willing to pay for either pre-commitment or for flexibility.

are aware of it, on the other hand, would be willing to pay to be able to adapt to the context once expectations becomes certain. Naive agents, of course, will be willing to pay for neither.

The next section evaluates the feasibility of applying these theories to data subjects. Section 4.4.1 evaluates whether data subjects' behavior resembles the behavior of other agents who face temptation, and section 4.4.2 evaluates whether their context resembles a context of a decreasing or uncertain hazard rate.

3.4.! Contrasting Data Subject Behavior with Discounting Models

3.4.1.! Explaining consumer claims

One of the key features of self-control problems is that people recognize a certain behavior in themselves that is not consistent with a certain aim they have. They display a certain willingness to stop that behavior and—if sophisticated—they also recognize that they will probably continue to exhibit it. Pre-committing is then an optimal strategy.[330]

A model of data subjects who hyperbolically discount should lead one to conclude that an optimal strategy for data subjects is pre-commitment. Policy recommendations would then approach the privacy paradox from a paternalistic or libertarian-paternalistic standpoint.[331] The aim of a regulation that takes this interpretation of user behavior into account would be the provision of tools to pre-commit not to disclose personal information. Alternatively, a regulation aiming to do this can create a system of reward substitution—paying to avoid disclosure, charging to disclose, creating guilt, imposing additional obstacles, etc.

---

[330] See Ted O'Donoghue and Matthew Rabin, "Choice and Procrastination," *Quarterly Journal of Economics* 116, no. 1 (2001): 121.

[331] See Alessandro Acquisti, "Nudging Privacy: The Behavioral Economics of Personal Information," *Institute of Electrical and Electronics Engineers Security and Privacy Magazine* 7, no. 6 (2009): 82.

On the other hand, a model of uncertainty-based discounting data subjects such as the one suggested here would reverse this idea and lead to the conclusion that policy should provide data subjects with flexibility regarding their choices.

In order to distinguish between the two discounting mechanisms, as it was mentioned, it is relevant to ask: are data subjects and consumer associations demanding the introduction of pre-commitment mechanisms regarding their privacy, or are they asking for something else? In this context, regret does not seem to be a central driver of consumer claims. Even taking into account availability bias, most data subjects would say that they experience regret only on a small proportion of their information sharing. At the same time, at least anecdotal evidence shows surprise in data subjects when they discover how much others can know about their personal information based on what they disclose. Social network users do not typically promise themselves to close their profiles and fail to do so—as many dieters, smokers and people who want to do more exercise do—but they are sometimes shocked on how targeted advertisements display the topics they were recently concerned about.

The demands made by consumer associations typically focus on a lack of transparency in personal information processing. The European Data subjects Organization, for instance, has said through one of its members that "data subjects are sleep-walking in a world without privacy. They do not realize their data are being collected and processed."[332] Similarly, the popular objection against targeted advertising is a visceral reaction that qualifies it as "creepy" or "spooky."[333] Why would an increment in the relevance of advertising content with regards to data subjects' interests be qualified in such a way? It fits this characterization

---

[332] Matt Warman, "EU Fights 'Fierce Lobbying' to Devise Data Privacy Law," *The Telegraph*, February 9, 2012.

[333] See Paul Schwartz and Daniel Solove, "PII Problem: Privacy and a New Concept of Personally Identifiable Information, The," *NYU Law Review* 86 (2011): 1814; Blase Ur et al., "Smart, Useful, Scary, Creepy: Perceptions of Online Behavioral Advertising Perceptions of Online Behavioral Advertising," in *Proceedings of the Symposium On Usable Privacy and Security* (New York: Association for Computing Machinery Press, 2012).

to state that the reason is that those data subjects are not aware which companies have information about their interests until they find the advertisements and are surprised.

A simple but illustrative example can be obtained by imputing into Google Trends (which illustrates interest over time of chosen key words as expressed in Google searches) the key words "delete data" against "stop sharing data"—or similar alternatives. The numbers obtained, which in the case of those key words are 99% for "delete data" and 0% for "stop sharing data" for September 2013,[334] seem to indicate that data subjects—or at least data subjects searching on Google—are substantially more concerned, and are getting increasingly concerned, about how to delete their data (flexibility) as opposed to how to stop sharing it (pre-commitment).[335]

The experimental data reviewed in the first section also coincides with this. As it was seen, data subjects' reaction to privacy decisions change depending on the complexity of the decisions[336] and when information about privacy becomes more visible data subjects do respond to it by choosing higher privacy protections.[337] This behavior is less consistent with a model of irrational data subjects that display self-control problems than with a model of data subjects facing an uncertain decision-

---

[334] The company does not disclose the absolute search volumes, so numbers are relative, being 100% the maximum number of searches for any of the keywords in the chosen period.

[335] For an analysis of this since 2004 until now see http://www.google.com/trends/explore#q=delete%20data%2C%20%20stop%20sharing%20data%2C%20%20avoid%20uploading%20data&cmpt=q (Last time accessed 25/11/2013).

[336] See Luc Wathieu and Allan Friedman, "An Empirical Approach to Understanding Privacy Valuation," Harvard Business School Working Paper 07-75 (Boston, 2007); Leslie John, Alessandro Acquisti, and George Loewenstein, "Strangers on a Plane: Context-Dependent Willingness to Divulge Sensitive Information," *Journal of Consumer Research* 37, no. 5 (2011): 858.

[337] See Julia Gideon et al., "Power Strips, Prophylactics , and Privacy, Oh My!," in *Proceedings of the Second Symposium on Usable Privacy and Security* (New York, 2006), 133; Janice Tsai et al., "The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study," *Information Systems Research* 22, no. 2 (2011): 254.

making scenario, since irrationality would prevent data subjects from responding to these stimuli.

At a more general level, the fact that data subjects systematically display different valuations for different types of information about them[338] and that they react rationally to changes in context and accessibility[339] indicates that they have a rational approach towards their personal information. An agent who faces temptation and discounts hyperbolically should discount independently of context, while the available experimental evidence has shown that data subjects respond to context when such context is visible.

3.4.2.! Privacy breaches as a hazard rate

The case of internet privacy presents two differences with the traditional experiments on hyperbolic discounting. First, while in the latter agents have a choice between a monetary payoff in the present time and a larger monetary payoff in the future, in the case of internet privacy the tradeoff that agents have is between a certain penalty in the present time (not extracting the benefits of disclosing their information) and a larger penalty in the future in the form of a privacy breach.[340]

This risk of privacy breach represents the disutility of any use that can be made with the traded information that is unpleasant to the data subject, and hence he should take it into account as an expected cost when deciding whether to disclose. Therefore, it can take many forms, the most common ones ranging from mostly harmless annoyances such as receiving spam email, to more serious consequences such as public disclosure of

---

[338] See section 3.2.2.

[339] See section 3.2.3.

[340] There is also the element that data subjects face eventual losses instead of gains as it is the case in most of the hyperbolic discounting literature. This is illustrated in O'Donoghue and Rabin: while gains are preferred now better than later, losses are preferred later better than now. See Ted O'Donoghue and Matthew Rabin, "Doing It Now or Later," *The American Economic Review* 89, no. 1 (1999): 103. This is notwithstanding the fact that people seem to discount losses with a lower discount rate that the one they use to discount gains. See Richard Thaler, "Some Empirical Evidence on Dynamic Inconsistency," *Economics Letters* 8 (1981): 201.

embarrassing information, the acquisition of information by medical insurers or future employers that would financially damage the person, identity fraud or identity theft.

The second difference with decision of whether to disclose personal information online is the existence of uncertainty over the outcome. In this case, the privacy breach, which materializes the hazard rate, has an unknown probability of occurrence at each stage.

In experiments where agents have a choice between different monetary payoffs at different times, they are aware of the size of the payoffs and the probability of the larger payoff occurring. Similarly, when people face daily-life situations in which they hyperbolically discount they are aware of this as well. In the classic example where someone faces the choice of whether to eat cake or fruit salad, he already knows the extent to which cake might damage his health. If he chooses it still, one can argue he was discounting hyperbolically because he knew about the expected payoff beforehand—if he had not known the adverse health effects of cake then the decision would not have been based on hyperbolic discounting but on blissful ignorance.

On the other hand, when people decide whether to disclose their personal information, they ignore the probabilities of the bigger penalty (privacy breach) occurring in each period—this is, they ignore the hazard rate. This takes place not only due to the changing environment in which it takes place, given the changes in technology over time, but also due to the externalities present in data trading.

Every time a company trades a data subject's personal information with another, the data subject faces an increment in the risk of a privacy breach. This ranges from legitimate transfers of information, which can be traded to other companies with a different business model, to illegitimate transfers, such as hacking. A large amount of data-dredging practices, for instance, take place through virus attacks. As the number of databases that possess a certain piece of information increases, the more likely such piece of information is to be subject of a virus attack, keeping other conditions stable.

When companies trade this information, the data subject has his personal data out of his range of control—as his consent is not needed any more to trade it—while its use still has the potential of impacting his welfare negatively. In other words, there are externalities in data trading.[341] Securing such trade is the main role of companies who buy and sell aggregated data subjects' personal information acting as intermediaries between data collectors and advertisers.[342] While these exchanges are only agreed by data collectors and the intermediaries, or by the intermediaries and the advertising companies, data subjects also face expected costs from each of trade. These externalities imply an incentive for companies to overuse information, since they do not face all costs, which is aggravated by the fact that data subjects will often not learn about the over-disclosure and hence have no opportunity to discipline such companies.[343]

Hence, even if at the moment of making the decision of whether to disclose the data subject had full information about expected costs and benefits, he would make such decision based on an uncertain hazard rate because the risk of a privacy breach is not dependent on his behavior alone but also on the subsequent behavior of the companies that acquire his data. This fact leads both to difficulties in making a welfare-maximizing decision and, as the previous section showed, to a discount function that should resemble hyperbolic discounting.[344]

---

[341] See Kenneth Laudon, "Markets and Privacy," *Communications of the Association for Computing Machinery* 39, no. 9 (1996): 92; Hal Varian, "Economic Aspects of Personal Privacy," in *Cyber Policy and Economics in an Internet Age. Topics in Regulatory Economics and Policy Series.*, ed. William Lehr and Lorenzo Pupillo (Norwell: Springer, 2002), 127.

[342] See John Hagel and Jeffrey Rayport, "The Coming Battle for Consumer Information," *Harvard Business Review* 75, no. 1 (1997): 53.

[343] See Peter Swire and Robert Litan, *None of Your Business: World Data Flows, Electronic Commerce and the European Privacy Directive* (Washington, DC: Brookings Institution Press, 1998). 8.

[344] An example of these expected costs materializing that has turned famous due to its magnitude is the Sony scandal of 2011. In that year, data from 100 million users were stolen from the Sony Online Entertainment databases, including name, address, birth date, and in many cases debit and credit card information, which was user later on for different types of fraud. See Sony Online

Moreover, if behavioral research is to be taken into consideration, then the uncertainty over the hazard rate in the case at hand is not only determined by the externalities which are unknown to the data subject. There are arguments to believe that, in addition to this objective uncertainty, data subjects face subjective uncertainty, which could be produced by limitations in their computational capacities or by high information costs that are rationally not incurred.

Data subjects many times do not comprehend privacy policies and license agreements[345] and the available privacy protection tools.[346] Protecting privacy on internet properly requires technical skills that very few data subjects possess.[347] Some data subjects ignore the simplest behaviors to engage to protect their privacy, namely to avoid opening unwanted email (spam), sharing files, downloading from non-secure sites and clicking on pop-up advertisements. More than half of all Americans believe that the mere existence of a privacy policy means that companies cannot trade their data.[348] Several data subjects disclose their birth date in social networks under privacy configurations that make them visible to any other internet user, despite the fact that the increases the probability of making them victims of identity fraud[349] and identity theft.[350]

Entretainment Press Release, "Sony Online Entretainment Announces Theft of Data from Its Systems," 2011. Many of those data subjects did not use the device that uploads information to that database, but their information was in the database nonetheless because it had been replicated or moved. That replication, or that movement, had imposed on them an expected cost in the form of an externality of which they were not aware.

[345] See George Milne and Mary Culnan, "Strategies for Reducing Online Privacy Risks: Why Consumers Read (or Don't Read) Online Privacy Notices," *Journal of Interactive Marketing* 18, no. 3 (2004): 15.

[346] See Alessandro Acquisti and Jens Grossklags, "Privacy and Rationality in Individual Decision Making," *Institute of Electrical and Electronics Engineers Security and Privacy Magazine* 3, no. 1 (2005): 26.

[347] See Joseph Turow, "Americans and Online Privacy: The System Is Broken," *The University of Pennsylvania Annenberg Public Policy Center Report* (Philadelphia, 2003).

[348] See Joseph Turow et al., "Americans Reject Tailored Advertising and Three Activities That Enable It," *The University of Pennsylvania Annenberg Public Policy Center Report* (Philadelphia, 2009).

[349] In the Netherlands, for example, around 5% of the population was a victim of identity fraud in 2012 alone either by phishing or pharming—which are different

Since in cases of online disclosure of personal information the outcomes of the choice—a large negative payoff—do not occur with certainty, a study where a discount rate or discount factor is inferred only from observed consumption will include in the same category both the discounter for the delay of the penalty and the discounter for its hazard rate. Any perceived risk will therefore alter the observed discounting for delay.[351]

This suggests that models that incorporate uncertainty-based discounting might explain better the privacy paradox.

3.5.! Normative Implications

3.5.1.! The right to be forgotten

If one takes the argument that the uncertainty that data subjects face is a relevant problem in their interaction with service-providing companies, then one encounters the question on how to design regulations that can help data subjects to reduce it.

As with consumer claims, some of the main contemporary debates over the regulation of privacy seem to go in the direction of providing data subjects with additional flexibility regarding their choices of whether to disclose. A relevant example of this is the right to be forgotten, the most debated feature of the GDRP, and one of its main pillars.[352]

---

methods to use an internet site to obtain personal information. See Ministry of Security and Justice and the Central Bureau of Statistics, "Safety Monitor 2012," 2013.

[350] Comparing survey data with data from the FTC, studies seem to indicate that 73% of people underestimate the actual chances of identity theft. See Alessandro Acquisti and Jens Grossklags, "Privacy and Rationality in Individual Decision Making," *Institute of Electrical and Electronics Engineers Security and Privacy Magazine* 3, no. 1 (2005): 26.

[351] See Peter Sozou, "On Hyperbolic Discounting and Uncertain Hazard Rates," *Proceedings of the Royal Society of Biological Sciences* 265, no. 1409 (1998): 2015; Yoram Halevy, "Strotz Meets Allais: Diminishing Impatience and the Certainty Effect," *The American Economic Review* 98, no. 3 (2008): 1145.

[352] See Pere Simon Castellano, "The Right to Be Forgotten under European Law: A Constitutional Debate," *Lex Electronica* 16, no. 1 (2012): 1. See also article 17 of

As it will be seen with more detail in the following chapter, what the right to be forgotten attempts to provide data subjects with is a right to request entities that collect or process data to erase from their database any piece of information regarding that data subject, regardless of the source.

From the perspective of theory that has been evaluated above[353] one can see that the! right to be forgotten could be valuable to data subjects from a welfare perspective inasmuch as it provides them with additional flexibility when making decisions of whether to share personal information. Data subjects would be able to publish a certain piece of information and later on reverse their decision by requesting its deletion. This possibility, as it was mentioned, would be helpful for them if dealing with an uncertain hazard rate in personal information sharing. [354]

This is linked to some of the main arguments in favor of the right. Namely, the argument that individuals should be able to act and speak freely without the fear that this will lead to dire consequences in the future as the freedom to change is an element of self-development.[355] Similarly, A29WP has expressed that control over one's personal information is a central aspect of informational privacy, where control is commonly instrumented by consent.[356]

---

the GDRP. The right to be forgotten with be further analyzed in chapter 4, and particularly in the context of the GDRP, in section 4.2.

[353] See sections 4.2.3 and 4.3.2.

[354] In the Frequently Asked Questions of the proposed regulation, for instance, it is stated that "a reinforced 'right to be forgotten' will help people better manage data protection risks online" European Commission, "Data Protection Reform: Frequently Asked Questions," *MEMO/12/41*, 2012.

[355] See Jean-François Blanchette and Deborah Johnson, "Data Retention and the Panoptic Society: The Social Benefits of Forgetfulness," *The Information Society* 18, no. 1 (2002): 33; Chris Conley, "The Right to Delete," in *Intelligent Information Privacy Management* (Palo Alto: Association for the Advancement of Artificial Intelligence, 2010); Franz Werro, "The Right to Inform v. the Right to Be Forgotten: A Transatlantic Clash," in *Haftungsbereich Im Dritten Millennium (Liability in the Third Millennium)*, ed. Aurelia Colombi Ciacchi et al. (Baden: Nomos, 2009), 285.

[356] See A29WP, "O.J. 15/2011 On the Definition of Consent" (Brussels, July 13, 2011).

This feature, in addition, appears to be a central aim of the regulation. In the Frequently Asked Questions, for instance, it is stated that "a reinforced 'right to be forgotten' will help people better manage data protection risks online."[357]

The right to be forgotten has been, at the same time, criticized from different angles, mainly due to the limits it imposes for freedom of expression.[358] The right, indeed, might be socially costly, and it could be difficult to defend in efficiency terms. What this perspective indicates is that the right has some value also beyond a deontological perspective, and that inasmuch as it increases flexibility it is not unreasonable to consider it in a more limited version in the public debate.

3.5.2.! Increasing transparency

While it is hardly possible to completely eliminate uncertainty for data subjects, providing marginal increases in flexibility is possible from a regulatory standpoint at lower burdens for providing companies than those that the right to be forgotten would present.

The experimental literature reviewed points to the relevance of context in the disclosure of information. Evaluating the contextual differences that helped at informing data subjects can, potentially, reduce the uncertainty over the hazard rate.

A policy that might appear attractive at a first glance are publicly run privacy seals. Privacy seals are a type of trust seal issued by a certain entity to a website or a company to show that they comply with certain minimum requirements regarding data protection. In such way, they aim to operate as signaling devices to data subjects, for whom it would be costly to acquire the information by themselves. However, besides being costly to implement, it has been suggested that privacy seals are largely

---

[357] European Commission, "Data Protection Reform: Frequently Asked Questions," *MEMO/12/41*, 2012.
[358] See Jeffrey Rosen, "The Right to Be Forgotten," *Stanford Law Review Online* 64 (2012): 88.

ineffective.[359] Most seals consist in an image that, with a certain level of technical ability, the owner of an unsafe website can copy and paste, reducing its signaling value. Additionally, once a seal is granted to a website, its level of security can change, and it is too expensive for the entity managing the seal to screen all websites with enough frequency to ensure that the seal reflects its current level of safety. Moreover, there are already available privacy seals programs that have emerged in the private market, reducing the added value of publicly-run programs.

A useful first step would be to require complete privacy policies. An example of this insufficiency is the frequent use of Flash cookies by many websites—with the ability to track despite having been deleted—even though few of them mention it in their privacy policies. Another is the even less transparent re-spawning of traditional cookies by data storage mechanisms that other websites use and not always mention to their users.

A second step is working on the transparency of such documents.[360] The topic of the incorporation of privacy policies is inevitably connected to the limits in computational ability that data subjects have. Showing the actual document—as opposed to only a hyperlink to it—and allowing data subjects to accept it only after scrolling it to the bottom can marginally improve their incorporation, like it is done with regular contracts—one cannot sign a contract at the top as a manifestation of agreement, even if one does not read it when signing at the bottom. This consideration is in line with the experimental literature on the topic.[361] Although the difference in the information absorbed by making data subjects screen a document is probably small, given that the cost of the change is negligible it is a useful requirement to consider.

---

[359] See Kai-Lung Hui, Hock Hai Teo, and Sang-Yong Lee, "The Value of Privacy Assurance: An Exploratory Field Experiment," *Management Information Systems Quarterly* 31, no. 1 (2007): 19.

[360] Transparency is, in fact, one of the central values of EU DPL. See Directive 1995/46/EC.

[361] See Janice Tsai et al., "The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study," *Information Systems Research* 22, no. 2 (2011): 254.

Still, privacy policies in their current state are costly to read; it has been estimated that an average user would spend 201 hours per year reading all privacy policies.[362] An improvement on this would be to provide a digested summary at the top of privacy policies stating its most relevant elements, which by reducing the cost of reading would increase the probability of being read by data subjects.[363] While 70% of people consider privacy policies are difficult to understand,[364] research indicates that when privacy is offered in a clear and understandable way people do value it.[365] The experimental literature on visceral notices also suggests this measure should have a relevant impact.[366] These summaries can also be set to clarify a list of pre-defined facts that are considered relevant to increase transparency, such as whether the company is allowed to trade the user's information with others, which uses it is authorized to give to the information that it receives, and whether the information is deleted after the user removes it from the system. At a more general level, privacy policies should be made more readable.[367]

---

[362] See Aleecia McDonald and Lorrie Faith Cranor, "The Cost of Reading Privacy Policies," *I/S: Journal of Law and Policy for the Information Society* 4 (2008): 543. This would cost, according to the authors, $3,534 to the average American internet user each year.

[363] See Ian Ayres and Alan Schwartz, "The No-Reading Problem in Consumer Contract Law," *Stanford Law Review* 66 (2004): 545. The authors propose a similar system to be applied to standard-form contracts in consumer law in general.

[364] See Joseph Turow, Lauren Feldman, and Kimberly Meltzer, "Open to Exploitation: American Shoppers Online and Offline," *The University of Pennsylvania Annenberg Public Policy Center Report* (Philadelphia, 2005).

[365] See Adam Shostack and Paul Syverson, "What Price Privacy? (and Why Identity Theft Is about Neither Identity nor Theft)," in *Economics of Information Security,* ed. Jean Camp and Stephen Lewis (Norwell: Kluwer, 2004), 129.

[366] See Victoria Groom and Ryan Calo, "Reversing the Privacy Paradox: An Experimental Study," in *Proceedings of the 39th Telecommunications Policy Research Conference* (Schertz, 2011).

[367] See Patrick Kelley et al., "Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach," in *Proceedings of the Association for Computing Machinery Special Interest Group on Computer-Human Interaction Conference* (New York: Association for Computing Machinery Press, 2010), 1573; Patrick Gage Kelley et al., "A 'Nutrition Label' for Privacy," in *Proceedings of the Fifth Symposium On Usable Privacy and Security* (New York: Association for Computing Machinery Press, 2009), 4.

Articles 7(2) and 11 of the GDRP work in this direction. The first requires that if consent for processing data is requested in a declaration that also addresses other issues then the request must be made distinguishable. The second demands that data controllers have privacy policies that are transparent and easily accessible and that communications to data subjects regarding the processing of their personal data should be done in an intelligible way, with plain language that is adapted to the data subject. So do articles 14(1) and 14(2), regarding information and the access to data, and 19(2), which states that the right to object must be explicitly and intelligibly manifested to the data subject.

Implementations of this idea have been designed in the form of Facebook nudges to raise awareness about privacy.[368] These nudges introduce visual cues about the audience to which posts are visible, time delays for posts—as Gmail has as an optional feature—and feedback about potential negative perception of posts based on cue words. An implementation of this can require a disclaimer that warns data subjects when a certain information disclosure will be completely public, as some companies have already done, providing information in a way that is accessible for users.

Regarding types of information, while it is not always easy to distinguish between sensitive and non-sensitive information, online and offline information can be easily distinguished, and it seems that they should also be treated differently, since online information presents smaller expected externalities than offline information. It has been shown that data subjects value online and offline information very differently,[369] which reflects the fact that most disutility for data subjects stems from disclosure of offline information since all sensitive information is necessarily offline information. Simultaneously, most behavioral

---

[368] See Yang Wang et al., "Privacy Nudges for Social Media: An Exploratory Facebook Study," in *Proceedings of the Twenty Second International Conference on World Wide Web Companion*, 2013, 763.

[369] See Juan Pablo Carrascal et al., "Your Browsing Behavior for a Big Mac: Economics of Personal Information Online," in *Proceedings of the 22nd International Conference on World Wide Web* (Geneva, 2013).

advertising—and hence most profit—is taken from browsing patterns, which is online information.

Finally, it is possible to introduce an incentive system in order to nudge companies into nudging data subjects, which can be implemented in a similar way to how governments nudge companies into other behaviors such as taking care of the environment. Focusing on compensation instead of punishment—for instance, via partial tax exemptions—has been successful in the past. This focus can be implemented to this issue with means such as the creation of social prestige: for example, a prize to the companies that take care of their data subjects the best. Guidelines that reward companies who follow them are easier to design and to monitor than the creation of a strict regulation that imposes fines to companies who do not follow it, and they can fit with what we know about the way in which data subjects behave.

3.6.! Keeping the Money Where the Mouth Is

The chapter explained the privacy paradox and provided an economic explanation for it not considered in the privacy literature so far. This explanation bases itself on the fact that internet consumers (data subjects) seem not to have different preferences from standard consumers, but a different scenario.

The inference of self-control problems from observed choice reversals depends crucially on the absence of uncertainty.[370] As it was argued, data subjects who have a choice of whether to disclose personal information encounter a high level of uncertainty regarding the likelihood of eventual future penalties. Hence, an uncertainty-based choice reversal model with stable preferences can explain their behavior.

In turn, policy recommendations that equate non-constant discounting and dynamic inconsistency can produce welfare-decreasing

[370] See Jesus Fernandez-Villaverde and Arijit Mukherji, "Can We Really Observe Hyperbolic Discounting?," Penn Institute for Economic Research Working Paper 02-08 (Philadelphia, 2006).

outcomes if agents were in fact dynamically consistent.[371] The elimination of future choices or pre-commitment, although optimal for hyperbolically discounting agents, is rarely optimal when more information is expected to arrive in the future.[372] This arrival of future information is likely to be the case in contexts where costs depend on future behavior of other agents and where benefits largely depend on network externalities. Data subjects, when encountered with a non-exceptional change of context, many times simply change their minds.

This framework reverts the policy recommendations in favor of pre-commitment devices for data subjects that stem from the privacy paradox literature. The policy conclusions of an uncertainty-based model fit consumer claims and policy debates better than those of the hyperbolic discounting model. Pre-commitment is neither what data subjects and consumer associations demand nor what policymakers consider implementing as additional regulation for new technologies. Increasing flexibility with devices such as the right to be forgotten, and reducing of uncertainty with devices such as the requirement for informed consent, on the other hand, seem to match the demands that are currently present in the public debate.

3.7.! Appendix A to chapter 3

Formal explanation of discounting based on uncertainty

The seminal model can be used to formally show the discounting mechanism explained in the chapter.[373]

The expected utility model where the discounting is based on this risk of disappearance of the payoff—as opposed to the cost of waiting—can be illustrated as

---

[371] See Omar Azfar, "Rationalizing Hyperbolic Discounting," *Journal of Economic Behavior & Organization* 38 (1999): 245.
[372] See Manuel Amador, Ivan Werning, and George-Marios Angeletos, "Commitment vs. Flexibility," *Econometrica* 74, no. 2 (2006): 365.
[373] See Peter Sozou, "On Hyperbolic Discounting and Uncertain Hazard Rates," *Proceedings of the Royal Society of Biological Sciences* 265, no. 1409 (1998): 2015.

$$u(\tau) = u_0 s(\tau) \quad (1)$$

where u is the utility derived from the reward (or penalty), $u(\tau)$ is that utility after waiting time τ and u_0 is that utility at time 0, while $s(\tau)$ is the survival function that translates in the probability of the payoff surviving after the delay τ.

The proposed discounting mechanism can be then represented as

$$u(\tau) = \frac{u_0}{1 + k\tau} \quad (2)$$

where k is a constant whose value symbolizes discounting (the larger k the higher the discounting) and $k > 0$.

Hyperbolic discounting rates are identified with the form $\frac{x}{kt}$ as opposed to the form $\frac{x}{t}$ of regular discount functions.[374] The survival function that corresponds to this (hyperbolic) time preference function is then

$$s(\tau) = \frac{1}{1 + k\tau} \quad (3)$$

Now, say that the hazard rate (λ) is constant but unknown, and it is drawn from a known distribution $f(\lambda)$. The hazard rate is different at each period, but each time it is drawn from the same distribution, so it is neither decreasing nor increasing over time. The survival function will be the aggregation of all those hazard rates at different moments, so one can draw the survival function by direct superposition. If λ can take any value of a certain set N, and the probability of $\lambda_1$is p_1, that of λ_2 is p_2, and so forth until λ_N and p_N, then the probability of surviving until time τ is

$$s(\tau) = p_1 e^{-\tau\lambda} + p_2 e^{-\tau\lambda} + \cdots p_N e^{-\tau\lambda} \quad (4)$$

then by taking the Laplace transform of $f(\lambda)$ the survival function for the reward after a certain delay τ will be

[374] The first function converges into the second as t becomes larger.

$$s(\tau) = \int_0^{\infty} e^{-\tau\lambda} f(\lambda)\, \mathrm{d}\lambda \tag{5}$$

which defines the time-preference function precisely in the same way as hyperbolic discounting. If $f(\lambda) = a$ where $a > 0$ and f is continuous at 0, then the value of the integral should decline hyperbolically as τ increases.[375]

Now, substituting (3) into (5) we have that $f(\lambda)$ has to satisfy

$$\int_0^{\infty} e^{-\tau\lambda} f(\lambda)\, \mathrm{d}\lambda = \frac{1}{1 + k\tau} \tag{6}$$

which gives that

$$f(\lambda) = \frac{1}{k} e^{-\lambda/k} \tag{7}$$

3.8.! Appendix B to chapter 3

Experimental Design

Based on the existing experimental literature on how to distinguish between dynamically consistent diminishing impatience and dynamically inconsistent diminishing impatience,[376] an experimental design can be suggested to distinguish uncertainty-based discounting from temptation-based discounting in data subjects.

Subjects of the experiment face a series of decisions that aim to measure their preference either for pre-commitment or for flexibility. Instead of facing a choice between two alternative payments—as in traditional experiments for choice switch—each subject faces two decisions at different times: first, one at in the lab during the experimental session,

[375] Omar Azfar, "Rationalizing Hyperbolic Discounting," *Journal of Economic Behavior & Organization* 38 (1999): 245.

[376] See Marco Casari, "Pre-Commitment and Flexibility in a Time Decision Experiment," *Journal of Risk and Uncertainty* 38, no. 2 (2009): 117.

and second, one over email later on. Since subject do not need to interact, this can be done in a field experiment.

On the baseline treatment (treatment 1), each subject faces a series of choices between a smaller payment in the form of a discount in a shopping simulation accompanied by a privacy loss (*SP*),[377] and a larger payment in the form of a lower discount with the avoidance of such privacy loss (*LP*).[378] During the experimental session, subjects can either pre-commit to *LP* or postpone the choice between *SP* and *LP* to the future, deciding upon the reception of an email that will be sent to them after one week, when the payment will take place. The date of realization of the payments remains the same regardless of the choice made during the experimental session. Two variants of this choice are then introduced under separate treatments.

Treatment 2 makes pre-commitment costly. In order to do this, it incorporates a lower payment amount for the choice made during the session (with $LP' < LP$). Under this treatment, subjects choose between *LP'* and having the later choice between *LP* and *SP*, so pre-commitment is not available for free but for a cost in order to measure whether subjects are willing to pay for pre-commitment (*WTPC*).

Treatment 3 makes flexibility costly. In order to do this, instead of paying a cost to restrict the choice set, it makes subjects pay a cost to make it wider (with $LP'' = LP' < LP$). Under this treatment, subjects choose between *LP* and having the later choice between *LP"* and *SP*, so flexibility is only available at a cost, measuring whether subjects are willing to pay for flexibility (*WTPF*).

The difference between the number of subjects who are willing to decide now under treatment 2 compared to the number of subjects who are willing to do so on the baseline treatment shows how much subjects value pre-commitment in the choice. In turn, the difference between the number of subjects who are willing to decide later under treatment 3 compared to

[377] For example, a $10 discount card with the disclosure of the name and email of the person in a website.
[378] For example, a $7 discount card without the disclosure.

the number of subjects who are willing to do so on the baseline treatment shows how much subjects value flexibility in the choice

Moreover, if the number of subjects who are willing to pay under treatment 2 is higher than the number of subjects who are willing to pay under treatment 3 ($WTPC > WTPF$), then subjects have a preference for pre-commitment over flexibility. If the reverse is true ($WTPC < WTPF$), then subjects have a preference for flexibility over pre-commitment. The first shows that they discount dominantly based on temptation, while the second shows that they discount dominantly based on uncertainty.

The conjecture about the results of the experiment is illustrated in figure 2.

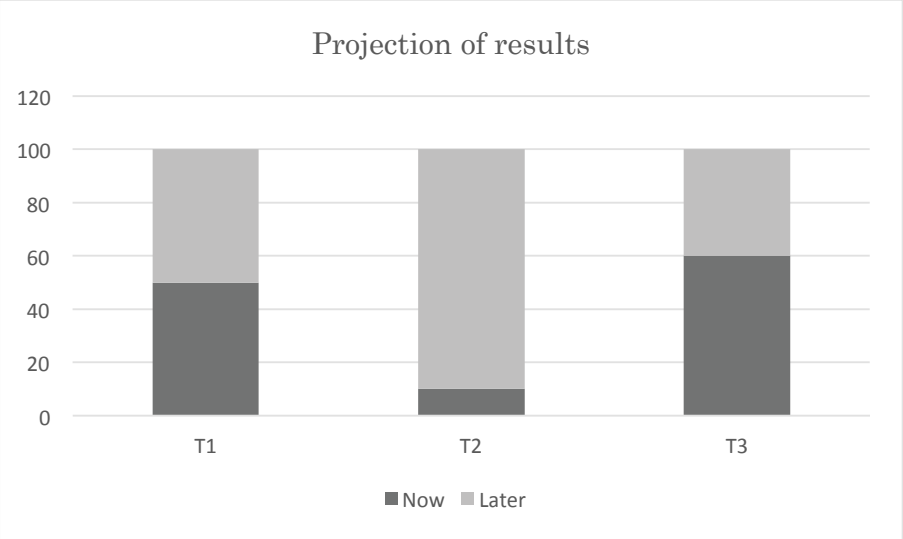

Figure 2. Illustrates expected results of the experiment proposed. Subjects who must pay for pre-commitment prefer to choose later with a significant deviation from the baseline. Subjects who must pay for flexibility prefer to choose now with a slight deviation from the baseline.

4. The Right to Be Forgotten

4.1.! The Right to be Forgotten as a Right to Erase

The right to be forgotten was popularized in the public debate by Mayer-Schönberger's story about Stacy Synder.[379] Synder was studying to become a high school teacher when one of her professors encountered a picture she had posted on her profile in a social network website drinking with a pirate hat and with a caption stating "drunken pirate." After the professor contacted the university authorities, she was expelled and disallowed to continue her studies elsewhere in the US. She sued to reverse that decision but did not succeed.[380]

Another case that motivated debate is the case of Mario Costeja, who requested Google and a Spanish newspaper to eliminate an article which reported details of a government auction on his house. The national court requested an opinion from the Court of Justice of the European Union (CJEU). The opinion of the advocate general stated that the current European legal framework does not provide a right to eliminate truthful but embarrassing information, and in addition that under the current

[379] The idea originally comes from the French *droit à l'oubli* and the Italian *diritto al' oblio* for criminal records—sometimes called right to oblivion, and literally translatable as right to forget. Both rights were affirmed by courts based on the constitutional dispositions about the social reinsertion aims of prison punishments, stating that it is in the interest of both social reinsertion and the privacy of people who were convicted for the records to be erased after some time. This works in the same lines as the 1931 US case *Melvin v. Reid*, where the court ordered the creators of the movie "The Red Kimono" to avoid using the real name of the acquitted criminal who's trial the movie is based on, focusing still not on a right to privacy but on a right to rehabilitation (see 297 P. 91, Cal. Ct. App. 1931). The same decision was made by another court in 1971 in *Briscoe v. Reader's Digest Association Inc.* (see 483 P.2d 34, Cal. 1971). However, both decisions were later on overruled for the protection of freedom of expression. See Steven Bennett, "The 'Right to Be Forgotten': Reconciling EU and US Perspectives," *Berkeley Journal of International Law* 30, no. 1 (2012): 161; Alessandro Mantelero, "The EU Proposal for a General Data Protection Regulation and the Roots of the 'right to Be Forgotten,'" *Computer Law & Security Review* 29, no. 3 (2013): 229.

[380] See Viktor Mayer-Schönberger, *Delete: The Virtue of Forgetting in the Digital Age* (Princeton: Princeton University Press, 2009). 1-15.

regulation Google is not a data controller but only a search engine.[381] As it will be seen later in this chapter, the court disagreed with his opinion.[382]

Mayer-Schönberger argued that one of the main problems of data storage is that it lacks the human characteristic of forgetting.[383] He thus proposed what can be called "the right to forget," meaning that information should have expiry dates.[384] There are several possible objections to this idea.

Firstly, there are memories (information) that indeed remain permanent in the human mind—for example, the name of one's spouse, or the birthdays of one's children. It seems implausible that policymakers would make a distinction of their retention in databases as opposed to other types of information. Secondly, humanity has been trying through history to make accurate records of information, ranging from paintings to hand written and then printed books. This has allowed us to profit from the works of ancient thinkers and historians and, more generally, to "stand in the shoulders of giants" as the much quoted phrase by Isaac Newton poses. It seems implausible for the European regulation proposal to include a pretension for societies to suddenly abandon these efforts. Thirdly, even if this idea was desirable, it is easy to elude the regulation. Information can be copied and pasted somewhere else, constituting "new" information, which could have a new expiry date. Moreover, information can be found from a different source, and information can be found in a different jurisdiction.[385]

Policymakers, especially in the European Union (EU), were sympathetic to the idea that one has a right to escape one's past, but

---

[381] This opinion was based on the interpretation of article 2(b) of the Data Protection Directive given by the ECJ in *Lindqvist*. See *Bodil Lindqvist v. Åklagarkammaren i Jönköping*, ECJ C-101/01 (2003).
[382] See section 4.3.
[383] See Ibid., 92-127.
[384] See Ibid., 169-195.
[385] For an interesting criticism of the right to forget see Daniel Solove, "A Tale of Two Bloggers: Free Speech and Privacy in the Blogosphere," *Washington University Law Review* 84 (2006): 1195.

detached from the automatic deletion of the right to forget.[386] While the right to forget focuses on the expiration of information after some time, the right to be forgotten focuses on the control over one's personal information.[387]

The right to be forgotten has been deemed to signify any of three possible things.[388] First, and least controversially, the right to be forgotten can mean that one has the right to delete information that one posts online. Many websites already allow for this. Second, it can mean that one has the right to delete any information about oneself that one originally posted online, including information that others have re-posted later on, reproducing one's initial post. This seemed to be the original intention of Reading when proposing the right.[389] Third, it can mean that one has the right to eliminate any information that is available online about oneself, regardless of its origin. This is the scope of the right to be forgotten in the GDRP.

As it is stipulated in the GDRP, the right establishes that anyone could demand information about himself to be deleted by entities that collect or process data.[390] This extends the right of data subjects allowing them to request any data controller, at any time, to eliminate from their databases any piece of information regarding that data subject, regardless of the source of the information, and regardless of whether that information produces harm. The analyses of this disposition have mainly focused on supporting it from the perspective of the human right to

---

[386] See Jeffrey Rosen, "The Right to Be Forgotten," *Stanford Law Review Online* 64 (2012): 88., 89

[387] See Rolf Weber, "The Right to Be Forgotten More Than a Pandora's Box?," *Journal of Intellectual Property, Information Technology and E-Commerce Law* 2 (2011): 120.

[388] See Peter Fleischer, "Foggy Thinking About the Right to Oblivion," *Privacy*, March 2011; Jeffrey Rosen, "The Right to Be Forgotten," *Stanford Law Review Online* 64 (2012): 88.

[389] See John Hendel, "Why Journalists Shouldn't Fear Europe's 'Right to Be Forgotten,'" *Atlantic*, January 2012.

[390] See Viviane Reding, "The Upcoming Data Protection Reform for the European Union," *International Data Privacy Law* 1 (2011): 3.

privacy, being left to evaluate its dynamics as it is drafted in the regulation and its potential consequences.

In order to perform this analysis, the next section evaluates the draft of the right to be forgotten as it would be incorporated in the European Data Protection regime by the GDRP. This is followed by an evaluation of the *Google v. Spain* case, which has been said to incorporate a milder version of such right, in section 4.3. Section 4.4 considers the potential consequences of the right to be forgotten from a law & economics perspective, and section 4.5 suggests a modification of the right to account for the different situations that it regulates and, in such way, to avoid some of its main drawbacks. Section 4.6 concludes the chapter.

4.2.! The EU Regulation Proposal

4.2.1.! Disentangling the GDRP

The right to be forgotten is incorporated to the GDRP in its article 17(1).[391] The article states that people can request data controllers to erase any piece of data that is related to them when any one of four conditions are met. The first condition is that the data are no longer necessary for the purpose for which it was collected (purpose limitation principle).[392] The second is that the data subject withdraws his consent when such consent was the legitimating basis for the collection of data.[393] The third one is that the data subject exercises his right to object.[394] The fourth is a residuary clause that includes any violation of the regulation.[395]

The new right that the right to be forgotten would incorporate in the European data protection system is captured by the second condition of the article, and to some extent the fourth. This is, by the withdrawal of consent of a data subject without need to prove harm. The other three

[391] See also recitals 53 and 54.
[392] Article 17(1)(a).
[393] Article 17(1)(b).
[394] Article 17(1)(c).
[395] Article 17(1)(d).

conditions are already present, although not systematically, in the Data Protection Directive.[396] While the first and the fourth condition of article 17 seem clear, the second and third condition, which are the most controversial since they allow data subjects to require the elimination of data without a violation of the regulation, can benefit from some explanation.

The second condition refers to article 6(1) of the proposal, which determines in which cases it is legitimate to collect or to process personal data, and in particular to its part (a), which refers to consent. Data subjects can hence request the elimination of their personal data based on a change of mind according to the article, but only when their consent was originally the legitimating basis for acquiring (or processing) their personal data. If the data were acquired based on legitimizing reasons other than consent,[397] then article 17(1)(b) is not applicable. This is a significant limitation since sections (b) to (f) of article 6(1) contain legitimating purposes that could be applicable; concretely, the performance of a contract,[398] the existence of a legal obligation,[399] vital interest of the data subject,[400] public interest,[401] and legitimate interests of the data controller.[402]

Regarding the third condition, it refers to the right to object, currently recognized in article 14 of the Data Protection Directive,[403] with the requirement of proving compelling legitimate grounds relating to a particular situation. The proposal stipulates it in article 19, which

---

[396] See Meg Ambrose and Jeff Ausloos, "The Right to Be Forgotten Across the Pond," *Journal of Information Policy* 3 (2013): 1. See also section 4.3.
[397] Sections (b) to (f) of article 6(1).
[398] Article 6(1)(b).
[399] Article 6(1)(c).
[400] Article 6(1)(d).
[401] Article 6(1)(e).
[402] Article 6(1)(f). The article clarifies that those legitimate interests cannot override the rights of data subject (which could not be otherwise since any interests that do so would not be legitimate) and mentions special protection for minors.
[403] Directive 1995/46/EC

contemplates two situations in which a data subject can object to the use or processing of his data.

The first part of article 19 refers to situations in which the data were acquired based on vital interest of the data subject, public interest, or legitimate interests of the data controller,[404] "unless the controller demonstrates compelling legitimate grounds for the processing which override the interests or fundamental rights and freedoms of the data subject."[405] This requirement excludes data acquired based on consent,[406] on contracts,[407] and for the carrying out of a legal obligation.[408] Data acquired based on consent[409] needed not to be included in the disposition because this is already done by the second condition of article 17(1). However, it is salient that there is no right to ask for the deletion of data when the legitimating basis is the performance of a contract or a legal obligation of the data controller, while there is a right to ask for deletion when there is a vital interest of the data subject to keep it, public interest or legitimate interest of the data controller.[410]

The second part of article 19 refers to the situation where the data are processed for marketing purposes (i.e. behavioral advertising),[411] independently of the legitimizing means of their acquisition. Hence, it covers all legitimizing means,[412] not only those covered by the first part of the article. The disposition turns then redundant for any information acquired under consent,[413] which is covered by the second condition of article 17(1), and any information acquired under vital interest of the data

[404] Sections (d) to (f) of article 6(1).
[405] Article 19(1).
[406] Article 6(1)(a)
[407] Article 6(1)(b).
[408] Article 6(1)(c).
[409] Article 6(1)(a).
[410] The regulation does not specify the grounds that can override fundamental rights of data subjects. These grounds, however, could not be a legal obligation, public interest, a vital interest of the data subject, or legitimate interest of the controller, because if they were so then the article would then be contradictory.
[411] Article 19(2).
[412] Article 6(1).
[413] Article 6(1)(a).

subject, public interest or legitimate interests of the data controller,[414] which are covered by the first part of the article. The right is already granted for those cases by other dispositions without making it conditional on the data being used for marketing. It is then relevant only for data acquired under a contract[415] and a legal obligation[416]—the loopholes identified in the previous paragraph. This requirement leaves two interpretative options: either data controllers have the duty to eliminate data subject's information that they must store due to a legal obligation, and thus breach that legal obligation, but only when that data has been used for marketing; or there is a mistake in article 17(1)(c) and the reference should not be to article 19 in general but to article 19(1) only.

Two additional facts should be noted about article 19. The first is that the article only mentions a duty to stop using or processing data—the right to object—but not eliminate it, so there is no duty to eliminate based on article 19 itself but only based on the reference article 17(1)(d) makes of article 19. The second is that the exceptions contained in it apply only to article 17(1)(d), which references it, and not to article 17(1) (a) to (c).

4.2.2.! Discussion

Given its interrelation with articles 6(1) (a) to (f) and 19(1), the final disposition of 17(1) seems to be the following. The general rule is that any person can request a data controller at any time to eliminate data that can be traced back to himself, unless (exemption 1) that data are being processed in the carrying of a legal obligation of the data controller or (exception 2) there is some (undetermined) legitimate ground to override the fundamental rights of the data subject. Even if one of the former exceptions are applicable, the data subject can require the elimination of the data if (exception to the exceptions 1) the data were acquired based on direct consent of the data subject, (exception to the exceptions 2) they are no longer needed for the purpose for which they were collected, or

[414] Article 6(1) sections (d), (e) and (f).
[415] Article 6(1)(c).
[416] Article 6(1)(d).

(exception to the exceptions 3) their storage violates any other part of the regulation.

Table 1 captures this formulation structuring the right to be forgotten based on the sections of article 17, while Table 2 does so by structuring it from the legitimating basis for processing.

Fact	**Condition**	**Exception(s)**
Data are no longer necessary for purpose	-	-
Consent is withdrawn	Basis for processing was consent	-
Right to object	Basis for processing was (i) Vital interest of the subject, (ii) public interest, or (iii) legitimate interest of controller.	Compelling ground to override fundamental rights and freedoms
Regulation is violated	-	-
Data are used for marketing	-	-

Table 2. The right to be forgotten in the GDRP structured by the fact that can trigger it.

Basis for processing	**Right to be forgotten**	**Exception(s)**
Consent	Always	-
Contract	When (i) Data are no longer necessary for purpose, (ii) regulation is violated, or (iii) data are used for marketing	
Legal obligation		
Vital interest of the subject	When no ground to override fundamental rights and freedoms	(i) Data are no longer necessary for collection purpose, (ii) regulation is violated, or
Public interest		
Legitimate interest of controller		

		(iii) data are used for marketing

Table 3. The right to be forgotten in the GDRP structured by basis of processing

Article 17(1), as it can be seen, can lead to some questionable results. Namely, in the framework of the EU it is unorthodox to establish an undetermined possibility to override fundamental rights, and a possibility to force a data controller to breach legal obligations to keep data if such data were used for marketing. It is easy to imagine situations in which information that was initially collected for marketing becomes socially useful and hence desirable to remain in storage. Some of these situations are mentioned in other sections of the regulation itself but not incorporated in the disposition.

4.2.3.! General exceptions for data subjects

Notwithstanding the exceptions and conditions established in article 17(1) for the different justifications for right to be forgotten, the proposed regulation also establishes general exceptions applicable to all of them, which attempt to reconcile the right with otherwise conflicting principles. Article 17(3) establishes five exceptions for the right to be forgotten specifically: freedom of expression,[417] public interest in public health,[418] research purposes,[419] a legal obligation to retain the data by the Union or a Member State (MS),[420] and the variety of cases in which processing data should be restricted instead of eliminated.[421]

The first exception—freedom of expression—refers to article 80 of the proposed regulation, which addresses the issue of freedom of expression. Article 80, however, only indicates that MS must establish some exceptions that reconcile the right to privacy with freedom of

[417] Article 17(3)(a), referring to article 80.
[418] Article 17(3)(b), referring to article 81.
[419] Article 17(3)(c), referring to article 83.
[420] Article 17(3)(d).
[421] Article 17(3)(e), referring to article 17(4).

expression—and notify the EC of such dispositions. Making the right to be forgotten compatible with freedom of expression is one of the cruxes of the former, since freedom of expression is the basis for one of the main criticisms to the right. This makes the delegation problematic given that the proposed regulation does not provide concrete guidelines for it,[422] and MS could have large differences in implementing it, resulting in different scopes for the right which would defeat the purpose of having a unified, rather than harmonized, DPL.

The second exception—public health—refers to article 81, which has three parts. The first part, which is the most relevant, refers to the exception of health purposes for the prohibition to process sensitive data[423]—to clarify the disposition.[424] The second part reaffirms the exception of research purposes[425] to which the article treats as a fourth case, and the third part refers to the delegation of power of article 86.

The third general exception—research purposes—refers to article 83.[426] The article allows in its first part for personal information to be processed for historical, statistical or scientific research[427] when (i) this cannot be done with anonymous data[428] and/or (ii) the data that identifies the data subject is kept separately when possible.[429] In its second part, the article establishes that the data processed for these conditions can be publicly disclosed[430] when (i) there is consent,[431] (ii) disclosure is necessary to present findings or facilitate further research,[432] and/or (iii) the data subject publicly disclosed the data.[433]

---

[422] While recital 121 also refers to the matter, it is not specific.
[423] Article 9(2)(h).
[424] See also recitals 122 and 123. It would improve clarity, if back-references are used, that the article also referred article 17(3)(b) together with article 9(2)(h).
[425] Article 83.
[426] See also recitals 125 and 126, referring to the topic although not specifying matters further.
[427] Article 83(1).
[428] Article 83(1)(a).
[429] Article 83(1)(b).
[430] Article 83(2).
[431] Article 83(2)(a).
[432] Article 83(2)(b).
[433] Article 83(2)(c).

The fourth exception—obligation to retain data—refers to a legal obligation by the EU or by a MS. In that respect, it is similar to the exception of carrying out of a legal obligation,[434] but it is more restrictive. While article 6(1)(c) refers to any legal obligation, article 17(3)(d) requires that such obligation is made by the Union or by a State that is member to it. The article also adds that if the legal obligation derives from a law of a MS it should meet an objective public interest, respect the essence of the right and be proportional, although this requirement would be applicable to any law and not only to those referring to the right to be forgotten.

The last general exception refers to article 17(4), which contemplates four situations under which, instead of eliminating the data, the data controller should restrict its processing. The first one is when the data subject challenges the accuracy of the data during the period in which the controller verifies its accuracy.[435] The second is when the data has to be maintained for proof purposes.[436] The third one is when the data subject asks for the restriction in the processing of data instead of its deletion when its processing does not have a legitimate basis.[437] The last one is when the data subject provided the data himself (consent or contract) and he invokes his right to data portability.[438]

In addition to this, in a continuation of the policy in European DPL to give sensitive information a special protection,[439] article 9 prohibits the processing of data "revealing race or ethnic origin, political opinions, religion or belief, trade union membership, and the processing of genetic data or data concerning health or sex life or criminal convictions or related security measures."[440] The exceptions for this prohibition are consent,[441]

---

[434] Article 6(1)(c).
[435] Article 17(4)(a).
[436] Article 17(4)(b).
[437] Article 17(4)(c).
[438] Article 17(4)(d).
[439] Sensitive information is given a stricter protection by article 8 of Directive 1995/46/EC.
[440] Article 9(1).
[441] Article 9(2)(a).

exercise of a legal obligation,[442] exercise of a right of employment law,[443] protection of the vital interests of the data subject or someone else unable to give consent,[444] activities of a non-profit body regarding its members,[445] data made public,[446] legal claims,[447] public interest,[448] health purposes as defined in article 81,[449] scientific purposes as defined in article 83,[450] and data for security measures processed by an official authority.[451]

Although article 9 does not provide a right to eliminate personal information processed in breach of this prohibition, this information falls in the general reference of article 17(d) and hence the situations in article 9 are covered by the right to be forgotten under the proposed regulation.

While most exceptions of the article seem reasonable, the exception of article 9(2)(e)—data made public—seems problematic. Companies can process, according to the provision, personal data about a data subject on sensitive topics without his consent if he manifestly made it public. However, this exception only applies for this type of data and it is not present in the general exceptions. Hence, data controllers can process sensitive data—for which the regulation attempts more protection—without the data subject's consent when it was made public, but they cannot process non-sensitive data—for which the regulation attempts less protection—under the same situation.

4.2.4.! Connected duties of data controllers

Having described how the proposed regulation establishes the right, it is left to see how this right affects the duties of data controllers in the

[442] Article 9(2)(b).
[443] Article 9(2)(b).
[444] Article 9(2)(c).
[445] Article 9(2)(d).
[446] Article 9(2)(e).
[447] Article 9(2)(f).
[448] Article 9(2)(g).
[449] Article 9(2)(h).
[450] Article 9(2)(i).
[451] Article 9(2)(j).

disposition. Due to the close relation between rights and obligations, this element will also affect data subjects' possibilities to enforce their right.[452]

The main article for this is article 17(2)—which refers to duties of data controller. The disposition states that, when a data subject expresses his will to exercise his right to be forgotten, the controller who is responsible for the publication of the data must take all reasonable measures to eliminate the data and to communicate to other parties who are processing the data to eliminate it as well.

The most relevant aspect of this rule is that it is a negligence rule. The controller is not responsible for the result—the actual elimination of data—but for undertaking reasonable means for such result. Therefore, data controllers are not liable if they took reasonable means and the information is still on the internet.

On the one hand, the presence of a negligence rule should mitigate a portion of the controversy over the right to be forgotten. Some of its participants are weary of the right due to the duty it imposes on data controllers to eliminate information that has disseminated over the internet since, being out of their database, it is difficult when not impossible for data controllers to eliminate it. Even though the scope of the reasonable means to which the regulation refers is still to be determined, a negligence rule in the matter is significantly less burdensome for companies than the strict liability rule that the objection seems to imply. The requirement of reasonable means of a negligence rule excludes by definition these difficult technical situations in which controllers cannot eliminate the data.

On the other hand, this negligence rule significantly limits the right to be forgotten that data subjects seem to acquire with few limitations in article 17. If data controllers face a negligence rule and not a strict liability rule, then data subjects do not have a right to be forgotten in a strict sense,

---

[452] See Wesley Newcomb Hohfeld, "Some Fundamental Legal Conceptions as Applied in Judicial Reasoning," *Yale Law Journal* 23, no. 1 (1913): 16; Wesley Newcomb Hohfeld, "Fundamental Legal Conceptions as Applied to Judicial Reasoning," *Yale Law Journal* 26, no. 8 (1917): 710.

but only a right to request data controllers to display reasonable means for the deletion of their information.

4.2.5.! The right to be forgotten in Europe

As it was seen, the European Commission (EC) issued a communication to the European Parliament in 2010 stating that, although the core principles of the Data Protection Directive are still valid, a new regulation is needed to enhance data protection in order to address the impact of new technologies.[453]

The right to be forgotten has been a concrete topic of policy debate in the EU since then,[454] its importance increasing since Commissioner Reding presented the GDRP in 2012.[455] Although the regulation proposal follows the general principles of the Data Protection Directive as requested by the EC, it incorporates additional elements, the most relevant of them being the right to be forgotten.[456] In commissioner Reading's words, "if an individual no longer wants his personal data to be processed or stored by a data controller, and if there is no legitimate reason for keeping it, the data should be removed from their system."[457]

One of the central elements of the regulation regarding the right to be forgotten, if not the central element, is the second condition of article 17(1), which incorporates in the European data protection system the possibility to revoke consent without the need to prove harm. This

---

[453] See European Commission, "A Comprehensive Approach on Personal Data Protection in the European Union," *Communication from the Commission to the European Parliament, the Council, The Economic and Social Committee and the Committee on the Regions*, November 2010. See also chapter 1.

[454] In the US a similar right to the right to be forgotten has also been proposed but limited to children, through an amendment to the Children's Online Privacy Protection Act.

[455] See European Commission, "Proposal for a Regulation on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data," 2012.

[456] The similar right to erasure is already present in article 12(b) of the Directive, but the proposed regulation would impose significant modifications on it.

[457] Viviane Reding, "The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age," *Speech 12/26 at the Innovation Conference: Digital, Life, Design* (Munich, January 24, 2012).

condition refers to the article that defines the legitimate collection and processing of personal data, particularly as it pertains to consent. This means that, in situations where the subject's consent was originally the basis for acquiring or otherwise processing the data, data subjects could request the elimination of their personal data from a database, based solely on a change of mind and without needing to prove to a court that the subject suffered actual harm.[458]

Shortly after the second anniversary of the regulation proposal, the CJEU ruled on *Google v. Spain*. [459]

4.3.! Google v. Spain

4.3.1.! The case

In 2010, Mario Costeja requested that Google and the Spanish newspaper La Vanguardia remove two articles published January 19, 1998 and March 9, 1998 (along with the corresponding links in the search engine) that reported details of a government auction on his house due to his failure to pay social security debts.[460]

The Spanish Data Protection Authority did not back the claim against the newspaper due to the fact that the information was published lawfully. However, it did order Google Spain SL and Google Inc. to "take steps to remove its index data and preclude future access to the same."

---

[458] If the data were acquired based on legitimizing reasons other than consent, then Article 17(1)(b) is not applicable. This limitation is relevant since parts (b) to (f) of Article 6(1) contain legitimating purposes that could be applicable; concretely, the existence of a contract (Article 6(1)(b)), of a legal obligation (Article 6(1)(c)), vital interest of the data subject (Article 6(1)(d)), public interest (Article 6(1)(e)), and legitimate interests of the data controller (Article 6(1)(f)). Directive 1995/46/EC.

[459] *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, CJEU C-131/12 (2014). Hereafter, *Google v. Spain*.

[460] See *Google v. Spain*.

Both Google Spain SL and Google Inc. appealed the resolution, and the case arrived to the court *Audiencia Nacional*.[461]

Audiencia Nacional requested a preliminary ruling from the CJEU.[462] In the request, the court was asked three questions: (i) if the European data protection framework established in the Data Protection Directive is applicable to Google, (ii) if search engines are considered data controllers under the Directive, and (iii) if a data subject can demand a search engine to remove the indexation of a certain piece of information.[463]

Regarding the first question, the advocate general and the court agree that the European framework does apply to Google, not because it is dealing with EU citizens, but because Google Spain is a subsidiary of Google Inc. situated in Spanish territory which sells advertisement spots in Spain that, in turn, finance the search engine. Therefore, even if data are not processed in Spain, the processing is done within the context of the activities of an establishment in a MS.[464] This part of the ruling confirms a previously issued opinion by A29WP, which has expressed an equivalent position for the applicable law of the directive.[465]

Regarding the second question, both the advocate general and the court noted that Google is dealing with personal information. The court further affirmed that by indexing data, Google retrieves, records and organizes data, even if Google's indexing is done automatically without distinguishing content and when this data were previously published elsewhere. Accordingly, the Court treats Google (and other search engines) as a controller, with the duties that such classification implies under the Directive.[466]

The third question is the most relevant for the purposes of this comment. The question reads:

---

[461] See Ibid. at ¶¶ 15-18.
[462] See generally TFEU, 2008 O.J. C 115/47, art. 267.
[463] See *Google v. Spain*, at ¶¶ 19-20.
[464] See Ibid.
[465] A29WP, "O.J. 8/2010 on Applicable Law" (Brussels, December 16, 2010).
[466] See *Google v. Spain*, at ¶¶ 66-88.

> *"Must it be considered that the rights to erasure and blocking of data, provided for in Article 12(b), and the right to object, provided for by [subparagraph (a) of the first paragraph of Article 14] of Directive 95/46, extend to enabling the data subject to address himself to search engines in order to prevent indexing of the information relating to him personally, published on third parties' web pages, invoking his wish that such information should not be known to internet users when he considers that it might be prejudicial to him or he wishes it to be consigned to oblivion, even though the information in question has been lawfully published by third parties?"*[467]

Regarding this question, the court considered that, if the inclusion of certain links in the search results is at some point in time incompatible with the provisions of the Directive, and the data subject requests so, such links must be erased. The Court emphasized that, due to Article 7 of the Directive, data processing must be lawful at all times in order to be allowed to be continued.[468] In addition, even information initially collected in a lawful way can—with the passing of time—become unlawful to maintain when the data becomes inadequate, irrelevant, or excessive for the purposes of the processing.[469]

For data processing to be incompatible with the Directive, the information does not necessarily have to be incorrect. It is sufficient that the data are inadequate or excessive for the purpose of the data processing, that they are outdated or that they are kept for a time longer than necessary for such purpose.[470] The court noted that sensitive information contained in sixteen-year-old search links, can fall under the aforementioned categories.[471]

As a response to the ruling, Google established a governance mechanism on May 30th through which European data subjects can now fill an online form to request that obsolete data about them be deleted from

---

[467] Ibid.
[468] See Ibid. at ¶ 95.
[469] See Ibid.
[470] See *Google v. Spain*, at ¶¶ 72, 92-9; Directive 1995/46/EC at art. 6(c)-6(e).
[471] See Ibid. at ¶¶ 94-98.

the lists of results.[472] The search engine has already received more than 70,000 requests.[473]

4.3.2.! Applicable norms

The court explains that the preliminary ruling is centrally concerned with Articles 2(b), 2(d), 4(1)(a), 4(1)(c), 12(b) and 14(1)(a) of the Data Protection Directive.[474] While Article 2 concerns definitions and Article 4 concerns applicable national law, Article 12 refers to the right to erasure and Article 14 to the right to object.[475] The latter two articles are relevant for the third question posed.[476]

The directive contains a similar right to the one proposed in Article 17 of the regulation proposal in Article 12(b) and Article 6(1)(e). However, only the second condition of that article is new.[477] Article 12(b) of the directive establishes the right to erasure, which allows data subjects to request the elimination of their personal data when its retention or processing violates the terms of the directive, in particular (but not exclusively) because of being incomplete or inaccurate.

While a narrow reading of the article will interpret "in particular" as "exclusively" and will only allow the deletion of the data when such data are incomplete or inaccurate, a broad reading will allow for such deletion whenever the data processing is in violation of any term of the directive.[478]

In turn, the directive establishes the purpose-limitation principle in Article 6(1)(e);[479] accordingly any collection, processing or storing of

---

[472] Online form at https://support.google.com/legal/contact/lr_eudpa?product=websearch

[473] See Rosa Jimenez Cano, "Google Comienza a Aplicar El 'Derecho Al Olvido,'" *El País*, July 13, 2014.

[474] See *Google v. Spain*, at ¶ 1.

[475] The court also mentions later on Articles 6, 7, 9 and 28. See Ibid. at ¶ 1.

[476] See Ibid. at ¶ 89.

[477] See Bert-Jaap Koops, "Forgetting Footprints, Shunning Shadows: A Critical Analysis of the 'Right to Be Forgotten' in Big Data Practice," *SCRIPT-Ed* 8, no. 3 (2011): 229. 230, 232-233 & 240-245.

[478] This, as it was seen, is similar to the fourth element of Article 17 of the regulation proposal. See GDRP.

[479] See generally A29WP, "O.J. 03/2013 on Purpose Limitation" (Brussels, October 2, 2013).

personal data must be done based on a specific, explicit and legitimate purpose.[480] The last of the three requirements indicates that companies need a legitimizing basis to collect personal data, of which the most common is consent.[481]

Data cannot be kept for longer than is necessary for the purposes for which it is collected or processed—a purpose that is defined, however, by the data controller. This rule is extended to secondary use, according to which the data are retained for a legitimate purpose that is different than the original purpose.[482] This obligation for data controllers and data processers can be invoked, if original purpose terms are violated, by data subjects claiming the right to erasure contained in Article 12(b) when interpreted broadly,[483] as Costeja seems to have done.

The right to object is recognized in Article 14 of the Directive. It establishes that a data subject, proving compelling legitimate grounds relating to a particular situation, can object to the continued processing of his personal data. If a data subject does object, and he can successfully prove compelling legitimate grounds, then the controller must stop processing the data subject's personal data, although is the controller has no duty to eliminate data already processed.[484]

---

[480] The Directive is applicable, according to its Article 2(a), whenever there is collection, processing or storing of personal information, where personal information is defined as any information that can be traced back to a data subject. See Directive 1995/46/EC.

[481] As it was seen, consent is defined in Article 2(h) of the Data Protection Directive as "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement." See Directive 1995/46/EC.

[482] See Bert-Jaap Koops, "The Inflexibility of Techno-Regulation and the Case of Purpose-Binding," *Legisprudence* 5 (2011): 171.

[483] See Bert-Jaap Koops, "Forgetting Footprints, Shunning Shadows: A Critical Analysis of the 'Right to Be Forgotten' in Big Data Practice," *SCRIPT-Ed* 8, no. 3 (2011): 229.

[484] Individuals have a right to withdraw their consent when they desire to, but this withdrawal only affects future processing. This means that data subjects do not have, under the current directive, the right to request the elimination of any data solely based on the withdrawal of consent. See A29WP, "O.J. 15/2011 On the Definition of Consent" (Brussels, July 13, 2011).

4.3.3.! An application of different rights

Under the classification made above on the possible interpretations of the right to be forgotten, the regulation proposal would establish the third, most expansive category of the right, while the data protection directive does not establish any of the three classifications. Under the third category, the right to be forgotten would likely involve not only the publisher of the content but also search engines that link to that content.[485] This, however, does not mean that any involvement of search engines in terms of liability for published content pertains the right to be forgotten.

As can be seen in the previous sections,[486] none of the three questions presented to the court are, strictly speaking, about the right to be forgotten. Even though the third question is related to it, and although *Audiencia Nacional* asked it mentioning the right to be forgotten,[487] the actual question refers in its formulation only to the rights of erasure and the right to object.[488]

The opinion of the advocate general Jaaskinen, in turn, is clear in stating that the rights to erasure (Article 12(b)) and the right to object (Article 14(a)) in the Data Protection Directive are not equivalent to the right to be forgotten. The opinion is categorical in pointing out that the right to be forgotten is nowhere to be found in the current EU legal framework for cases in which the publication of information is de facto legitimate. European DPL does not provide a right to eliminate truthful but embarrassing information.[489]

Even when deciding differently than the advocate general, the CJEU seems to maintain this principle in its ruling. The court extends the broad reading of Articles 12 and 14 of the directive to hold that any

---

[485] See Jeffrey Rosen, "The Right to Be Forgotten," *Stanford Law Review Online* 64 (2012): 88.
[486] See section 4.3.2, contrasted to sections 4.1 and 4.2.5.
[487] Concretely, "regarding the scope of the right of erasure and/or the right to object, in relation to the 'derecho al olvido' (the 'right to be forgotten')." *Google v. Spain*, at ¶ 20.
[488] See *Google v. Spain*, at ¶¶ 66-88.
[489] See *Google v. Spain*, at ¶ 17.

information that is no longer relevant violates the directive, and its elimination can be therefore requested by invoking the right to erasure.

The central difference between the right to erasure and the right to be forgotten is that the latter also includes data that does not breach any norm.[490] This difference might not always be as clear as it seems. A certain processing of information could be considered as breaching a general provision of the directive because it harms a data subject; or, as the court does, because it is no longer relevant, even without being outdated or inaccurate. At the margin, the difference means that with a right to be forgotten, a data subject could request the deletion of the data based on a whim, or a preference, while under the current system there are significant probative and argumentative efforts necessary to prove to a court that such data are harmful and they violate personality rights.[491]

If the right to be forgotten was enforced in the EU data protection system, a data subject's personal information would have to be deleted at his request irrespective of harm or of the legality of the processing—with differing levels of amplitude depending on which of the three versions of the right is enforced. The right, additionally, would likely cover not only links displayed by search engines but also the original publications of the content.

In the form established by Google, however, data subjects' requests must be justifiable and will be evaluated individually on their merit. In that evaluation, the company has the ability to reject them, and those who disagree with the decision made by the company will have to ask a court to intervene. In this way, the result of the case illustrates the differentiating elements between the right to be forgotten and the rights data subjects have under the directive, which someone must evaluate—in this case, Google supervised by the court. Unless European data subjects can prove a violation of the directive and the presence of harm, they will at least for now have to face being remembered.

---

[490] See Bert-Jaap Koops, "Forgetting Footprints, Shunning Shadows: A Critical Analysis of the 'Right to Be Forgotten' in Big Data Practice," *SCRIPT-Ed* 8, no. 3 (2011): 229.
[491] See Ibid.

4.3.4.! Critical discussion

Under the E-commerce Directive, internet service providers in the EU are not liable for hosting illegal content; only the users who upload the content are liable. [492] The reason behind this rule is that, otherwise, providers might find themselves forced to police the internet in order to remove content for which they could be held liable.[493] The social costs of such policing activity—both in the form of the actual costs for the company and the costs of the chilling effects it would intake—are likely to be higher than its benefit.[494] The only way to eliminate false negatives (allowing illegitimate content, which should have been removed) would be to incur in false positives (removing legitimate content, which should have been allowed), thus leading to collateral censorship.[495]

Until recently, there was a debate on whether a similar immunity would apply to the data protection directive, both for internet providers and for search engines.[496] *Google v. Spain*, as it was seen, makes it clear that for the moment it will not.

A problem with adopting this decision is that search engines such as Google work with automatic algorithms, which makes it difficult for them to become a censor of what is published and what is not published. Google localizes information but it does not control it; Google cannot make

---

[492] Directive 2000/31/EC.

[493] See Giovanni Sartor and Mario de Azevedo Cunha, "The Italian Google-Case: Privacy, Freedom of Speech and Responsibility of Providers for User-Generated Contents," *International Journal of Law and Information Technology* 18, no. 4 (2010): 356.

[494] See generally Doug Lichtman and Eric Posner, "Holding Internet Service Providers Accountable," *Supreme Court Economic Review* 14 (2006): 221; Mark Lemley, "Rationalising Internet Safe Harbors," *Journal of Telecommunication and High Technology Law* 6 (2007): 101; Keith Hylton, "Property Rules, Liability Rules and Immunity: An Application to Cyberspace," *Boston University Law Review* 87 (2007): 1; James Grimmelmann, "The Google Dilemma," *New York Law School Law Review* 53 (2008): 939.

[495] See Jack Balkin, "The Future of Free Expression in a Digital Age," *Pepperdine Law Review* 36 (2008): 427.

[496] See Giovanni Sartor, "Providers' Liabilities in the New EU Data Protection Regulation: A Threat to Internet Freedoms?," *International Data Privacy Law* 3, no. 1 (2013): 3.

any choices regarding its means and purposes in terms of Article 4(d) of the directive.

This, as the advocate general makes clear in his opinion, makes it close to impossible for Google to make sure all information it indexes complies with Articles 6, 7 and 8 of the directive on data quality. It would be one thing to shift the responsibility from the content creator (in this case, La Vanguardia) to the content indexer (in this case, Google) if (and only if) the content indexer displayed reasonable means to prevent the indexation of such content, but to place search engines as the internet's censors is something different.

Still, this is not the main problem with the *Google v. Spain* decision. The main problem is that free speech is not about being able to express oneself in a vacuum, but about being able to transmit a message to people who want to hear it.

The court argues in the case that the information indexed by Google is not relevant. But the decision begs the question of who decides what is relevant. If what information is relevant enough to be accessed is to be decided neither by people looking for such information nor by the person publishing that information, but centrally decided by a court, both freedom of expression and the right to access information will suffer a blow.

Search engines are not megaphones, sending content unilaterally to passive recipients. Search engines are an intermediary. Recipients of the information that they index choose the results they look for and they choose which web pages from those results they read. The European Court of Human Rights (ECHR), from this perspective, has mentioned that people have the right to obtain information that is of general interest, and that the internet is a key actor to obtain such information.[497]

The job of search tools such as Google is to help those internet users find the content they want to find.[498] This means that if a certain piece of

---

[497] See *Fredrik Neij and Peter Sunde Kolmisoppi v. Sweden,* ECHR 40397/12 (2013).

[498] James Grimmelmann, "Don't Censor Search," *Yale Law Journal Pocket Part* 48 (2007): 117. (further arguing that his enhances autonomy since locating

information (such as the auction of Costeja's house) appears in the top search results, it does so because a large number of internet users considered it to be relevant: they searched for it, and when finding the result they accessed it.

If there was a problem with search engines leading internet users to find unwanted content by accident, and such content was harmful for other internet users, then search engines would have incentives to correct this as fast as possible.[499] But this is not the problem the court is concerned with.

The court is concerned with people who look for such information and find it, and cobbles a solution allowing for the existence of the information but making it unavailable for the public who look for it on search engines. It is difficult to say, in such case, that the information is not relevant; moreover, it is hardly consistent to say that the information should be kept online (since it was published legally) but made inaccessible at the same time.[500]

4.4.! The Hazards of Forgetting

4.4.1.! Freedom of expression

A section of the media[501] and politicians[502] have opposed the right to be forgotten based on the idea that it conflicts with free speech, to a point in

---

information is important for making choices, and it is economically efficient by allowing numerous welfare-enhancing information exchanges that would otherwise not take place).

[499] Ibid.

[500] Ibid. (stating that if it is considered desirable to suppress the content given its harm, then one should note that the owner of the website in which it appeared will have, in most cases, better information about the content itself as well as about its truthfulness and about who created it).

[501] See, for example, Tessa Mayes, "We Have No Right to Be Forgotten Online," *The Guardian*, March 11, 2011.

[502] See, for example, Kenneth Clarke, "Data Protection (Speech)" (London, May 26, 2011).

which the right has been called "the biggest threat to free speech on the internet in the coming decade."[503]

These fears raise a series of difficult questions. The traditional doctrinal position that attempts to balance the relation between privacy and free speech is that it is against free speech, and hence not protected by the right of privacy, to prevent the dissemination of embarrassing but truthful information when that information was legitimately acquired.[504] Is there a sufficient reason to change this in online information?[505] If an individual makes a true statement about someone else through the internet, should the second have the right to request the server to eliminate the content? Why is this so for the internet and not for other massive means of communication such as the television or radio? Can one say truthful but embarrassing things about someone in a printed newspaper but not in an online newspaper?

The *Google v. Spain* case, while less intrusive than the GDPR on freedom of expression, has been criticized for overriding it, and for ignoring the ECHR case law on the balancing of the right to privacy and the right to freedom of expression,[506] and that search engines have a freedom of

---

[503] Jeffrey Rosen, "The Right to Be Forgotten," *Stanford Law Review Online* 64 (2012): 88. 88.

[504] This is mainly the doctrine of the USSC set in *Florida Star v. B.J.F.* (491 U.S. 524). It is also related to the doctrine of actual malice for freedom of the press. See "*The New York Times v. Sullivan*" (1954), "*Time Inc. v. Hill*" (1967), "*Rosembloom v. Metromedia*" (1967) and "*Gertz v. Roberts Welch*" (1974).

[505] The treatment of peer-to-peer privacy violations and provider liability varies per jurisdiction. See Mario de Azevedo Cunha, Luisa Marin, and Giovanni Sartor, "Peer-to-Peer Privacy Violations and ISP Liability: Data Protection in the User-Generared Web," *International Data Privacy Law* 2, no. 2 (2012): 1; Giovanni Sartor and Mario de Azevedo Cunha, "The Italian Google-Case: Privacy, Freedom of Speech and Responsibility of Providers for User-Generated Contents," *International Journal of Law and Information Technology* 18, no. 4 (2010): 356; Giovanni Sartor, "Providers' Liabilities in the New EU Data Protection Regulation: A Threat to Internet Freedoms?," *International Data Privacy Law* 3, no. 1 (2013): 3.

[506] Stefan Kulk and Frederik Zuiderveen Borgesius, "Google Spain v. Gonzalez: Did the Court Forget about Freedom of Expression?," *European Journal of Risk Regulation* 5, no. 3 (2014): 389.

expression claim protected by article 10 of the European Convention on Human Rights.[507]

The third category of the right to be forgotten also raises conflicts in need of balance with freedom of the press. A right to eliminate any information about oneself which is electronically stored limits the scope of people who can inform others about true facts, as it restrict such scope to those who have the approval of those involved in the piece of information. The right could be used, along these lines, as a tool for censorship.

While article 80, as it was seen, attempts to address this problem requiring MS to issue regulations that will make these rights compatible, it does not provide guidelines to do so. In turn, it seems unclear how this possibility can materialize at all without either restricting the right to be forgotten to one of the two other categories or stating that privacy in these cases simply overrides freedom of expression.

4.4.2.! Access to information

The first problem that the right would generate from the perspective of the right to access information are the prospective chilling effects that the right would produce. In the light of the strict requirements and the high fines that the regulation imposes on data processors and controllers, they might react by acting conservatively regarding data management in order to avoid large expected costs. Upon receiving a request to eliminate content, the data controller or intermediary must decide whether the request is well-founded and the content should be eliminated, or it is not and the content should remain. Allowing for a piece of information upon a request poses the risk of producing a high fine if the judgement was mistaken, while disallowing for the piece of information has no direct negative consequences. For almost all cases, this expected cost would exceed the expected benefit that such information can represent to the intermediary; when in doubt, it will be better for the intermediary to

[507] Joris van Hoboken, *Search Engine Freedom. On the Implications of the Right to Freedom of Expression for the Legal Governance of Web Search Engines* (Alphen aan den Rijn: Kluwer Law International, 2012).

delete the content even if the probability of the request being well-founded is low.[508] This would produce a chilling effect: it would reduce the flow of information in the internet, which could be socially costly and, in turn, would affect the right to access information of the same data subjects that are being protected with the right to be forgotten.

A related issue is the creation of uncertainty regarding who owns which piece of information. The right to eliminate content that refers to oneself but belongs to someone else—for example, a picture in someone's photo album where both appear—without that person's consent also raises issues regarding the property of such information, especially if the argumentation of this new right frames it as a fundamental human right.[509] Such a rule crosses a distinct line between the right to have control over one's data and the right to have control anyone's data that somehow relates to one. From that perspective, the focus changes from allowing people to control the information that they own, to giving everyone somehow involved with it a veto power.

Some information presents due to its type a high social value produced by the uses it can be given. Medical records, for instance, while containing sensitive information are valuable to determine—in aggregation—public health policies that are beneficial for the population as a whole. Criminal records can be valuable due to security reasons in crimes with high recurrence rates. Tax records are valuable to evaluate the government´s revenue and to fight tax avoidance. Electoral rolls are important for statistical purposes. There are several pieces of information that, notwithstanding freedom of speech, are needed for security reasons, innovation, art, and literature.

---

[508] The potential indirect negative consequence is that, if one assumes a competitive scenario among intermediaries, then if an intermediary eliminates a substantially larger amount of information than its competitors, and users are able to detect this, they might vote with their feet and move to their competitor if doing so is costless. This, however, is likely to have a milder effect that the risk of fines.

[509] The first recital of the proposed regulation states that "the protection of natural persons in relation to the processing of personal data is a fundamental right", and refers to article 8(1) of the Charter of Fundamental Rights of the European Union and to article 16(1) of the Treaty.

Article 83 of the proposed regulation attempts to protect the generation of "historical, statistical and scientific research." However, the proposed regulation does not define the scope of "historical, statistical and scientific research", which is a broad term. The relevance of the exception seems to require clarification. Is any record of any fact historical research? Is any quantitative study statistical research? Are student papers scientific research?[510]

More problematic is that it is not evident from the article if the conditions are cumulative or alternative. In article 83(1) it would seem that the requirements are that research cannot be done with anonymous data *and* the data that identifies the data subject is kept separately when possible—this is, that they are cumulative. Indeed, it would not be proportional, when it is sufficient to use anonymous data, to use non-anonymous data and keep the identity separate. However, in article 83(2) it would seem that the requirements are that there is consent, disclosure is necessary to present findings or facilitate further research *or* the data subject publicly disclosed the data—this is, that they are alternative. Indeed, consent is an autonomous legitimizing means in the rest of the GDRP, and it would hence not be coherent to require in this case that the data subject previously made it public in addition to giving his consent, or that disclosure is necessary in addition to the given consent. However, if one enumeration is cumulative and the other is alternative, why would the article use the exact same sentence structure? And if both dispositions have the same logical structure, are they both cumulative or both alternative?

4.4.3.! Implementation costs

The proposed right, simultaneously, presents implementation costs that would make it a costly mechanism to increase data subjects' control over their information. This overlooked aspect is not negligible, at least

[510] Moreover, is historical and statistical research not within the scope of scientific research? If it is, why are the three categories stated as separate? If it is not, what other disciplines are not considered within the scope of scientific research?

inasmuch it is relevant in order to be aware of the social cost to be paid for the right.

Firstly, the right to be forgotten is likely to present obstacles in the relation with companies from outside the EU due to the significant difference between the treatment of personal information under the proposed regulation and its treatment under other legal systems.[511] Obstacles in bilateral relations are especially likely to arise with the US, with whom the EU has signed the Safe Harbor agreement.[512] How will the proposed regulation be harmonized with the agreement? If American companies cannot invoke Safe Harbor regarding the proposed regulation, then the agreement would be rendered useless and its economic benefits would dissipate; it would be then left to see how many American companies that collect or process data continue doing business in the EU. If the so-called data giants—all based in the United States—can invoke the agreement in their collecting and processing of data, then the right to be forgotten would find itself limited to local firms, finding its utility strongly limited.[513]

---

[511] See Paul Schwartz, "The EU-US Privacy Collision: A Turn to Institutions and Procedures," *Harvard Law Review* 126 (2013): 1966.

[512] The agreement, signed between the EC and the US Department of Commerce, establishes a voluntary program for US firms to show they comply with a set of standards that is a combination of the EU and US standards on privacy. Compliance is overseen by the FTC and most claims in Europe have to be taken to the US. See Virginia Boyd, "Financial Privacy in the United States and the European Union: A Path to Transatlantic Regulatory Harmonization," *Berkeley Journal of International Law* 24 (2006): 939; Stephen Kobrin, "Safe Harbours Are Hard to Find: The Trans-Atlantic Data Privacy Dispute, Territorial Jurisdiction and Global Governance," *Review of International Studies* 30, no. 1 (2004): 111; Alexander Zinser, "The Safe Harbor Solution: Is It an Effective Mechanism for International Data Transfers Between the United States and the European Union?," *Oklahoma Journal of Law & Technology* 1 (2004): 11.

[513] Recital 79 of the proposed regulation states that the regulation should not interfere with international agreements between the Union and other countries regarding the transfer of personal data. This would indicate that, from the two aforementioned scenarios, the latter would be the case, and American companies would still be able to invoke the Safe Harbor agreement. However, since recitals do not have binding power this is still to be materialized in a binding disposition. In addition, it does not seem certain that this would cover the Safe Harbor agreement, since the recitals only refers to the transfer of data.

Moreover, the obligations adjacent to the right would increase the costs of local small and medium firms by imposing requirements such as to hire additional personnel and to consult with data protection authorities. At the same time, the limits in the use of information for advertising will reduce their profits. It has been estimated that the average small to medium firm in the EU will find its annual costs increased by 3000 to 7200 Euros, depending on the industry, which represents a 16% to 40% cost increase.[514] These increases in costs are likely to have a negative impact on business creation and on employment.[515]

At a more general level, this new right lacks a new justification. One of the fundamental lessons of economics is that transactions between consenting parties in a world where exchange is instantaneous and information is perfect is beneficial to all parties and to society as a whole.[516] Policy recommendations that foster intervention, for this reason, should attempt to identify which of these conditions is not fulfilled in order to define how to address the problem.

The right to be forgotten, aimed mainly at protecting internet consumers, would be a substantial intervention for any company that processes or stores individuals' personal data. Does this right address any market failure that justifies the intervention? More importantly, does the right address a market failure that is not already tackled by the traditional means of addressing privacy issues? Even though the right is novel, privacy protection is not. So it seems appropriate to ask whether the new technologies for data collection and data processing justify a different type of regulation; and if they do, to what extent.

---

[514] See Laurits Christensen et al., "The Impact of the Data Protection Regulation in the EU," *Intertic Policy Paper 13-1*, 2013. (Last time accessed on 09/10/2013)
[515] See Ibid. Technical implementation problems have also been pointed out. See Luiz Costa and Yves Poullet, "Privacy and the Regulation of 2012," *Computer Law & Security Review* 28, no. 3 (2012): 254.
[516] This is the central idea behind the first fundamental theorem of welfare economics.

4.4.4.! Risk compensation

A drawback that the right to be forgotten would present if incorporated in the EU which is likely to be more relevant than the previous is that, due to the technological limits to its implementation, it could induce data subjects to engage in offsetting behavior which leads to risk compensation. Based on the promise of being able to delete their information, data subjects could develop a feeling of safety that would lead them to engage in risky behavior that they would have otherwise not engaged in, and later find that the information cannot be deleted. Due to this problem, which extends to any of its three interpretations, the existence of the right could take data subjects to a situation in which they are worse off than with no right to be forgotten at all.

The main driver of this limitation is that the most relevant exposure for any type of personal data is the initial exposure in which the data goes online. After such exposure, it is often not possible to take the situation back and eliminate the information permanently from the internet in general—and from the minds of those who saw it already.[517] This might not be a problem in an ideal scenario where each data subject could enforce his right to be forgotten without practical limitations, but it turns into one given the factual limitations that regulators have in the internet's context.

At a general level, this problem is present even in an ideal scenario where a legal system (such as the EU) attributes to data subjects a right to be forgotten and companies succeed in complying with their obligation to delete all requested data. A certain amount of people, in this scenario, will have already learned the information, possibly even storing either digital or analog copies, which makes it difficult if not impossible for the information to disappear.

Still, this difficulty is even more present in the current context, where the EU can regulate the content of search engines and websites in

[517] This is especially so with the advancements in search and storage mentioned before. See section 1.1.

its jurisdiction—but these are a minority, since most are based in the US—and it cannot regulate the content of search engines and websites under the jurisdiction of other countries. For this reason, the only way the EU could effectively implement the right would be moving to a model of State-monitored internet like those implemented by countries that heavily regulate it.[518] Otherwise, its users can still access the content through websites based in the US or elsewhere. While the CJEU can request Google to remove contents from Google.es, Europeans can still find the content by entering Google.com.[519]

In addition to this general problem, it is difficult at an individual level to target all companies that managed a certain disseminated content, and it is especially difficult to target all search engines that index such content. A clear example of this lays in the *Google v. Spain* case through two mechanisms: one inside, and one outside of the courtroom.

The first is the paradox of any attempt to claim privacy via the public system of administration of justice: a vastly larger amount of people know that Costeja's house was appropriated after the case that granted him the right to delete the information than before. The attempt to remove information had, in this way, the unintended effect of publicizing it further.[520]

The second mechanism is formed by the limitations that these claims have outside of the courtroom: if someone wants to read about the

---

[518] An example of this is the system in place in China. In an extreme case, this would lead to a model of closed internet such as the one in place in North Korea.

[519] The A29WP issued an opinion stating that the results should be removed from all domains, including the .com. See A29WP, "Guidelines on the Implementation of the Court of Justice of the European Union Judgment on 'Google Spain and Inc. v. AEPD and Mario Costeja Gonzalez'" (Brussels, November 26, 2014). However, this opinion is contestable, given that according to the court EU DPL was applicable not because the case dealt with European data subjects but because Google Spain—managing the results of google.es—is situated in EU territory, which is not the case of Google Inc.—managing the results of google.com. See *Google v. Spain*, at ¶¶ 19-20, and section 4.3.1.

[520] This has been called "the Streisand effect." See Yoan Hermstruwer and Stephan Dickert, "Tearing the Veil of Privacy Law: An Experiment on Chilling Effects and the Right to Be Forgotten," Preprints of the Max Planck Institute for Collective Goods (Bonn, 2013).

appropriation of Costeja's house, they only need to open Bing, Yahoo, or any other competitor of Google. These might willingly remove the links to certain content after a prominent case such as Costeja's, but it is not possible for them to know of and eliminate all content that is denounced by data subjects to Google, which means that the content will remain both in the internet and indexed by search engines.

If data subjects are not fully aware of these significant limitations, the right to be forgotten would produce in them an increased false feeling of safety when sharing personal information. They might upload and share, for this reason, more information than they would have without the incorporation of an imperfect right to be forgotten in the EU, trusting that they are able to delete it later on if they wish to do so.

This effect has been called 'the Peltzman effect' after the scholar who discovered it, originally for seatbelt regulations.[521] What Peltzman argued is that, counter-intuitively, after the introduction of the rule that mandated the use of seatbelts in the US, the frequency of car accidents increased. This occurred due to the fact that people wearing seatbelts felt safer while driving (and the law told them that with seatbelts they were safer while driving), which made them drive more recklessly than before. Peltzman's methodology has been criticized and his study remains controversial,[522] but these criticisms were said to be limited to the case study and not pertain the effect at a general level.[523] The size of the offsetting behavior will differ from case to case, and the presence of the

[521] See Sam Peltzman, "The Effects of Automobile Safety Regulation," *Journal of Political Economy* 83, no. 4 (1975): 677.
[522] See Hans Joksch, "Critique of Sam Peltzman's Study: The Effects of Automobile Safety Regulation," *Accident Analysis & Prevention* 8, no. 2 (1976): 129; Leon Robertson, "A Critical Analysis of Peltzman's 'The Effects of Automobile Safety Regulation,'" *Journal of Economic Issues* 11, no. 3 (1977): 587.
[523] See John Graham and Steven Garber, "Evaluating the Effects of Automobile Safety Regulation," *Journal of Policy Analysis and Management* 3, no. 2 (1984): 206; Sam Peltzman, "A Reply to Robertson," *Journal of Economic Issues* 11, no. 3 (1977): 672.

effect will depend on it.[524] This effect has also been found to be present in in childproof safety caps,[525] food labels disclosing health risks,[526] and medical breakthroughs such as the discovery of antibiotics.[527]

A similar effect has been experimentally shown for data subjects, who have an increased perception of control over their personal information when PETs are in place. In these situations, data subjects seem to increase their willingness to disclose to a point in which they increase the objective risk.[528] If this offsetting behavior is also substantial for the right to be forgotten—and a Peltzman effect is hence present—this would mean that the regulation in question would fail to increase data subjects' privacy.

A perfect implementation of the right to be forgotten, where all jurisdictions incorporate it simultaneously and data subjects have no search costs—being possible for them to request all entities managing or indexing that content to delete it—would not present this problem. However, the imperfect right to be forgotten that the EU can incorporate could introduce, in some magnitude, a Peltzman effect. This is largely an empirical question, which policymakers could take into account before deciding whether to incorporate the right. This effect, if present, could make the right to be forgotten not only self-defeating but also, depending on its magnitude, counterproductive.

---

[524] See Robert Crandall and John Graham, "Automobile Safety Regulation and Offsetting Behavior: Some New Empirical Estimates," *American Economic Review* 74, no. 2 (1984): 328.

[525] See Kip Viscusi, "The Lulling Effect: The Impact of Child-Resistant Packaging on Aspirin and Analgesic Ingestions," *American Economic Review* 74, no. 2 (1984): 324; Kip Viscusi, "Consumer Behavior and the Safety Effects of Product Safety Regulation," *Journal of Law and Economics* 28, no. 3 (1985): 527.

[526] See Kip Viscusi and Wesley Magat, "Informational Regulation of Consumer Health Risks: An Empirical Evaluation of Hazard Warnings," *RAND Journal of Economics* 17, no. 3 (1986): 351.

[527] See Sam Peltzman, "Offsetting Behavior, Medical Breakthroughs, and Breakdowns," *Journal of Human Capital* 5, no. 3 (2011): 302.

[528] See Laura Brandimarte, Alessandro Acquisti, and George Loewenstein, "Misplaced Confidences: Privacy and the Control Paradox," *Social Psychological and Personality Science* 4, no. 3 (2012): 340.

4.5.! Flexibility without Censorship

4.5.1.! The right under the framework

It has been shown that there are different interpretations of the right to be forgotten,[529] of which the GDRP establishes the strongest one[530] and the *Google v. Spain* case establishes none since it requires proof of harm.[531] Then, it has been shown that the right to be forgotten in general, and its implementation in the GDRP in particular, have significant drawbacks from an economic perspective.[532]

After evaluating this, the right can be seen from the perspective of the framework previously proposed[533] in order to evaluate its merits, and be able to contrast them with the aforementioned costs. It has been shown that data subjects would benefit from an increment in flexibility regarding their data management,[534] which points to an economic reason in support of the right to be forgotten, which by allowing data subjects to withdraw their consent and delete information about themselves would undoubtedly grant them flexibility regarding their personal information.

From this perspective, a right to be forgotten without the implementation problems evaluated could be seen as analogous to an inalienability rule.

A full property right includes the right of alienation, and therefore the characteristic that upon trade property is transferred.[535] An inalienability rule, on the other hand, takes alienation out of a bundle of

[529] See section 4.1.
[530] See section 4.2.
[531] See section 4.3.
[532] See section 4.4.
[533] See chapters 2 and 3.
[534] See chapter 3, particularly section 3.4.
[535] See Guido Calabresi and A. Douglas Melamed, "Property Rules, Liability Rules, and Inalienability: One View of the Cathedral," *Harvard Law Review* 85, no. 6 (1972): 1089.

rights, hence including a prohibition to transfer the good to others in a binding way.[536]

Similarly to an inalienability rule, the right to be forgotten would include the right to nullify *ex-post* any transfer of personal information which had consent of the data subject as a legitimizing basis. In such way, it would include the possibility to retract the good offered (personal information) without returning the good obtained (use of a product).[537] Under a full property rule of informational privacy, transfers of private information would be binding for the data subject offering such information, who would not be able to take it back without the consent of the person he contracted with. Under an inalienability rule, on the other hand, the data subject would be able to nullify the transfer and obtain the information back. This ability to claim back the exchanged good is functionally equivalent to the power that would be given to data subjects by the right to be forgotten.

As it was seen, property rules over personal information were considered under the suggested framework to be too protective for informational privacy.[538] This is even more so with an inalienability rule, which would imply a higher level of protection than a property rule. It has been argued that data protection presents a convex function with respect to the amount of information available, and that both a zero protection rule and an absolute protection rule would reduce the amount of information available.[539] For this reason, the right to be forgotten would be considered too protective if the objective is to increase information flow.[540]

---

[536] See Ibid.; Randy Barnett, "Contract Remedies and Inalienable Rights," *Social Philosophy and Policy* 4 (1986): 179.

[537] This would be, in some sense, similar to a permission to breach a contract, if privacy policies were taken to be so.

[538] See section 2.4.2.

[539] See chapter 2, in particular section 2.3.

[540] This coincides with the argument that informational privacy does not fit within the traditional justifications for inalienability given from an economic perspective. See Kenneth Arrow, "Gifts and Exchanges," *Philosophy & Public Affairs* 1, no. 4 (1972): 343; Susan Rose-Ackerman, "Inalienability and the Theory of Property Rights," *Columbia Law Review* 85, no. 5 (1985): 931; David Andolfatto, "A Theory of Inalienable Property Rights," *Journal of Political Economy* 110, no. 2 (2002):

This theoretical prediction falls in line with the concrete concerns expressed regarding freedom of expression and access to information,[541] and is confirmed by experimental data suggesting that the right to be forgotten does not reduce chilling effects of information sharing.[542]

4.5.2.! An alternative formulation of the right

To this one can add one last consideration regarding the scope of the right. The right to be forgotten regulates simultaneously two situations that involve different agents in the interaction. First, there is the case of someone sharing personal information about himself and then wanting to delete that information—for example, Stacy Synder. Second, there is the case of someone sharing information about someone else, and that second person wanting to delete that information—for example, Mario Costeja.

These situations present different incentive structures with different costs and benefits. The first involves a degree of relevance for flexibility, while the second does not. One can ask, due to this, if it is possible to formulate an alternative version of the right that can maintain that benefit while avoiding its larger costs.

The main economic reason in favor of the right, it was argued, is that data subjects acquire an additional flexibility that is helpful when dealing to the uncertain hazard rate that sharing personal information implies. That reason refers to the first of the two situations that are regulated by the right. The most important costs of the right, however, refer not to data subjects' ability to eliminate the information they upload themselves, but the conflicts the right presents when allowing someone to eliminate data that has been uploaded by someone else. It is when one allows people to delete information which is shared by someone else that

382; Shi-Ling Hsu, "A Two-Dimensional Framework for Analyzing Property Rights Regimes," *University of California Davis Law Review* 36, no. 4 (2003): 813; Lee Anne Fennell, "Adjusting Alienability," *Harvard Law Review* 122, no. 5 (2009): 1403.

[541] See sections 4.4.1 and 4.4.2.

[542] See Yoan Hermstruwer and Stephan Dickert, "Tearing the Veil of Privacy Law: An Experiment on Chilling Effects and the Right to Be Forgotten," Preprints of the Max Planck Institute for Collective Goods (Bonn, 2013).

the right presents conflicts with freedom of expression, freedom of press, right to access information, and welfare impacts in the form of obstacles regarding chilling effects and potential harms to valuable information.[543]

Although this means that there are arguments to consider that the right to be forgotten has an economic reason behind it, this reason would not include cases in which freedom of expression is concerned, since flexibility is only relevant when one is evaluating whether to disclose information about oneself. The problematic that the second situation currently approached by the right to be forgotten presents (information published about others) is the potentiality of a negative externality from the publisher of the data to the person to whom the data refers. This is an equivalent externality to those which traditional tort law internalizes, which seems to indicate that this branch of law is sufficient to internalize this problem as well. Moreover, the situation presents an incentive structure that is not modified by the technological developments which motivate DPL: publishing information about someone else in an online newspaper and in a physical newspaper introduce, essentially, the same challenges for privacy, freedom of expression and access to information.

In these lines, an alternative formulation of the right can be suggested. One could propose a version of the right to be forgotten where data subjects can request data processors and data controllers to eliminate the content they shared themselves, while not extending this right to information that was shared by others. This formulation is equivalent to the first, more restrictive interpretation of the right. In turn, it is supported by the intuition that it is often appropriate to have two different regulations where there are two different situations involving different actors with different incentives. The second case, in which someone shares information about someone else, can also present problems, but these are similar to the problems generated by newspapers, photo cameras and

[543] The Peltzman effect would remain.

televisions, and which traditional privacy law has been able to address long before the existence of DPL.[544]

This tailored alternative presents the advantage of avoiding most of the mentioned costs of the right to be forgotten. While it strips internet users of some of the benefits they can derive from the right in the proposed regulation, it maintains the benefit of flexibility, which seems to be the main welfare gain from the right.

This proposal, in addition, is in line with the suggestion made before that, in order to incentivize information, there should be a higher level of protection where consent is the basis for data processing than in those cases where external parties incurred in costs to develop such information, and with the argument that in order to incentivize the generation of information some property interests should be granted to the creator of information, independently of whom the information is about.[545]

A limitation that the right could present in any of its forms is that it might create a risk compensation problem. It is not always possible to take information back, even when exercising a right to be forgotten. If data subjects are not fully aware of this, they might have a false feeling of safety when sharing personal information, and this effect could turn the right useless or even counterproductive, depending on its magnitude.[546]

4.6.! A Step in the Right Direction?

The chapter shows some unintended consequences of the main policy change of the last decade regarding privacy. In the way in which is it formulated in the regulation proposal, the right to be forgotten overrides freedom of expression and access to information, has large implementation

---

[544] These are similar but not identical, since technology has also reduced the cost of acquiring information. However, there is an argumentative step to be made between the reduction of this cost and a regulation such as the right to be forgotten in its ample interpretation.
[545] See section 2.5.4.
[546] See Sam Peltzman, "The Effects of Automobile Safety Regulation," *Journal of Political Economy* 83, no. 4 (1975): 677.

costs, and could introduce a risk compensation problem that has the potential of making it self-defeating.

The question that is left to answer is then how much are data subjects willing to pay for the increase in flexibility that the right to be forgotten represents, both in the form of sacrificing parts of other fundamental rights such as freedom of expression and access to information, and in the form of the social costs of monitoring that such measures would imply. The answer to this question will determine if a society will prefer mild regulations focusing on transparency,[547] or if it will prefer the possibility for its members to be forgotten.

Data subjects in a society could be willing to sacrifice a lot, leading to public-interest driven policymakers to accept the regulation proposal as it is. Also, they could also be willing to sacrifice less, leading the same policymakers to modify the scope of the right to one of the two more restrictive interpretations, in which one has the right to delete what one uploaded but not the right to delete information uploaded by someone else. This would retain the risk compensation problem but it would eliminate the frictions with freedom of expression and access to information, together with most of its costs. Finally, by accepting that the right to be forgotten cannot be properly enforced by one jurisdiction alone, they could be willing to sacrifice little or nothing at all, and abstain from incorporating the right to be forgotten in any of its forms. These options present, after all, a societal choice that depends on the values that are placed on each of these rights, which makes it unsurprising that some jurisdictions (such as the EU) are discussing strong version of the right while others (such as the US) are not considering the right at all.

The right to be forgotten can mean different things in the European data protection regime, among which the GDRP seems to pertain to the stricter one and *Google v. Spain* seems to pertain to none. The case is centrally about defining the legal obligations of intermediaries such as search engines under the directive. In it, the CJEU dictates that the

[547] See section 3.5.2.

processing of data, which is no longer relevant, violates the terms of the directive and extends the right to erasure and the right to objection to include search engines as a consequence of considering them data controllers (question 2) who fall under the jurisdiction of the European data protection system (question 1). Defenders of freedom of expression might be relieved. One should not forget, still, that it can be dangerous to censor search.

4.7.! Appendix to chapter 4

Proposed modification of article 17(1)

Article 17

Right to be forgotten and to erasure

1.! The data subject shall have the right to obtain from the controller the erasure of their personal data and the abstention from its further dissemination, especially in relation to personal data which are made available by the data subject while he or she was a child, where one of the following grounds applies:

a.! the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

b.! the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1);

c.! the storage period consented to has expired;

d.! there is no legal ground for processing of the data.

5.! Online Tracking

5.1.! Regulating Cookies for Online Tracking

Most of the content on the internet is financed through advertising.[548] From this perspective, it is advertisers, and in particular online behavioral advertisers, who receive the main benefits from tracking devices such as cookies. Unlike methods of mass advertising such as billboards, the internet is able to show personalized content. Having more information about data subjects' interests, companies are able to increase the relevance of advertisements, targeting the particular interests of the person to whom the advertisement is shown. This increase in relevance allows for an increment in sales, and in turn for a higher rent for advertising spots, allowing for an increment in revenue both for sellers and websites. The click-through rate of advertisements (the fraction of visitors that click on them), commonly used as a measure of their success, has been shown to increase by approximately 670% with online behavioral advertisement compared to traditional advertisements.[549]

The most commonly used devices for this function are cookies. Cookies are small text files that websites send to their visitors' devices—such as a computer, a tablet, or a smartphone—where they are stored. Cookies, later on, allow these websites to identify the device when it visits the website again, remembering some details about the interaction. Their function is to identify devices for websites.

There are two main types of cookies. Session cookies disappear when the browser is closed, while permanent cookies remain in storage. The latter has several sub-types, such as third-party cookies, which automatically send the information they contain to other parties. Data subjects who know how, can delete (permanent) cookies they have in

---

[548] See Lokke Moerel, *Big Data Protection. How to Make the Draft EU Regulation on Data Protection Future Proof* (Tilburg: Tilburg University Press, 2014). Chapter 1. See also Alexander Furnas, "It's Not All about You: What Privacy Advocates Don't Get about Data Tracking on the Web," *The Atlantic*, March 15, 2012.

[549] See Jun Yan et al., "How Much Can Behavioral Targeting Help Online Advertising?," in *Proceedings of the Eighteenth International Conference on World Wide Web* (New York: ACM, 2009), 261.

storage by using the options in their browsers or directly from the operating systems in their devices.

Cookies can also present benefits for data subjects. They make navigation faster, prevent people from having to enter information such as their language preferences or their username and password repeatedly, and allow for useful features such as a shopping cart. They sometimes also increase the relevance of what is shown to a data subject on the internet, disregarding useless information and potentially saving his time[550]—such as in the case of Google searches, and some advertisements that the data subject might genuinely be interested in seeing.

The main disadvantage of tracking devices is that they can make public certain pieces of information that people prefer to keep private, raising privacy concerns. This disadvantage is especially present regarding sensitive information, which typically consists of information that could be a basis for discrimination, such as racial or ethnic origin, political opinions, sexual orientation or religious beliefs.

This chapter recurs to the experience of the EU and the behavioral economics literature on default rules to shed light on the question of how we can improve existing regulations on online tracking devices such as cookies. The argument made here is that few European regulations effectively prohibited tracking unless there is a previous and explicit manifestation of consent, and they faced severe difficulties in their implementation because behaviorally biased data subjects were framed by websites into opting into the tracking system.

This framework leads to suggesting policy changes to approach online tracking. What the literature refers to as an active choice system presents itself as a strong candidate to achieve the goals of default-based policies in this case. Additionally, price theory seems to indicate that regulations could have undesirable unintended consequences unless they treat different kinds of cookies in a different way, in particular session cookies and permanent cookies. Finally, a way of tackling what the default

[550] See Weihong Peng and Jenniffer Cisna, "HTTP Cookies. A Promising Technology," *Online Information Review* 24, no. 2 (2000): 150.

rules framework indicates as a central weakness of the current implementations of the policy can be engaging web browsers, who have fewer incentives to frame data subjects than websites, as the enforcing agents of the policy, even if they are not data controllers.

The next section introduces the literature in behavioral economics on regulatory default rules, which can be used to study the online tracking regulations. Section 5.3 reviews the online tracking policy debate and some of its suggested solutions. Following this, section 5.4 explains the regulations that were made in the framework of the EU directives, with particular attention to The Netherlands and the UK, which are representative examples of implementations with explicit and implicit consent, respectively. Section 5.5 evaluates these regulations from the perspective of the behavioral literature introduced. Section 5.6 provides policy suggestions which combine this literature with the lessons derived from the Dutch and British experiences, and section 5.7 concludes the chapter.

5.2.! Regulatory Default Rules

5.2.1.! Reason to regulate

The main economic problem that appears in this interaction seems to be an asymmetric information problem. Websites know more than data subjects about the cookies that they install in their devices and data subjects do not know enough about them to be able to provide informed consent, which was identified as the aim of the regulation.

This, however, is not enough of a reason in itself to justify a regulatory intervention from an economic viewpoint, since regulation cannot always perform better than the market at solving information asymmetries. Data subjects, for example, might be able to educate themselves about the functioning of cookies in a less costly way than the one implied by a regulation about them. Websites could also have some degree of incentives to care about their users' privacy since that would

bring them more revenue from privacy-informed data subjects—even when such interest for privacy would be lower than the interest of data subjects themselves. More importantly, a change from an opt-out to an opt-in default system should not matter for well-informed and rational data subjects in a scenario where the cost of switching system is very low. This leaves us with two possibilities.

One possibility is considering that data subjects are well informed and rational. Since the costs of opting in or opting out the default system are low in this context, if data subjects are fully informed and rational then they should choose the system according to their preferences, and the number of people opting into a tracking system under a do-not-track (DNT) default should be the same as the number of people not opting out of the tracking system under a track-me default. In such a case, a regulation changing the default system would be unhelpful. Under this assumption, adopting an opt-in system with explicit consent, an opt-in system with implicit consent, or an opt-out system, would be irrelevant. What is more, since explicit consent implies more transaction costs, the most protective system would be, in this scenario, the worst alternative of the three.

The other possibility is to consider that the informational asymmetry is part of a composite problem. One could consider that data subjects not only are uninformed about the specifics of cookies, but also they do not want to be informed. This could be so because the costs of informing themselves are too high, relating to the uncertainty problem addressed before, and the costs for companies of informing consumers are also high in terms of loss of information acquired and as a consequences of profit from advertising.[551] Alternatively, it could be due to a status-quo bias—which could be caused either by reference dependence or by implied endorsement.[552] Along these lines, one could consider that—as it is

[551] See chapter 3.

[552] See Craig McKenzie, Michael Liersch, and Stacey Finkelstein, "Recommendations Implicit in Policy Defaults," *Psychological Science* 17, no. 5 (2006): 414.

explored in the following subsection—a change in the choice system is significant because data subjects tend to stick to the default rule.[553]

This would lead to an approach in which the regulatory intervention aims at protecting data subjects that do not engage in the necessary actions to protect themselves.

5.2.2.! Sticking to the default

A few years ago, Thaler and Sunstein coined the term libertarian paternalism.[554] They argued, based on different findings of behavioral economics, in favor of choice design mechanisms that nudge people into making better choices without reducing their range of options, or coercing them into choosing one thing in particular.

One way to nudge people into making a choice is changing the default option—from an opt-out system to an opt-in system, or vice-versa. Default-based policies apply the research on the status-quo bias, which indicates that, when offered a choice that contains a default, people have a tendency to remain in that default option.[555] This effect, which is relevant for nudging in choice design, is found even when the costs of switching away from the default choice are close to zero (such as ticking a box in a form the person is handed).[556]

The tendency to stick to the default choice has been found in several domains. Adherence to savings plans has been found to increase up to 50%

---

[553] See Russell Korobkin, "Inertia and Preference in Contract Negotiation: The Psychological Power of Default Rules and Form Terms," *Vanderbilt Law Review* 51, no. 6 (1998): 1583.

[554] See Cass Sunstein and Richard Thaler, "Libertarian Paternalism Is Not an Oxymoron," *The University of Chicago Law Review* 70, no. 4 (2003): 1159; Richard Thaler and Cass Sunstein, "Libertarian Paternalism," *American Economic Review* 93, no. 2 (2003): 175.

[555] See William Samuelson and Richard Zeckhauser, "Status Quo Bias in Decision Making," *Journal of Risk and Uncertainty* 1 (1988): 7; Daniel Kahneman, Jack Knetsch, and Richard Thaler, "Anomalies: The Endowment Effect, Loss Aversion, and Status Quo Bias," *Journal of Economic Perspectives* 5, no. 1 (1991): 193.

[556] See Cass Sunstein, "Impersonal Default Rules vs. Active Choices vs. Personalized Default Rules: A Triptych," Harvard Law School Working Paper 13-01 (Boston, 2013); Eric Johnson and Daniel Goldstein, "Defaults and Donation Decisions," *Transplantation* 78 (2004): 1713.

when employees are enrolled automatically.[557] The number of organ donors has been found to be much higher in countries where being a donor is the default choice—also when comparing countries with similar cultures—with differences of up to 400%.[558] The effect has been also found in insurance,[559] food choices[560] and, lastly, in online marketing, where the difference in the number of consumers who accept e-mail marketing has been found to vary up to 50% depending on the default.[561]

In contracts most rules are default rules, ultimately leaving the decision over their incorporation to the parties,[562] but in regulations defaults are a less orthodox approach. Default choices that attempt to nudge people can be either established as policy defaults or as penalty defaults. Policy defaults aim at increasing the amount of people that will choose the default option, relying on user inertia to make most people remain in the default choice.[563] Penalty defaults, on the other hand, aim at providing some private party with an incentive to provide information to another private party in order to correct for rent-seeking behavior under information asymmetries.[564] In such way, penalty defaults rely on the

---

[557] See Brigitte Madrian and Dennis Shea, "The Power of Suggestion: Inertia in 401(k) Participation and Savings Behavior," *Quarterly Journal of Economics* 116, no. 4 (2001): 1149.

[558] See Eric Johnson and Daniel Goldstein, "Medicine: Do Defaults Save Lives?," *Science* 302, no. 5649 (2003): 1338; Eric Johnson and Daniel Goldstein, "Defaults and Donation Decisions," *Transplantation* 78 (2004): 1713.

[559] See David Cohen and Jack Knetsch, "Judicial Choice and the Disparities Between Measures of Economic Values," *Osgoode Hall Law Journal* 30 (1992): 737; Colin Camerer, "Prospect Theory in the Wild: Evidence from the Field," in *Choices, Values and Frames*, ed. Daniel Kahneman and Amos Tversky (Cambridge: Cambridge University Press, 2000), 294.

[560] See Julie Downs, George Loewenstein, and Jessica Wisdom, "Strategies for Promoting Healthier Food Choices," *American Economic Review* 99, no. 2 (2009): 159.

[561] See Eric Johnson, Steven Bellman, and Gerald Lohse, "Defaults, Framing and Privacy: Why Opting In-Opting Out," *Marketing Letters* 13, no. 1 (2002): 5.

[562] See Ian Ayres and Robert Gertner, "Filling Gaps in Incomplete Contracts: An Economic Theory of Default Rules," *Yale Law Journal* 99, no. 1 (1989): 87.

[563] See Craig McKenzie, Michael Liersch, and Stacey Finkelstein, "Recommendations Implicit in Policy Defaults," *Psychological Science* 17, no. 5 (2006): 414.

[564] See Ian Ayres and Robert Gertner, "Filling Gaps in Incomplete Contracts: An Economic Theory of Default Rules," *Yale Law Journal* 99, no. 1 (1989): 87; Jason

incentives of the agent with more information to initiate a negotiation in order to persuade the other agent to switch away from the default choice.[565]

The general principle in default rules is that the default should be set in the option that the parties would have chosen if contracting was costless. In other words, the judge or regulator should rule as the parties would have decided if they had expressed their preference explicitly.[566] Both policy defaults and penalty defaults, however, stand in contrast to rules that the parties to the interaction want. The appeal of policy default rules in this context comes from a paternalistic aim to shape people's preferences.[567] The appeal of penalty defaults stems from the idea that, under a Rawlsian veil of ignorance, without knowing *ex-ante* if they will be contract drafters or contract adherents, potential parties would (*ex-ante*) have wanted the default as well—the benefit for the contract adherent would be larger than the disfavor for the contract drafter.[568]

Penalty defaults are intended, as mentioned above, for contexts of information asymmetries where the party with more information withholds that information from his counterpart engaging in rent-seeking behavior. This behavior occurs when such withholding reduces the size of the surplus to be divided between the parties, and the party withholding the information still does so in order to achieve a larger portion of such surplus for himself. This is possible when the share-of-the-pie-effect is

---

Johnston, "Strategic Bargaining and the Economic Theory of Contract Default Rules," *Yale Law Journal* 100, no. 3 (1990): 615; Ian Ayres and Robert Gertner, "Strategic Contractual Inefficiency and the Optimal Choice of Legal Rules," *Yale Law Journal* 101, no. 4 (1992): 729.

[565] See Rip Verkerke, "Legal Ignorance and Information-Forcing Rules," *William and Mary Law Review* 56 (2015): 833.

[566] See Frank Easterbrook and Daniel Fischel, "The Corporate Contract," *Columbia Law Review* 89 (1989): 1416.

[567] See Cass Sunstein and Richard Thaler, "Libertarian Paternalism Is Not an Oxymoron," *The University of Chicago Law Review* 70, no. 4 (2003): 1159; Richard Thaler and Cass Sunstein, "Libertarian Paternalism," *American Economic Review* 93, no. 2 (2003): 175.

[568] See Ian Ayres and Robert Gertner, "Filling Gaps in Incomplete Contracts: An Economic Theory of Default Rules," *Yale Law Journal* 99, no. 1 (1989): 87. 106.

larger than the size-of-the-pie effect.[569] In those cases it is efficient to set a rule that incentivizes the party to reveal the information since that will increase the size of the surplus to be divided. In an analogous way to presumptions in procedural law, penalty defaults in these contexts can sometimes counteract those incentives to strategically withhold information, making the rule attractive under a veil of ignorance.[570]

This said, default rules (both under the policy type and under the penalty type) have disadvantages. From the perspective of information, precisely because of the status-quo bias, default rules cannot express true preferences as well as active choices.[571] When people stick to a default choice, it is not always possible to know if they did so because they genuinely prefer that option or if they did so because of inertia.[572]

From the perspective of incentives, penalty defaults face the additional disadvantage that default rules have the potential of creating an endowment effect for the parties,[573] which is intended for policy defaults but not for penalty defaults. A default rule necessarily establishes a certain status-quo from which parties can negotiate away, but the establishment of such status-quo can work in such a way that the person who benefited from the default will require a higher compensation to forfeit it than that he would have offered to acquire it, even when parties

---

[569] See Ibid.

[570] See Ibid. 107.

[571] See John Payne, James Bettman, and Eric Johnson, *The Adaptive Decision Maker* (New York: Cambridge University Press, 1993).

[572] They might not know this themselves. For example, in countries where a large number of people become organ donors for not opting out in their driver's license forms (Austria 99.98%, Belgium 98%, France 99.9%, Hungary 99.9%, Poland 99.5%, Portugal 99.6%, Sweden 85.9%), compared to countries with an opt-in system for organ donation in these same forms (Denmark 4.25%, The Netherlands 27.5%, UK 17,2%, Germany 12%), it is unlikely that people would declare that their decision to become a donor was motivated by the presentation of the choice. See generally Eric Johnson and Daniel Goldstein, "Defaults and Donation Decisions," *Transplantation* 78 (2004): 1713.

[573] See Russell Korobkin, "The Status Quo Bias and Contract Default Rules," *Cornell Law Review* 83 (1998): 608.

have a clear valuation of the rights in play.[574] This means that whatever default rule is chosen, it will generate situations in which the rule stays without being the most beneficial outcome for the parties, which reduces the difference in the outcomes of mandatory rules and default rules that is suggested by traditional economic analysis.[575] Hence—as long as the objective is not to shape preferences—this general disadvantage of penalty defaults is a good reason to consider implementing a requirement for parties to select the preferred option or to set a default that is preferred by the majority, as opposed to a penalty default, when the information release generated by the default is low.[576]

Which type of default rule one will consider that was established by the amended e-Privacy Directive will depend on the aim one considers the directive has. If the aim of the directive is to reduce the overall amount of tracking devices being installed, then the default would be a policy default, while if its aim was to ensure informed consent, as it is considered here, then the default would be a penalty default. The idea that a DNT default in cookies works as a penalty default has been suggested before.[577] There are good reasons, in fact, to consider that by changing the default option into the one that is more burdensome for websites (independently of how much each option benefits consumers) the choice mechanism forces them to educate data subjects in order to get them to switch away from the default.[578]

This leads to the expectation—which might have been shared by the drafters of the Electronic Communications Framework Directive and of the Dutch cookie law—that changing the default system for cookies from

---

[574] See Russell Korobkin, "The Endowment Effect and Legal Analysis," *Northwestern University Law Review* 97 (2003): 1227; Cass Sunstein, "Switching the Default Rule," *NYU Law Review* 77 (2002): 106.
[575] See Ibid.
[576] See Russell Korobkin, "The Endowment Effect and Legal Analysis," *Northwestern University Law Review* 97 (2003): 1227; Russell Korobkin, "The Status Quo Bias and Contract Default Rules," *Cornell Law Review* 83 (1998): 608.
[577] See Jay Kesan and Rajiv Shah, "Setting Software Defaults: Perspectives from Law, Computer Science and Behavioral Economics," *Notre Dame Law Review* 82, no. 2 (2006): 583.
[578] See Ibid.

an opt-out to an opt-in will leave data subjects better informed on the functions, the advantages and the disadvantages of cookies.

5.2.3.! When default rules fail

In some cases, default rules do not give out the expected outcomes.

A condition under which default rules are likely to fail is when they trust their own application to an agent who (i) has an interest on whether the other agents involved make a choice switch, and (ii) has the power of shaping the way the default rule is presented.[579] Choice architecture can be a powerful device when policymakers design the choice mechanism but, when the choice is being designed by companies, they can often circumvent policymakers' intentions.[580] This possibility to circumvent regulation is especially attractive with penalty defaults, where the party engaging in rent-seeking behavior should find its profit reduced by the default rule.

An example of a penalty default not meeting its objective due to this mistake was the regulation for overdraft charges in the US. A national regulation required banks to obtain prior and explicit consent from their consumers (hence opting in) in order to provide them with overdraft coverage. The drafters of the regulation stated explicitly that they intended it as a default rule intended to protect consumers. However, most consumers opted-in, and the policy was considered a failure.[581]

Why was that so? When faced with the regulation, banks sent a letter to their consumers asking them if they wanted to keep their account the same and maintain the benefit they had so far of being able to withdraw money on overdraft, or to change the status of their account, by checking either yes or no in a form. The forms gave the options "yes: keep my account working the same with Shareplus ATM and debit card overdraft coverage / no: change my account to remove Shareplus ATM and

---

[579] See Lauren Willis, "When Nudges Fail: Slippery Defaults," *University of Chicago Law Review* 80, no. 3 (2013): 1155.
[580] See Ibid.; Lauren Willis, "Why Not Privacy By Default?," *Berkeley Technology Law Journal* 29, no. 1 (2014): 61.
[581] See Ibid.

debit card overdraft coverage."[582] Advertising done by banks, additionally, stated "Don't lose your ATM and debit card overdraft protection."[583]

What banks were able to do without breaching the law, in other words, was to manipulate the opt-in system into an active choice. An active choice or forced choice system is one in which agents (in this case bank clients) do not face a clear default but are faced with two alternatives from which they must choose.[584] Moreover, the choice was not neutral. Banks were able to change the perception of the status-quo and prime consumers into opting into the system by favoring one alternative in the active choice and highlighting the losses in the other.[585] The regulation failed because it did not take into account that it targeted agents (banks) who were behaviorally informed (they were aware of the effects of default rules and active choices) and whose interests were against it.[586]

For a change in the default choice system to yield the expected results people under both regimes must be treated, to the extent that this is possible, in the same way, yielding the same payoffs regardless of the choice under which they place themselves.[587] If companies are able to present their customers with increasing incentives to switch choice, then most benefits of a default system will be lost. Regulation can hypothetically establish limits on to what extent differential treatment is allowed, but those limits are difficult to establish and even more difficult to monitor.[588] The bank overdraft regulation could have been more specific in the design of the choice mechanism but it is likely that, even if in a less overt manner, banks would have found a way to re-frame the choice, and

---

[582] See Lauren Willis, "When Nudges Fail: Slippery Defaults," *University of Chicago Law Review* 80, no. 3 (2013): 1155.
[583] See Lauren Willis, "Why Not Privacy By Default?," *Berkeley Technology Law Journal* 29, no. 1 (2014): 61.
[584] See Gabriel Carroll et al., "Optimal Defaults and Active Decisions," *Quarterly Journal of Economics* 124, no. 4 (2009): 1639.
[585] See Punam Keller et al., "Enhanced Active Choice: A New Method to Motivate Behavior Change," *Journal of Consumer Psychology* 21, no. 4 (2011): 376.
[586] See Cass Sunstein, "Acceptance Speech for the Title of Honorary Doctor at Erasmus University Rotterdam," November 8, 2013.
[587] See Lauren Willis, "Why Not Privacy By Default?," *Berkeley Technology Law Journal* 29, no. 1 (2014): 61.
[588] See Ibid.

the more specific choice design would have carried high monitoring costs without ensuring a benefit. This, at is will be seen later, has implications for online tracking.[589]

5.3.! Policy Debate

5.3.1.! First considerations

The central polemic which online tracking devices generate is that they are installed on data subjects' devices without their explicit consent, which often means that they are installed without their consent at all.[590] Additionally, it has become a common practice to utilize third-party cookies, which are considered especially problematic because they allow for data subjects' data to be directly aggregated by a different website or advertising company than the one the data subject interacts with, often without his awareness.

Unlike social networks, where data subjects share their information and know who has it in storage, in the case of tracking devices it is possible that in the absence of regulation data subjects do not know who collects their personal information, and who stores it. While social networks are familiar to the data subjects whose information they retain, that is not the case for data brokers, which are not consumer-facing.

These features can, on top of the societal costs produced by the potential individual harm derived from privacy breaches, lead data subjects to consider the internet as an unsafe environment. This can lead data subjects to equate all advertising with spam or attempt to block all advertising on privacy concerns, which is an undesirable result for all agents in the interaction. This leads to the question of whether regulation

[589] See section 5.5.2.
[590] See Joasia Luzak, "Much Ado about Cookies: The European Debate on the New Provisions of the ePrivacy Directive Regarding Cookies," *European Review of Private Law* 21, no. 1 (2013): 221.

should allow websites and advertisers to continue tracking data subjects without their knowledge or consent.[591]

5.3.2.! The EU directives

The regulatory efforts regarding tracking devices such as cookies started in Europe with the Data Protection Directive (1995)[592] and continued with the e-Privacy Directive (2002)[593], the Electronic Communications Framework Directive (2009),[594] and country-level regulations made on their basis.

The Data Protection Directive—applicable whenever there is collection, processing or storing of personal information[595]—establishes the purpose specification principle,[596] according to which any collection, processing or storing of personal data must be done based on a specific, explicit and legitimate purpose. The latter indicates that companies need a legitimizing basis to collect personal data, of which the most common is consent.[597]

At the passing of the Data Protection Directive, cookies were still a new technology, having been created only one year before.[598] Under the framework of a directive that was meant for protecting personal information in general, the EU implicitly adopted an opt-out system for cookies. This meant that data subjects were considered to have given their consent for the installation of cookies unless they indicated otherwise, but

---

[591] See Lauren Willis, "Why Not Privacy By Default?," *Berkeley Technology Law Journal* 29, no. 1 (2014): 61.
[592] Directive 1995/46/EC.
[593] Directive 2002/58/EC.
[594] Directive 2009/136/EC.
[595] Directive 1995/46/EC, article 2(a).
[596] See A29WP, "O.J. 03/2013 on Purpose Limitation" (Brussels, October 2, 2013).
[597] Directive 1995/46/EC, article 2(h).
[598] Cookies were created in 1994 by Montulli and Giannandrea at Netscape. Before that, the way to trade these data was with session identifiers, which form a relatively unsafe system since there is no guarantee that only one person is using the identifier.

they had to be given an option to opt-out of the system.[599] In other words, they were given a right to refuse tracking.

After the passing of the directive, the use of cookies increased and issues of privacy in electronic commerce gained more prominence. The system in force had the problem that data subjects did not have an easy way of exercising the refusal: they could not directly tell a website to avoid installing cookies on their devices but had to use one of the available PETs to block their installation. Although this feature is now usually available in web browsers themselves, this option was not so salient and not all data subjects knew how to operate it. This led policymakers to pass the e-Privacy Directive, concerning data protection specifically in the electronic communications sector.

At the passing of the e-Privacy Directive there was a debate on whether there should be a change towards an opt-in system where data subjects' prior explicit consent is required for the use of cookies. The opt-out system was maintained mainly due to industry arguments, which claimed that the change would hinder electronic commerce.[600] As a result, article 5(3) of the e-Privacy Directive essentially repeated the requirements of the Data Protection Directive—which can be useful for clarification purposes, as they have a relation of *lex specialis* and *lex generalis*, but did not add new rights or obligations.[601] Article 5(3) reinforced the right to refuse tracking, leaving data collectors with two main obligations: to provide information about the purposes of information collection and to give data subjects the right to refuse it (opt-out).

In 2009, the Electronic Communications Framework Directive was passed introducing modifications to the e-Privacy directive and changing article 5(3). The new article requires for the installation of technologies

---

[599] See Joasia Luzak, "Much Ado about Cookies: The European Debate on the New Provisions of the ePrivacy Directive Regarding Cookies," *European Review of Private Law* 21, no. 1 (2013): 221.
[600] See Sylvia Mercado Kierkegaard, "How the Cookies (almost) Crumbled: Privacy & Lobbyism," *Computer Law & Security Review* 21, no. 4 (2005): 310.
[601] See Frederic Debussere, "The EU E-Privacy Directive: A Monstrous Attempt to Starve the Cookie Monster?," *International Journal of Law and Information Technology* 13, no. 1 (2005): 70.

that collect information that the data subject has given his consent. In this way, the article seems to indicate that consent has to be given previously, since although the word "previous consent" is not used, it refers to consent that "has [been] given."[602]

These regulations were complemented with the Working Document 02/2013 ("providing guidance on obtaining consent for cookies"), which requires that data subjects are offered a real and meaningful choice, and that websites obtain their consent before installing any cookies. According to the A29WP, the EU finally moved with the new article 5(3) into an opt-in system.[603] Still, the wording of the article does not rule-out the possibility of implicit consent, only requiring it to be previous. In the use of the terms by its interpretative authority, it seems that for an opt-in system to be in force only previous consent is necessary, being thus possible to have opt-in systems with implicit and with explicit consent. [604]

5.3.3.! Regulatory aim

The debate on tracking devices as a subject of regulatory concern emerges in the framework of privacy and data protection on the internet, which is a high priority topic in the Digital Agenda for Europe 2020.[605] In that context, the A29WP has expressed that control over one's personal

[602] This does not concern cookies specifically but is technology-neutral, and aims to regulate the tracking of data subjects by any means. This said, the directive refers to "the storing of information, or the gaining of access to information already stored", which limits its scope as it excludes tracking technologies that do not store information in a device nor retrieve information that is stored, such as some cases of fingerprinting or IP addresses. See Peter Eckersley, "How Unique Is Your Web Browser?," in *Privacy Enhancing Technologies Symposium*, ed. Mikhail Atallah and Nicholas Hopper (Berlin: Springer Lecture Notes in Computer Science, 2010), 1.

[603] A29WP, "O.J. 2/2010 on Online Behavioral Advertising" (Brussels, June 22, 2010). 13; A29WP, "O.J. 15/2011 On the Definition of Consent" (Brussels, July 13, 2011). 9, 30.

[604] In these lines, here we will consider that for an opt-in system to be in force only previous consent is strictly necessary.

[605] See European Commission, "Digital Agenda for Europe. A Europe 2020 Initiative," 2015, http://ec.europa.eu/digital-agenda/. Pillar III, action 35.

information is a central aspect of informational privacy, where control is commonly instrumented by consent.[606]

Consent is additionally mentioned as a determinant of lawfulness in the Data Protection Directive,[607] to which the e-Privacy Directive and the Electronic Communications Framework Directive refer to in the subject matter. While the same directive mentions the importance of explicit consent,[608] it does not discard the possibility to manifest it implicitly, defining it as "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement."[609]

Consent as a regulatory aim, additionally, seems deductible from article 5(1) of the e-Privacy Directive on the confidentiality of communications, which determines the rationale of article 5(3). Article 5(1) focuses on the fact that the data subject has provided consent for the interception of his communications. This idea is further confirmed by document 02/2013 of the A29WP ("providing guidance on obtaining consent for cookies").

Finally, this idea is in line with article 8.2 of the Charter of Fundamental Rights of the EU on protection of personal data, which highlights the importance of consent to ensure a right to privacy.

In sum, the aim of these regulations seems to be to ensure data subjects' meaningful consent as a requirement for online tracking.

5.3.4.! A comparison with the US

Although the US does not have yet a specific regulation on the topic to be compared with the European approach, the Federal Trade Commission (FTC) and the US Commerce Department have suggested the implementation a DNT header in browsers.[610] The header works in a

---

606 See A29WP, "O.J. 15/2011 On the Definition of Consent" (Brussels, July 13, 2011).
607 Directive 1995/46/EC, recital 30.
608 Directive 1995/46/EC, recital 33.
609 Directive 1995/46/EC, article 2(h).
610 See Omer Tene and Jules Polonetsky, "To Track or 'Do Not Track': Advancing Transparency and Individual Control in Online Behavioral Advertising," *Minnessota Journal of Law, Science & Technology* 13, no. 1 (2012): 281. This idea

similar way to the do-not-call registry, which was a list first created in the US and then incorporated by other countries in which people can subscribe to remove their telephone numbers from public lists and avoid receiving calls from telemarketers.

The DNT header is an HTTP header field that is meant to express the preference of the data subject regarding tracking—for this reason, it is often referred to as the DNT browser feature.[611] If the header is set to 1, it shows that the data subject does not want to be tracked, and if it is set to 0 it shows the data subject does not object to tracking. There is also the possibility to send no header at all, which is the default mode. All five major browsers already have this possibility embedded.[612]

While valuable, the limitations of the DNT header are significant. The header expresses a preference, but it does not block tracking devices, and websites can choose whether to respect the data subject's wishes or not. Setting the default header to 1, thus expressing that the user of the device does not want to be tracked unless he expresses otherwise,[613] would be in some way a default DNT system similar to the one implemented by the amended e-Privacy Directive, although no binding for websites. For this reason, it is understandable that some might think it is not enough to enhance data protection.

Despite pressures to incorporate a stricter regulatory approach to online tracking in the US, the FTC has confirmed that it considers DNT a feasible data protection mechanism.[614] Its 2012 privacy report states, in addition, that despite consumer inertia the difference between opt-in and

---

started in 2007 when public interest groups which focus on privacy issues (such as World Privacy Forum, CDT and EFF) requested the FTC to incorporate a DNT list for online behavioral advertising.

[611] It is also sometimes called the DNT policy, which is an inconvenient term as it is not the only possible policy that stops online tracking devices.

[612] Last year, the Tracking Protection Working Group moved DNT to "last call status", which means that from a technological standpoint it is complete and ready to be implemented. See W3C Tracking Protection Working Group, "W3C Last Call Working Draft," *Tracking Preference Expression (DNT)*, April 24, 2014.

[613] This was done, for example, by Internet Explorer.

[614] This runs contrary to the opinion of A29WP in the matter. See A29WP, "O.J. 2/2010 on Online Behavioral Advertising" (Brussels, June 22, 2010). 13.

opt-out mechanisms is not relevant for online privacy, clearly separating itself from the opinion of EU policymakers.[615]

On a different line, a legislation proposal called the Securely Protect Yourself Against Cyber Trespass Act (also called "SPY Act") has been taken to the legislative power, and is currently under committee evaluation in the US Senate. The act attempts to turn the default system for tracking devices in the US into an opt-in system.[616] In particular, the act states that, in order for tracking devices to be allowed, it is required that the data subject has consented to them.[617]

The protection mechanism of the SPY Act is equivalent to the provision of the e-Privacy Directive amended by the Electronic Communications Framework Directive. The experience that the EU had with its implementation, which follows in the next section, might then be useful not only to improve the European regulations themselves but also for other jurisdictions, to be able to incorporate the successful elements of the European opt-in system while avoiding its obstacles.

5.4.! Implementation of the Directives

5.4.1.! Differing implementations in the EU

Regarding the MS, some have chosen to stay within an opt-out system, either in breach of the amended e-Privacy Directive or in a different interpretation of it than that of the A29WP. Most, however, made modifications in their regulations.

In order to evaluate how the different MS incorporated the directive, data were gathered from their legislations and regulations (when available) to determine if MS made any modifications in their regulatory framework after the change in directive took place. The applicable norms

---

[615] See Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change. Recommendations for Business and Policymakers" (Washington, DC, March 26, 2012).
[616] Securely Protect Yourself Against Cyber Trespass Act, section (a)3.
[617] Securely Protect Yourself Against Cyber Trespass Act, section (a)(2)(A).

were searched for, together with their dates of modification, and countries were classified either under an opt-in or an opt-out system for online tracking. For the countries falling under the first, they were further classified either as opt-in with implicit consent allowed or opt-in with a requirement of explicit consent.

Implicit consent (typically used in trials) is the consideration that a certain person has agreed on an action without explicitly manifesting such agreement; he has implicitly manifested it with his actions or his inaction upon particular circumstances.[618] Although there are parallels between opt-in vs. opt-out systems and implicit vs. explicit consent—they both either give or do not give significance to inactivity—, they are not equivalent binomials. One can either implicitly or explicitly opt-in or opt-out of a certain choice, and a legal system can adopt any combination of the two binomials for a certain choice. While the first classification refers to the timing of consent, the second refers to the form in which such consent must be given.

Countries were considered to be under an opt-in system when previous consent was needed in order for websites to be allowed to track data subjects' behavior, and in an opt-out system if this requirement was not present. Countries were classified under opt-in with explicit consent if their legislations additionally required that such previous consent is explicit, and under opt-in with implicit consent if such requirement was absent or if the legislation or the regulation specified that consent can be manifested implicitly.

The following table schematizes how the directive was implemented in the different MS:

Country	Norm	Date of amendment	System	Consent	Authority	Regulation
Austria	Telecommunications Act (section 96.3)	22 November 2011	Opt-in	Implicit	Österreichische Datenschutzbehörde	No

[618] See Elizabeth Fuller, "Implied Consent Statutes: What Is Refusal?," *American Journal of Trial Advocacy* 9 (1986).

Belgium	Electronic Communications Act	28 June 2012	Opt-in	Implicit	Commission de la protection de la vie privée / Belgian Telecom Regulator (IBPT)	Yes
Bulgaria	Electronic Messages Act	29 December 2011	Opt-out	-	Commission for Personal Data Protection	No
Croatia	Electronic Communications Act (Zakon o elektroničkim komunikacijama)	15 July 2011	Opt-in	Implicit	Croatian Personal Data Protection Agency	No
Cyprus	Regulation of Electronic Communication and Postal Services Law	18 May 2012	Opt-in	Implicit	Commissioner for Personal Data Protection	No
Czech Republic	Act No. 101/2000 Coll.	1 January 2012	Opt-out	-	Office for Personal Data Protection	No
Denmark	Act on Electronic Communications Networks and Services (Act No. 169)	14 December 2011	Opt-in	Implicit	Datatilsynet	Yes
Estonia	Electronic Communications Act	Not amended	Opt-out	-	Estonian Data Protection Inspectorate	N/A
Finland	Personal Data Act (Henkilötietolaki 1999/523)	25 May 2011	Opt-in	Implicit	Office of the Data Protection (Data Protection Board)	No
France	Article 32 II of the Act of 6 January 1978	27 August 2011	Opt-in	Implicit	Commission Nationale de l'Informatique et des Libertés	Yes
Germany	Telecommunications Act	Not amende	Opt-in	Implicit	Der Bundesbeauf	N/A

		d			tragte für den Datenschutz und die Informations freiheit	
Greece	Law 3471/2006 amended by Law 4070/2012	10 April 2012	Opt-in	Implicit	Hellenic Data Protection Authority	
Hungary	Act CVII of 2011 on Communications	3 August 2011	Opt-out	-	Data Protection Commissioner of Hungary	No
Ireland	Electronic Communications Networks and Services	1 July 2011	Opt-out	-	Data Protection Commissioner	No
Italy	Article 122 of the Data Protection Code	28 May 2012	Opt-in	Implicit	Garante per la protezione dei dati personali	Yes
Latvia	Law on Information Society Services	8 June 2011	Opt-in	Implicit	Data State Inspectorate	No
Lithuania	Law on Electronic Communications	1 August 2011	Opt-in	Implicit	State Data Protection Inspectorate	Yes
Luxemburg	2005 Act on the specific provisions for the protection of individuals in relation to the processing of personal data in the electronic communications sector	1 September 2011	Opt-in	Implicit	Commission Nationale pour la Protection des Données (CNPD)	No
Malta	Legal Notice 239 of 2011	1 January 2013	Opt-in	Implicit	Office of the Data Protection Commissioner	No
The Netherlands	Telecommunications Act article 11.7a	5 June 2012	Opt-in	Explicit	College bescherming persoonsgegevens	Yes

Poland	Telecommunications Law	22 March 2013	Opt-in	Implicit	Bureau of the Inspector General for the Protection of Personal Data	No
Portugal	Law 46/2012 amending Law 41/2004	29 August 2012	Opt-in	Implicit	Comissão Nacional de Protecção de Dados	No
Romania	Ordinance 13/2012 amending Law 506/2004	26 April 2012	Opt-out	-	National Supervisory Authority for Personal Data Processing	No
Slovakia	Act on Electronic Communications	1 October 2011	Opt-in	Implicit	Office for Personal Data Protection of the Slovak Republic	No
Slovenia	Electronic Communications Act (ZEKom-1)	15 January 2013	Opt-in	Implicit	Information Commissioner	Yes
Spain	Information Society and Electronic Commerce law (34/2002) amended by Royal Decree 13/2012	2 April 2012	Opt-in	Implicit	Agencia de Protección de Datos	Yes
Sweden	Electronic Communications Act (Sw. lagen om elektronisk kommunikation, 2003:389)	1 July 2011	Opt-in	Implicit	Datainspektionen	Yes
UK	Regulation 6 PECR	26 May 2011	Opt-in	Implicit	Office of the Information Commissioner Executive Department	Yes

Table 4. Summarizes incorporation of the directive by EU country and classifies them by system.

Five years after the passing of the Electronic Communications Framework Directive, its implementation in the EU has occurred in the following way: there are six MS that decided to stay in an opt-out system (Bulgaria, Czech Republic, Estonia, Hungary, Ireland and Romania), twenty one that have incorporated an opt-in system but allowing for implicit consent (Austria, Belgium, Croatia, Cyprus, Denmark, Finland, France, Germany, Greece, Italy, Latvia, Lithuania, Luxemburg, Malta, Poland, Portugal, Slovakia, Spain, Sweden, Slovenia and UK), and one that has incorporated an opt-in system requiring explicit consent (The Netherlands).

Given that only The Netherlands seems to have chosen the most demanding system (opt-in with explicit consent) it can be useful to evaluate its regulation further and to compare it with an example of the most widespread system (opt-in with implicit consent).

The British regulation was chosen for this function. Both the Netherlands and the UK have adopted article 5(3) of the directive almost literally following the wording of the e-Privacy directive in their legislations, and have undergone significant regulatory efforts to implement it. Like The Netherlands, the UK regulated the issue in a complete and detailed way that helps to avoid ambiguities. In addition, the British regulation is arguably the most complete of the ones allowing for implicit consent. It has been often taken by other MS as a reference and it is sometimes cited directly, as in the French regulation.

5.4.2.! The Dutch regulation

In the Netherlands, the right to refuse cookies exists since 2004 (two years after the e-Privacy Directive), having been established by the ministerial decree Decision on Universal Services and End-user Interests (*Besluit Universele Dienstverlening en Eindgebruikersbelangen*). The implementation of the directive came in place with the modification of Article 11.7a of the Dutch telecommunications law (*Telecommunicatiewet*)

on 5 June 2012,[619] which works in the framework of the Dutch Data Protection Act.[620] The new article, in line with the modification of article 5(3) of the e-Privacy Directive, states that websites cannot install cookies in data subjects' devices without prior and specific consent (terms used by the directive).

It is noticeable that the article, like the directive on which it is based (Electronic Communications Framework Directive), does not require consent to be explicit.[621] It was the National Regulatory Authority in charge of supervising the implementation of the Dutch telecommunications law (OPTA)[622] who added this requirement in its guidelines.[623] The authority considered that the Dutch Data Protection Act—which states in its article 23a that explicit consent is required for the collection of personal data—is applicable to tracking technologies in telecommunications and, in particular, to cookies. The obvious objection to this interpretation is that not all cookies collect this type of information, but the Dutch authority applied an inverse burden of proof according to which all cookies are

---

[619] The article reads: "Anyone who wishes to use electronic communications networks to store information on a user's equipment, or to obtain access to information already stored in the terminal equipment of a user should, unabated the Data Protection Act, a. provide the user with clear and comprehensive information in accordance with the Data Protection Act, and in any case about the purpose of storing this information, inter alia, gaining access to this information, and b. have obtained the user's consent for the concerned activity." Available (in Dutch) at http://wetten.overheid.nl/BWBR0009950/geldigheidsdatum_08-01-2014

[620] *Telecommunicatiewet*, articles 8 and 33.

[621] See Joasia Luzak, "Privacy Notice for Dummies? Towards European Guidelines on How to Give 'Clear and Comprehensive Information' on the Cookies' Use in Order to Protect the Internet Users' Right to Online Privacy," *Journal of Consumer Policy* 37, no. 1 (2014): 91.

[622] While Data Protection Authorities are concerned with the implementation of the Data Protection Directive, National Regulatory Authorities are concerned specifically with data protection in the telecommunications sector, as does the e-Privacy Directive.
The Dutch Data Protection Authority is the *College Bescherming Persoonsgegevens* (CBP). The Dutch National Regulatory Authority was the Dutch Independent Mail and Telecommunications Authority (*Onafhankelijke Post en Telecommunicatie Autoriteit*, OPTA) until April 1st 2013. In that date OPTA merged with the Consumer Authority (*Consumentenautoriteit*) and the Netherlands Competition Authority (*Nederlandse Mededingingsautoriteit*) to form the Authority for Consumer Market (*Autoriteit Consument en Markt*).

[623] See OPTA, "Veelgestelde Vragen over de Cookieregels," February 2013.

considered to carry personal data unless proved otherwise by the data collector.[624] Although it is usual for regulatory authorities to specify the application of a law, it is less usual for them to add a new and significant requirement of this sort.

To comply with the regulation, websites do not install cookies in the visitor's device upon entering, and display a banner asking if the visitor allows for the installation of cookies. When a certain website has asked a visitor for his consent, this can be stored in a cookie in the visitor's device avoiding the need to ask again the next time the website is used—although the visitor can "opt-out" again by deleting the cookie that stored his consent. So, if the visitor clicks on "yes", he will not be asked again. However, if he clicks on "no", he will be re-asked every time he visits the website or another section of the website, since as cookies are not allowed there is no way to record the negative answer.

If the visitor, when asked, refuses the installation of cookies, the website is allowed under the Dutch Regulation—same as in the e-Privacy Directive[625]—to block access.[626] This disposition became known as the "cookie wall."

In sum, the Dutch regulation not only almost literally adopts the wording of the directive, but goes a step further in the implementation of an opt-in system by requiring explicit consent unless the website proves no personal data are collected by a certain cookie.

5.4.3.! Implicit consent in the British regulation

As mentioned above, a useful case of implementation to compare with The Netherlands is that of the UK, which is a representative example of the opt-in system with implicit consent followed by twenty-one MS.

The UK implemented its regulation on cookies by an amendment in the Regulation 6 of the Privacy and Electronic Communications Regulations (PECR) on the 26 May 2011. The amended regulation follows

[624] See Ibid.
[625] Directive 2002/58/EC, recital 25.
[626] See Ibid. 4.

the language of the directive and requires in subsection 2(b) that the data subject "has given his or her consent", while the previous disposition only required that the data subject is given an opportunity to refuse (opt-out).

However, with the amendment of section 2 of Regulation 6 PECR to match the language of the amended e-Privacy Directive, section 3 was also amended redefining consent. The amended section 3 states that data subjects can signify consent when they make changes in the internet browser or some other program, hence allowing for implicit consent.[627]

The Information Commissioner's Office (ICO) issued detailed guidelines in May 2012 on how websites should gather data subject's consent about cookies.

Regarding the timing of consent, the guidelines state that "it is difficult to see that a good argument could be made that agreement to an action could be obtained after the activity the agreement is needed for has already occurred. This is not the generally accepted way in which consent works in other areas, and is not what users will expect."[628] However, they only require consent to be prior "whenever possible."[629]

The ICO guidelines, in line with regulation 6 PECR, do not require explicit consent, and allow interpreting that implicit consent was given when visitors take certain actions indicating so, such as visiting a website when cookies were not blocked. The British ICO has stated in this respect that "implied consent has always been a reasonable proposition in the context of data protection law and privacy regulation and it remains so in the context of storage of information or access to information using cookies and similar devices. While explicit consent might allow for regulatory

---

[627] The full text of the section reads: "For the purpose of paragraph (2), consent may be signified by a subscriber who amends or sets controls on the internet browser which the subscriber uses or by using another application or programme to signify consent."

[628] Information Commissioner's Office, "Guidance on the Rules on Use of Cookies and Similar Technologies" (London, May 2012). 1.

[629] Ibid. 5 (adding that "for implied consent to work there has to be some action taken by the consenting individual from which their consent can be inferred. This might for example be visiting a website, moving from one page to another or clicking on a particular button." Ibid. 6). Implied and implicit are used here as alternative terms.

certainty and might be the most appropriate way to comply in some circumstances this does not mean that implied consent cannot be compliant."[630]

However, for cookies that imply gathering of sensitive data, explicit consent could be required. According to the ICO guidelines, "website operators need to remember that where their activities result in the collection of sensitive personal data such as information about an identifiable individual's health then data protection law might require them to obtain explicit consent."[631]

This presents an important similarity with the system in force in The Netherlands, with two differences that provoke important divergences in their application. Firstly, the Dutch regulation requires explicit consent for all personal information, while the British would (potentially) require it for sensitive personal information only. Secondly, the Dutch regulation and the British regulation have an inverse burden of proof, and while The Netherlands requires that websites prove that the information carried is not personal information in order to avoid the requirement of explicit consent, the UK requires that the data subject (or a third party) proves that the information carried is personal and sensitive in order for explicit consent to be required. As it can be seen, despite having the same black letter law, the UK is much more lenient than The Netherlands in its regulatory application of the directive.

The differences mentioned add to the fact that, in practice, the UK has been even more lenient in the implementation of the e-Privacy directive than what its regulation leads one to expect. An open letter issued by the Department of Culture, Media and Sport on 2011 has stated that focusing on providing data subjects with information and choices regarding tracking is reasonable and sufficient to comply with the regulation. Furthermore, the letter has stated that consent is not time-

[630] Ibid. 5.
[631] Ibid. 6.

bound, and does not necessarily have to be given in a previous manner in cases in which it is impractical to do so.[632]

In the UK the requirement of explicit and prior consent has been deemed too burdensome when applied to all cookies, since many websites install cookies at the moment that data subjects open them.[633] The focus of the policy was shifted with the open letter to ensuring best efforts in minimizing the time between the installation of the first cookies and the obtaining of consent.[634] This is a very wide interpretation of the guidelines of the ICO—which, according to the letter, was consulted before its writing—which request the installation of cookies to be delayed until consent is given every time this is possible.

The British regulation, in sum, also almost literally copies the wording of the directive, but attenuates it strongly by allowing for implicit consent when no personal data are carried—with an inverse burden of proof compared to the Dutch regulation—and sometimes even for subsequent consent. It seems to stay, therefore, as close to an opt-out system as it is possible without breaching the directive.

The possible criticism to the British regulation (which could extend to all other MS incorporating an opt-in system with implicit consent) is that if a data subject visiting a website without blocking cookies in manifesting implicit consent and hence opting in, is it doubtful to what extent this is really an opt-in system and not an opt-out system with a duty of notification.

---

[632] See Department for Culture Media and Sport, "Open Letter on the UK Implementation of Article 5(3) of the E-Privacy Directive on Cookies" (London, May 24, 2011).
[633] See Information Commissioner's Office, "Guidance on the Rules on Use of Cookies and Similar Technologies" (London, May 2012).
[634] See Department for Culture Media and Sport, "Open Letter on the UK Implementation of Article 5(3) of the E-Privacy Directive on Cookies" (London, May 24, 2011).

5.5.! Default Cookie Rules and the Dutch Regulation

5.5.1.! Disappointments and modification of the regulation

When The Netherlands incorporated the opt-in system with explicit consent for cookies, there were several complaints about the regulation. From the side of the industry, it was stated that the regulation is "a very hard-to-explain deviation from the European directive, which doesn't help anybody and makes it more complicated for both us and for the consumer."[635] Before the passing of the law, stakeholders formally complained that the cookie law is not only excessive for the aim of the directive but also goes beyond the scope of personal information.[636] The law was deemed especially problematic because Dutch public media companies are required to reach a certain percentage of the population, which they partly do via their websites, and the impossibility to install any type of cookies prevents them from monitoring how many people view their contents.

Similarly, consumers seemed dissatisfied. Consumers associations have complained about what has come to be known as the "cookie wall" claiming that is has been mainly an annoyance for internet users, and requested privacy protection to be matched by user friendliness.[637]

Sectors of the public opinion seemed dissatisfied with the regulation as well. Some have stated that the law was a failure due to its impracticality.[638] Others stated that the law misses the point entirely,

---

[635] Matt Steinglass, "Dutch Cookie Law May Lead to Online Exodus," *TechHub*, June 21, 2011.
[636] See Jan Driessen et al., "Verzoek Tot Inhoudelijke Behandeling Wijziging van de Telcommunicatiewet," July 3, 2011.
[637] See Stephan Loerke, "The Dutch Find a Lighter Touch on Internet Privacy Laws," *AdAge*, July 3, 2013.
[638] See Arnoud Groot, "'Naïeve' Cookiewet Loopt Achter de Feiten Aan," *Emerce*, November 4, 2010; "Mislukte Cookiewet Is Een Wijze Les," *NetKwesties*, April 11, 2013.

since what is relevant for privacy is anonymity.[639] It was reported that consumers found the regulation annoying and unhelpful, and that it led people to mindlessly click to allow cookies every time they attempt to enter a website, being useless for its purpose.[640]

Dutch academics have called the regulation "a policy fiasco of impressive dimensions"[641] and "a regulatory failure."[642] It has also been stated that the main effect of the regulation is making services more difficult to be offered[643] and that it hinders e-commerce both within and outside the Netherlands.[644]

In addition, compliance has been low. A large amount of websites have breached the law and installed prohibited cookies in their visitors' computers,[645] including the websites of most political parties that voted in favor of it[646] and of the government itself.[647]

When faced with these results, a large fraction of political parties who originally voted in favor of the law objected to its continuation. On 21 November 2012, D66 filed a proposal to change the regime because they considered the current regime too strict and unclear, and proposed to change it for an informed consent approach.[648] Later on, both VVD and

---

639 See Freek Vos, "Waar Maakt Iedereen Zich Zo Druk over? Leve de Cookies!," *Volkskrant*, October 17, 2012.
640 See "Wetgever Maakt Surfen Onmogelijk," *Financieel Dagblad*, June 11, 2010.
641 Natali Helberger, "Freedom of Expression and the Dutch Cookie-Wall," University of Amsterdam Institute for Information Law Working Paper 13-01 (Amsterdam, 2013). 1.
642 Ronald Leenes and Eleni Kosta, "Taming the Cookie Monster with Dutch Law. A Tale of Regulatory Failure," *Computer Law & Security Review* 31, no. 2 (2015). 1.
643 See Bart van der Sloot, "Je Geld of Je Gegevens: De Keuze Tussen Privacybescherming En Gratis Internetdiensten," *Nederlands Juristenblad* 86, no. 23 (2011): 1493.
644 See Gerrit-Jan Zwenne and Maxime Verhagen, "Dutch Cookie Law to Affect Businesses Outside Holland," *E-Commerce Law & Policy* 13, no. 17 (2011): 1.
645 See Arnoud Engelfriet, "Websites Negeren Massaal de Cookiewet," *Cookierecht*, July 13, 2012.
646 See Robert van Hittersum, "Dutch Political Parties Violate Their Own Cookie Law," *FleishmanHillard*, June 7, 2012.
647 See "Opta Overtreedt Eigen Cookie-Regels," *NU*, October 26, 2012.
648 See "Voorstel Voor Ruimere Cookiewet," *NU*, November 21, 2012; "Kamp (EZ) Gaat Cookievoorstel D66 Bestuderen," *Emerce*, November 22, 2012.

PvdA stated that the regulation was unworkable, and called it a "cookie hostage" (*cookiegijzeling*) that must be put to an end.[649]

These circumstances led to the Dutch Minister of Economic Affairs publishing a letter on 20 May 2013 containing a revision of the regulation.[650] Besides clarifying issues regarding jurisdiction,[651] the revision incorporates two changes: it (i) allows websites to let users show consent by clicking in any part of the website if it is clearly shown to them that doing so signifies consent and (ii) it allows analytics (cookies that do not track individual behavior) without requiring consent.[652]

This means, in practice, that the Dutch regulation is moving to a system of implicit consent. While until it finally does the current regulation still applies,[653] this means that The Netherlands would join the majority of MS in their implementation of the e-Privacy directive.

5.5.2.! Explanation from the perspective of default rules

A possible reason why the Dutch regulation did not see its expected results in designing an opt-in system with explicit consent in compliance with the amended e-Privacy Directive is that, despite what was stated in the law, the regulation did not effectively make websites implement an opt-in system.

---

649 See "Kamer Wil Einde Pop-Ups Door Cookiewet," *NU*, February 13, 2013; "Meerderheid Tweede Kamer Wil Einde Aan Cookie-Popups," *Tweakers*, February 13, 2013.

650 See Henk Kamp, "Kamerbrief over Analytische Cookies En Artikel 11.7a van de Telecommunicatiewet" ('s-Gravenhage, December 20, 2012).

651 It states that the regulation is not limited to Dutch websites, but also includes under some circumstances foreign websites, as it is its aim to protect Dutch consumers. Although it is not specific on what websites fall under the regulation, it mentions that viable criteria could be the language, the possibility to order products from The Netherlands, and the type of information provided.

652 See "Cookiewet Versoepeld: Verplichte Melding Voor Minder Cookies," *Volkskrant*, December 20, 2012.

653 For example, on November 2013—after a long investigation—the Dutch Data Protection Authority sanctioned Google for gathering information of data subjects via cookies without their explicit consent. See College bescherming persoonsgegevens, "Onderzoek CBP Naar Het Combineren van Persoonsgegevens Door Google. Rapport Definitieve Bevindingen," November 25, 2013.

In a similar way to American bank customers deciding on whether to allow for overdraft coverage, data subjects were asked a polar question: whether they agreed with the use of cookies made by the website, or they did not. This choice different from being faced with a default opt-in system, as both the bank customers and data subjects had to make a conscious choice.

In both cases, the most effective way to get customers to switch away from the default system was not to inform them about the costs and benefits of each option. As a consequence, what data subjects faced after websites incorporated the regulation was not a DNT default but an active choice. This similarity illustrates what can happen when the choice architect has an interest in subverting the regulation.

Furthermore, data subjects under the cookie regulation had more pressure on choice than bank customers. While the latter could still normally use other bank services after choosing the "no" option (since they were paying for them independently), data subjects were often either not able to access the website due to the "cookie wall", or access it subject to several malfunctions because the negative choice also meant that session cookies, which are necessary for some features, would not be installed.

The "cookie wall", or the explanation offered in other cases presenting cookies as something necessary for the functioning of the website (which they sometimes are), framed data subject's choice. Data subjects were often not making a neutral choice on whether they desired to be tracked, but were making a choice on whether they still wanted to visit a certain website seconds after typing its URL. This effect was even stronger in other websites which placed together with the "cookie wall" a banner that allowed only for the "yes" option—data subjects who wanted to say no would have to directly leave the website since they had nowhere to manifest their choice.

As with other default choice systems, a DNT default choice system can work only if people under DNT regime are treated in the same way as

people in the track-me regime.[654] If websites are able to present data subjects with increasing incentives to switch choice, then most benefits of the policy are lost.[655] It has been argued before that the cookie wall was problematic since it can put pressure on choice.[656] This, although not amounting to coercion, can potentially hamper the validity of consent by violating the requirement of free consent established by the A29WP.[657]

The do-not-call registry mentioned before,[658] for example, which was largely considered a success,[659] was run not by telemarketers themselves but by a governmental agency. If telemarketers had run the registry it is likely that they would have made it more difficult for people to join, hence hampering the success of the policy.[660]

The implicit consent system implemented by the UK also traces back to the behavioral considerations made.[661] For this, one can pose the question of how would the bank overdraft regulation have worked if implicit consent had been allowed as a valid means to opt-in the overdraft system—as an opt-in policy more lenient towards banks—and whether this would have avoided its problems. In such a case, it becomes noticeable that it is difficult to imagine a choice design in which banks could have implemented an implicit consent opt-in in a way that it is not substantially the same for their clients as the previous opt-out regime.

---

654 See Lauren Willis, "Why Not Privacy By Default?," *Berkeley Technology Law Journal* 29, no. 1 (2014): 61.
655 See Ibid.
656 See Joasia Luzak, "Much Ado about Cookies: The European Debate on the New Provisions of the ePrivacy Directive Regarding Cookies," *European Review of Private Law* 21, no. 1 (2013): 221; Natali Helberger, "Freedom of Expression and the Dutch Cookie-Wall," University of Amsterdam Institute for Information Law Working Paper 13-01 (Amsterdam, 2013).
657 See A29WP, "O.J. 15/2011 On the Definition of Consent" (Brussels, July 13, 2011).
658 See section 5.3.4.
659 See Federal Communications Commission, "Trends in Telephone Service" (Washington, DC, August 7, 2003); Federal Trade Commission, "Annual Report to Congress for 2003 and 2004 Pursuant to the Do Not Call Registry" (Washington, DC, October 4, 2005).
660 See Lauren Willis, "Why Not Privacy By Default?," *Berkeley Technology Law Journal* 29, no. 1 (2014): 61.
661 See section 5.2.3.

For an implicit consent opt-in to function appropriately, there has to be an available set of actions which are conducing to the belief that the subject has manifested a choice, albeit not explicitly. If merely withdrawing money from an ATM in overdraft is taken to be within this set of actions, then the functioning of the opt-in system with implicit consent would have been identical to the functioning of the opt-out system, where bank clients could do this directly. In addition, to comply with the definition of consent of the Data Protection Directive, implicit consent needs to rest on a specific indication of the data subject's wishes.[662] The CJEU, in turn, has stated that silence does not signify consent under the EU data protection framework.[663]

This leads to a word of caution regarding the validity of many opt-in choices with implicit consent which is transferable to the case of online tracking; it leads to question whether accessing a website, unlike withdrawing money from an ATM, is sufficient to implicitly manifest an opt-in choice. If one considers that it is not, that would lead to the conclusion that countries with an implicit opt-in choice for online tracking are functionally staying in an opt-out system, disallowed by the amended e-Privacy Directive.

Besides the type of consent chosen, the Dutch and other European regulations asked agents who are behaviorally informed and who have counteracting interests to these regulations to be the choice architects of an opt-in default system—like the bank overdraft regulation, and unlike the do-not-call registry. This has been identified as a flaw in the choice system.[664] Are there regulatory alternatives that would avoid this problem?

---

[662] Directive 1995/46/EC, article 2(h). See also A29WP, "O.J. 15/2011 On the Definition of Consent" (Brussels, July 13, 2011).
[663] See *Volker und Markus Schecke GbR* and *Hartmut Eifert* (joined cases), CJEU C-92/09 and C-93/09 (2010).
[664] See section 5.2.

5.6.! Policy Suggestions

5.6.1.! Reconsidering the penalty default

Having evaluated how the different MS implemented the amended e-Privacy Directive's requirement of previous consent for tracking (opt-in system), one can pose the question of whether, in the context of the composite problem identified,[665] it is desirable for the aim of the regulation to make the choice an opt-in,[666] or if it is better to present it as an active choice with two options presented equally—as the Dutch regulation accidentally did.

As it was seen, default rules can be set as policy defaults or as penalty defaults, depending on the aim with which the default rule is set.

In the framework of policy defaults, opt-in choice systems are considered useful when there is a choice that is in itself more valuable than the other, either for most people facing the choice or for society in general.[667] This is the case, for example, of increased savings in retirement plans or organ donation, where some jurisdictions change the default to increase the number of donors based on the idea that organ donation is in itself something valuable.

However, for the case of tracking devices such as cookies it is arguable that it is desirable to reduce their use only inasmuch as they cost consumers more than they benefit them, and not to absolutely eliminate them from the internet, even when ignoring the benefits of companies, which should also be present in a social welfare function. Cookies are not inherently harmful, as they present both costs and benefits for the industry and for data subjects. The "stickiness" of an effective opt-in default policy, for this reason, could leave fewer cookies than what is socially desirable. This can have harmful dynamic effects. If the entry in the market of websites (which is financed by advertising) was diminished

---

[665] See section 5.2.1.

[666] See section 5.3.3.

[667] See Craig McKenzie, Michael Liersch, and Stacey Finkelstein, "Recommendations Implicit in Policy Defaults," *Psychological Science* 17, no. 5 (2006): 414.

by an opt-in system, this policy would lead to fewer websites in the future and a less interesting internet for data subjects. This idea is in line with the classification of this policy under penalty defaults.

Penalty defaults can make a stronger case in favor of an opt-in system for cookies than policy defaults, as companies are clearly more informed than data subjects about the functioning of the cookies they install.[668]

It was seen that penalty defaults are useful when (i) there is a party which is more informed than the other, (ii) he engages in rent-seeking behavior by withholding information and reducing total welfare and (iii) contracting around such default rule can release that information.[669] The question that one should ask in order to determine if a penalty default rule is useful to reduce an information asymmetry not solved by the market is then: does this rule increase the amount of available information by reducing what was previously withheld?

This question involves two central elements. The first is determining whether there is rent-seeking behavior exploiting the information asymmetry.[670] The second is whether the penalty default successfully poses a cost for the party with more information in such a way that it induces a negotiation between parties that involves disclosure of information that reduces the information asymmetry.[671]

In this case, the only information release which was produced by the regulation is that the website under consideration utilizes cookies. Although there is a clear information asymmetry between websites and data subjects regarding the functions of cookies, it is not clear if this was the basis of rent-seeking behavior, and it is clear that the default did not

---

[668] See Paul Schwartz, "Privacy Inalienability and the Regulation of Spyware," *Berkeley Technology Law Journal* 20 (2005): 1269; Rajiv Shah and Jay Kesan, "Policy through Software Defaults," in *Proceedings of the National Conference on Digital Government Research* (New York: Association for Computing Machinery Press, 2006), 265.

[669] See section 5.2.2.

[670] See Ian Ayres and Robert Gertner, "Filling Gaps in Incomplete Contracts: An Economic Theory of Default Rules," *Yale Law Journal* 99, no. 1 (1989): 87. 127.

[671] See Ibid. 128.

induce a negotiation.[672] In these lines, it has been argued that information-forcing rules such as penalty defaults fail to work in contract law when people sign the contracts without reading them.[673] Data subjects did not end up being more informed about the functions of cookies after clicking away the banners in the countries that applied the directive more strictly. Due to the high number of data subjects per product, entering individual negotiations that would induce them to opt into the tracking system would have high transaction costs, and it is difficult to determine if such provision of information about the characteristics of cookies would induce them to opt in.

Given the difficulties of assessing the costs and benefits of cookies for each particular case, applying the principle of informed consent to an active choice by data subject presents some benefits over an opt-in policy that regulates the way in which the choice is presented. If a data subject knowingly agrees to cookies, there are good reasons to believe that such exchange is valuable.

The presence of preference heterogeneity is commonly a substantial argument in favor of active choice designs instead of default rules,[674] and data subjects have heterogeneous preferences regarding cookies. Different people have different levels of disutility from tracking, and even the same person has different levels of disutility depending on the topic the tracking

---

[672] Mandatory notices have long been doubted by commentators in their ability to inform consumers. See William Whitford, "The Functions of Disclosure Regulation in Consumer Transactions," *Wisconsin Law Review* 2 (1973): 400; Homer Kripke, "Gesture and Reality in Consumer Credit Reform," *NYU Law Review* 44 (1969): 1; Robert Jordan and William Warren, "Disclosure of Finance Charges: A Rationale," *Michigan Law Review* 64, no. 7 (1966): 1285.

[673] See Rip Verkerke, "Legal Ignorance and Information-Forcing Rules," *William and Mary Law Review* 56 (2015): 833. For an argument in favor of the abandonment of this duty to read in consumer law, see Ian Ayres and Alan Schwartz, "The No-Reading Problem in Consumer Contract Law," *Stanford Law Review* 66 (2004): 545.

[674] See Cass Sunstein, "Impersonal Default Rules vs. Active Choices vs. Personalized Default Rules: A Triptych," Harvard Law School Working Paper 13-01 (Boston, 2013). The author has argued, similarly, that default settings have the cost of narrowing our experiences, and an argument can be made in favor of active choosing in context where one would want people to develop their own preferences and values. See Cass Sunstein, "Choosing Not to Choose," Harvard Public Law Working Paper 14-07 (Boston, 2014).

is about.[675] A neutral presentation of the choice of whether to allow for tracking that introduces both options equally might then be more appropriate for the aim of meaningful consent, which the regulation wants to achieve.

5.6.2.! Differentiating cookies

Cookies can present different levels of privacy costs. As a first distinction, session cookies and permanent cookies do not present the same risks for privacy breach. As mentioned above, session cookies disappear after the browser is closed, while permanent cookies remain in storage for a longer period of time, usually until deleted. If one assumes an equal risk of privacy breach per unit of time, then permanent cookies—which can last for years—present on average a much higher privacy risk than session cookies—which tend to last for a few hours. In addition, user profiling is normally done by using permanent cookies, while most cookies that allow functions in websites (such as a shopping cart) are session cookies. Permanent cookies, hence, present a higher (expected) total privacy cost than session cookies.

There are good reasons to consider, from the incentive structure of website providers, that permanent cookies and session cookies should be treated differently by regulations. In the same way as permanent cookies involve a higher privacy cost for data subjects than session cookies, they involve a larger total payoff for websites and advertisers, since by lasting for a longer time they make it easier to collect information.

A law that establishes a DNT default for all cookies reduces the amount that websites are able to install in data subjects devices (contingent on their consent) by making every cookie marginally less likely to be installed. This reduces websites' ability to make user profiles and tailor advertisements based on those profiles. This, in turn, reduces the total payoff of cookie use for websites. If websites can install fewer cookies, and they can choose which cookies to install because all of them are

[675] See sections 3.2.2 and 3.2.3.

treated equal, they will install those that are most profitable for them. Therefore, a regulation that treats all cookies equally reduces the payoff of cookie diversification. By setting incentives for websites to install only the most invasive cookies, it shifts the relative prices towards cookies that are more costly from a privacy perspective.

Even if one assumes that websites care about the privacy of their users and would thus install the least invasive cookie under a regulation that treats all of them equally, in a context where there is a fixed cost per installation of cookie (obtainment of consent), websites have to pay this cost only once for a permanent cookie, while they have to pay it several times if the same function is achieved by several session cookies. Assuming firms try to reduce costs, this will lead them to shift to permanent cookies whenever possible—both for websites under perfect competition and websites with monopoly power, as cost minimization is independent of market power. This increases the total privacy cost of cookies.

On the other hand, if less invasive cookies (such as analytics, or session cookies in general) are installed without complications, while more invasive cookies require previous consent, websites will have incentives to invest in diversification of cookies, requesting to send permanent cookies only when they are necessary for the required goal. This leads to a lower privacy cost for the average data subject without harming websites.

The same effect is caused from the side of the data subject. Under a regulation that does not differentiate cookies, data subjects face upon entering a website a notification that such website uses cookies, or a banner asking to agree to the use of cookies of that website. It is costly for that data subject to know, however, if such cookies are session cookies or permanent cookies, categories to which he could potentially have a different reaction. That banner or that notification alone will determine the perceived privacy risk, as well as the annoyance in browsing. In such situation, a website that maximizes the number of visitors will attempt to ask the question as few times as possible, hence recurring to fewer, more invasive permanent cookies.

On the other hand, under a regulation that requires authorization for permanent cookies but not for session cookies, the website has incentives to use session cookies as much as possible, and reduce the number of times data subjects will receive the notice or the banner for permanent cookies. This, simultaneously, makes the notice or banner more informative, since data subjects will know that it corresponds to permanent cookies. This should, additionally, make data subjects less prone to accept a banner requesting them to agree with cookie tracking—since each acceptance is more costly on average than an acceptance to a banner that does not differentiate cookies—thus enhancing average privacy protection.

From this point of view, the mechanism suggested in the following subsection to implement the DNT default, additionally, the benefit that it allows for session cookies while preventing permanent cookies from being installed.

5.6.3.! Targeting web browsers

A possible way to address the problems that were encountered by the Dutch regulation[676] is designing a regulation to target web browsers instead of websites.[677] This modification is technically possible and relatively easy, while political feasibility would require a more complex analysis and will fundamentally depend on the context; the main obstacle in this case would be enforcement. European DPL has always targeted data controllers and not technology creators, and it seems difficult for individual MS to put requirements on web browsers. It was probably unfeasible for the Dutch regulators to make demands to browsers that are based in another jurisdiction. However, more feasible for the EU in general and for the US. Given that browsers responded well to DNT headers, it seems possible that if enacted by the appropriate jurisdictions, they would comply with a regulation of this sort.

---

[676] See section 5.5.1.

[677] See Ian Brown and Christian Marsden, *Regulating Code: Good Governance and Better Regulation in the Information Age* (Cambridge, Mass.: MIT Press, 2013).

Firstly, a browser's business model is not harmed by a policy attempting to reduce the use of cookies—or it is only inasmuch as the company who owns the browser also owns websites or applications which profit from targeted advertising. Web browsers have less incentives than websites to twist the default policy, while they have the technical possibility of blocking them.

In a similar way as a regulation can call websites to apply a DNT preference and avoid sending cookies as was successfully done with DNT headers, it can call browsers to apply it by blocking cookies sent by websites. In this case, browsers operate as a gatekeeper, and the intention of websites notwithstanding, then can choose if to let cookies through or not. When this is done, it is more difficult for a website to set a cookie-wall as they did in The Netherlands and in the UK. Data subjects could have the choice, in this way, not between entering the website with cookies or not entering at all, but between entering the website with or without cookies.

Secondly, the costs of the regulation would be reduced, since web browsers are cheaper to monitor than websites regarding compliance. The internet has millions of websites. The browsers through which most of internet traffic goes through, on the other hand, are five.[678] Since web browsers are able to block cookies, requesting them to do so can effectively implement a DNT default at lower enforcement costs.

Together with enforcement costs, and also due to the reduced number of agents that have to direct efforts into enforcing the regulation, this would lower compliance costs. Under the current Dutch regulation, all websites that operate in The Netherlands have to design a banner for the opt-in mechanism—or the active choice. This consumes resources that could be used for something else, such as developing new features to attract customers.

Also, web browsers can present the question of whether to navigate with cookies in a context in which it has more relevance than the context

[678] To this time, Internet Explorer, Mozilla Firefox, Google Chrome, Safari and Opera.

in which—even when well-intentioned—websites can present it. In such way, browsers can implement the policy in a way that is less costly for data subjects. If websites are in charge of asking whether a data subject agrees with cookies to be installed, the data subject will be asked every time he changes website, which was found by most of them bothersome and not user-friendly.[679] This not only interrupts navigation and thus bothers data subjects but also makes it difficult for them to visit a certain website being tracked in some occasions and not being tracked in others—which is often a desired feature, for instance with search engines. If browsers are in charge of posing this question, on the other hand, data subjects can be asked every time they open the browser to start navigation. This does not interrupt navigation and makes it easier for them to switch system if they desire to do so—they just have to open a new window. Moreover, this feature is in line with the policy recommendation explained before of enhancing data subjects' flexibility when possible.[680]

Requesting web browsers to block cookies, then, allows for a more user-friendly way of knowing whether a certain data subject wants to browse with or without cookies. This idea is supported by the Electronic Communications Framework Directive, which states that the request for consent must be as user-friendly as possible within the applicable technical limitations.[681]

5.6.4.! How to target web browsers

If data subjects want to remain cookie-free, all five major browsers already offer a function under which they can navigate the internet without permanent cookies being installed. Data subjects can then navigate without leaving permanent traces in their device that allow for tracking, while receiving the less controversial session cookies that allow for the use of many functions of the websites, such as streaming video or placing items

[679] See Natali Helberger, "Freedom of Expression and the Dutch Cookie-Wall," University of Amsterdam Institute for Information Law Working Paper 13-01 (Amsterdam, 2013).
[680] See sections 3.5 and 3.6.
[681] Directive 2009/136/EC, recital 66.

in a shopping cart. This function prevents (with some exceptions) cookies, local storage, history and caches to remain in the computer after the browsing session is finished.[682]

This function imbedded in browsers offers data subjects a real opt-out choice for permanent cookies that only requires two clicks, and saves them the trouble of learning about and installing PETs. From a technical point of view, this opt-out choice is easy to turn into an opt-in; regulation can require browsers to open in Incognito Mode/Private Browsing, and switch to the now standard mode only after those two clicks are made.

Opinion 2/2010 of the A29WP states that browser setting can only effectively represent an opt-in choice for data subjects in some situations because they accept cookies by default, and because data subjects often do not know how to change them.[683] Although this flaw is of course true for current browser settings, it is not an obstacle for creating a regulation that approaches them to apply the DNT default instead of approaching websites.

Policymakers could, hypothetically, design detailed forms for data subjects to complete every time they enter into a website specifying which types of cookies they would like to allow, for how long they would like to allow them, for the use of whom, and so on and so forth. However, this would be of little use. From the point of view of user-friendliness, most PETs—especially those that are more sophisticated—have usability problems,[684] and so does a cookie wall applied by individual websites. This

---

[682] There are some exceptions for this. Information that is collected by browser-independent plugins such as Adoble Flash is not cleared, but most browsers offer the option to deactivate it when using Private Browsing or Incognito Mode. Firefox does not clear persistent storage (window.globalStorage), Internet Explorer does not clear IE userData, and Safari used on Windows does not clear data at all. See Katherine McKinley, "Cleaning Up After Cookies Version 1.0," *Technical Report for ISEC Partners* (San Francisco, 2010).

[683] See A29WP, "O.J. 2/2010 on Online Behavioral Advertising" (Brussels, June 22, 2010)., 14.

[684] See Pedro Giovanni Leon et al., "Why Johnny Can't Opt out: A Usability Evaluation of Tools to Limit Online Behavioral Advertising," in *Proceedings of the Association for Computing Machinery Special Interest Group on Computer-Human Interaction Conference* (New York: Association for Computing Machinery Press, 2012), 589.

function embedded in browsers, on the other hand, does not, as it is simple to use. Establishing this function as a default DNT choice would make it even simpler.

In sum, this regulatory suggestion could provide a simpler regulation with less incentives for the choice architect to undermine the policy.

5.7.! Online Tracking Meets Behavioral Economics

This chapter has argued that the behavioral economics literature on default rules can help in identifying why online tracking regulations in Europe faced difficulties in implementing the policy. These regulations either arguably stayed in practice within an opt-out default system by allowing for implicit consent, or their policy was neutralized by websites, having an active choice system as a result. As it was seen, the only MS who adopted a DNT default that requires both previous and explicit consent decided to attenuate it moving to implicit consent thereafter, while this option seems functionally equivalent to the opt-in system from which the amended e-Privacy Directive aimed to part.

Both The Netherlands and the UK implemented the wording of the amended e-Privacy Directive into their regulations but gave it in practice very different meanings. While the Dutch regulation follows what seems to be the intention of the amendment of the e-Privacy Directive and becomes what could be the strictest legal system in the world regarding cookies, the British regulation approaches the issue more conservatively and regulates it as close to an opt-out system as the wording of the amendment allows. Noting the implementation problems that the Dutch regulation faced, it might be easier to understand the reluctance of the British government to move to an opt-out system and why The Netherlands set itself in the way to moderating its own regulation later on.

It was suggested here that this could have happened because penalty default rules were applied outside their scope and their design was trusted to agents with incentives to undermine them. If this is the case,

reconsidering the opt-in system, relying on web browsers instead of websites for the choice design, and taking into consideration the differences in privacy costs between permanent and session cookies, could help in improving consumer choice.

The explanation and the policy suggestions offered can be potentially useful not only for The Netherlands but for any country considering incorporating a DNT default in their legislations. Within the EU, it can help in the design of an implementation that ensures informed consent and achieves the aims of the directive in line with the goal of Smart Regulations. The technology and the behavioral insights to implement effective limits on online tracking are already available; it is the law that needs to catch up.

6.! Conclusions

6.1.! Tradeoffs in DPL

The way in which we deal with our personal information and the limits of our privacy mutate with new technologies. The internet, the biggest agent in this change, has turned into a zero marginal cost distribution channel, both for voluntary and for involuntary exchanges. Thereafter, it has turned from a system of information storage by some and information retrieval by others to a system for connecting people, where anyone can create and retrieve content (peer-to-peer). This leads to personal information behaving as a good that, while still costly to produce from a privacy perspective, can be given costlessly to others; this implies the existence of positive spillovers that potentially lead to a deficit problem—much like the one addressed by copyright.

Informational privacy, and in particular data protection, concerns the ability to exclude others from one's personal information. Exclusion, in turn, takes us to the realm of entitlements and of the different possible ways to protect them: liability rules, property rules and inalienability rules. Some level of exclusion (this is, some level of data protection) creates incentives to generate information, reducing the deficit problem.

Informational privacy in cyberspace can be characterized as: (i) a public good, (ii) a good that can be traded with low transaction costs, (iii) a good that has not been yet produced, and (iv) a good that is produced as a by-product of a consumption activity. Due to the first characterization, its positive spillovers should be internalized for its level of production to be optimal. Due to the second and third, the allocation of entitlements defines such internalization, and DPL can establish production incentives and foster its generation by allocating those entitlements. Due to the fourth, DPL is not the only tool that can do this: the market can induce a certain level of information even in the absence of data protection, although this level is likely to be suboptimal.

This leads one to consider that the interdependence between privacy and access to information in the context of new technologies is not a negative relationship, but a positive concave relationship: data protection

and information are often not at a tradeoff. Zero data protection means the persistence of the deficit problem and hence a low level of information production (dynamic effect of DPL), while absolute data protection means a high level information production but without information flow (static effect of DPL).

The three classical canonical protections of entitlements in their pure form (liability rules, property rules and inalienability rules) generate problems that would undermine the utility of DPL if they were implemented in their pure forms. For liability rules, this would take place due to a causal uncertainty problem that is not resolvable with the traditional means used in other areas of law. For property rules, this would be due to the introduction of a moral hazard problem. For inalienability rules, the benefits of information production would be nullified by a reduction in information flow—at this high level of protection, privacy and information turn to be at a tradeoff.

Following the premise of the positive concave relationship between data protection and information flow, a mid-way between the first two rules can maximize both privacy and access to information for data subjects. This provides a direction for DPL: some level of exclusion is desirable, and such level can be set in a non-centralized way (in the style of property rights) with a level of exclusion in between property rules and liability rules.

This idea coincides with the general characteristics of European DPL. To provide data subjects with enhanced privacy, DPL generates entitlements over personal information. Moreover, the rationale of DPL is not based on an idea of ownership over data—it would be false to assert that the rights given to data subjects within it constitute a property right.

The incentives to generate information matter as long as data subjects are likely to respond to them. It is important to add, therefore, that data subject behavior can be interpreted within rational choice theory. The responses that data subjects have regarding the disclosure of their personal information are consistent with those of rational agents that discount in the context of an uncertain hazard rate. Moreover, data

subjects are responsive to context and when levels of data protection are visible they alter their levels of disclosure. This means that data subjects take incentives into account when deciding whether to disclose.

This is especially relevant in a context where people ignore most of what happens with their personal information, and they try to take control with self-protection mechanisms such as PETs, which are socially costly. For data subjects, taking control means knowing what happens with their information, and being able to make choices about it, if possible more than once.

These considerations lead to three theoretical conclusions. First, privacy and access to information are not countervailing rights; the social costs of lacking an adequate data protection are not only those corresponding to chilling effects, but also to underproduction of information. Second, an optimal level of exclusion to incentivize personal information is lower than a property rule, and lower than copyright, but higher than a liability rule. Third, European DPL addresses this fact, and from this point of view it is generally efficient.

By focusing on DPL as a mechanism to promote the generation of information, two gaps so far present in the literature regarding proposals to protect privacy are closed. First, the question of why the allocation of the entitlement is relevant in a scenario of low transaction costs is answered by seeing that distributional effects matter to incentivize production. Second, the question regarding how property elements over intangible goods can be justified in the face of a mismatch between the reasons to protect personal information and the reasons to protect intellectual property is addressed by noting that both branches of law foster the generation of information.

6.2.! Policy Implications

A common conception of policymakers and academics is that the right to privacy presents tradeoffs with the amount of information available and the right to access information. However, since some level of data

protection increases the amount of available information, these tradeoffs are not as linear as one would initially think.

The theoretical considerations that were made are relevant for policymaking inasmuch as they have an impact on the way in which the rights to privacy and to access information interact, which has consequences on how they should be balanced. More specifically, they provide us with an economic framework that can serve as a basis for explanatory and for normative evaluations of DPL. It can be used to evaluate whether policymakers designing central changes in DPL have acted as if privacy and information are to some extent complementary—as we have seen that they did in Europe. Moreover, it leads to general policy recommendations for this evolving branch of law.

From an economic perspective, the level of data protection given to a certain piece of information should depend on three factors. First, it should depend on who incurred in costs to generate the piece of information which is being protected. If a data subject has to invest to generate the information, this justifies a higher level of protection than the one in place for those cases in which an entity that collects or processes data invests in it, since the agent that needs to be incentivized to produce the information is different. Second, the level of protection should also depend on the social benefits that stem from the use of that information. When there are large social benefits from the information, for example because it is useful for research that can improve public health or help in the prevention of crime, a lower level of protection is justified compared to information that is only used for marketing purposes. For information with large social benefits, access turns to be more important within the tradeoff inherent in providing entitlements between incentives for production and access by others. Lastly, the level of protection should depend on the size of the externalities that its use would imply for the data subject since, in order to keep incentives to invest stable, one must grant a higher level of protection to information that can potentially be more harmful, keeping the social use and source of the information stable. This relates particularly to sensitive information, justifying its special protection.

Moreover, given the characteristics of the context in which data subjects engage in disclosure, DPL should focus, when possible, on increasing flexibility for data subjects in their choices regarding whether to disclose. When increasing flexibility is not possible, or it is too costly, DPL should focus on increasing transparency in order to reduce the uncertainty about the probability of a data leak with requirements such as digestible privacy policies and informed consent.

Focusing on concrete policy issues that are relevant for the EU, this framework can also be applied to two recent legal developments that are undergoing regulatory debates and had high media exposure in European DPL: the right to be forgotten and online tracking. Analyzing these data protection regulations from the theoretical considerations made can help to determine whether they are justified from a law & economics perspective, and if they are, whether it is possible that they went too far or that they have not gone far enough.

Any comment on the general principles of European DPL would be incomplete without addressing the right to be forgotten, both due to the prominence that its debate had inside and outside of academic circles, and due to the significance that it would have for all agents dealing with data protection. The right to be forgotten, in fact, is a good example of policymakers augmenting the level of exclusion in data protection by creating an entitlement. This entitlement increases data subjects' flexibility, but also presents large social costs.

A well-functioning right to be forgotten virtually poses an inalienability rule over personal information. This rule reduces information flows, and in such way it affects the right to access information of the same data subjects that it protects. Moreover, the rule has additional societal costs in the form of large implementation costs for data processers and a reduction in freedom of expression for data subjects.

In turn, the imperfect right to be forgotten that the EU can implement presents a risk compensation problem (Peltzman effect). This leads to an unfortunate CJEU decision in the *Google v. Spain* case, which materializes into an equally problematic implementation of the right,

modified to fit within current DPL to a point in which it is questionable whether the decision pertains the right to be forgotten at all.

The GDRP, in this way, by establishing the right in its article 17 goes beyond the scope of data protection that this framework justifies. In the best case scenario, it would create an inalienability rule that reduces information flow. In the worst case scenario, which is the most likely due to the jurisdictional limitations of the EU, it would create a Peltzman effect that leaves data subjects more vulnerable than before. An alternative version of the right to be forgotten can be formulated to maintain its central positive feature (increasing data subjects' flexibility) while avoiding the main problems of access to information, freedom of expression, and implementation costs. However, this version would not avoid the risk compensation problem that the jurisdictional limitations imply.

Another visible example of this exclusion mechanism are online tracking regulations, particularly pertaining cookies. Changing the default system for tracking from an opt-out to an opt-in system, where previous consent is needed to install cookies, is a way to create entitlements that enhance protection without creating property rights.

A relevant difference between this legal development and the last is that the theoretical background of the change in the default system for online tracking regulations goes beyond the rational choice framework; it bases itself on behavioral considerations. Accordingly, one must apply behavioral economics within the neoclassical framework described in order to evaluate the policy.

Online tracking regulations do fall within the scope of data protection that the framework explained in favor of DPL can justify. Still, some adjustments are recommendable from the perspective of behavioral economics and the technological characteristics of online tracking. The DNT laws set exclusionary power by establishing an opt-in mechanism but, in doing so, they apply policy defaults outside of their scope. The same level of exclusionary power can be set by presenting an active choice mechanism. Independently of the level of exclusionary power set, it is

recommendable to give the design of the choice system to agents who have the least possible counteracting interests to the policy. In the context of online tracking, this means targeting web browsers instead of websites. Finally, a stronger differentiation between session cookies and permanent cookies can be recommended, since the former carry lower privacy risks and are more important for the functioning of websites than the latter.

A visible common element of the two regulations is that they overtly seek to augment the level of control that people have over their own personal information by giving them the possibility to exclude others from it, giving data subjects an entitlement, but not a property right. These two central developments in DPL cannot be predicted or explained from an economic perspective without seeing DPL as a mechanism to allocate rights of exclusion to incentivize information, as the framework set here proposes.

6.3.! Future Research

Some extensions can be made from the lessons learned to other related topics within DPL. Namely, to the relationship between data protection and freedom of expression, to which is likely to be the future of DPL, and to the differences between the American and the European model of data protection.

What societies previously called liberty (the freedom to not have our information and actions controlled) they moved to call privacy, and in doing so they moved to worry not only about the freedom to not have our information and actions controlled by the government, but also by our peers. In this context, to disregard privacy is to allow for people to lose autonomy. Such right is more important from a consequentialist perspective than a mere ability to conceal information in order to deceive others; it is about allowing for a zone for thoughts, weaknesses and decision-making processes which is protected from the general public, and which by such protection eliminates fear of disclosure.

This opens the possibility to extend the conclusions made for the relationship between data protection and access to information to the relationship between data protection and freedom of speech. By the elimination of the fear of disclosure, privacy and freedom of speech, although sometimes at a tradeoff at the margin, are largely complementary: a lack of privacy imposes a chilling effect on freedom of speech. This idea is key to determining the optimal scope of balancing of both rights; independently of the weight a society might place in either of them, it is useful to make explicit what society is foregoing by placing itself on each part of the spectrum of such choice.

Regarding what one can expect of DPL, there seems to be a trend in data protection to grant more entitlements with increasing levels of exclusion to data subjects, while maintaining itself in the mid-way described between property and liability rules.

Although DPL augments levels of exclusion for data subjects, the Data Protection Directive does not border on the establishment of a property regime for personal data. The GDRP, while in the same line, presents more property elements than the Data Protection Directive; it broadens the requirement of data subjects' consent,[685] it strengthens property-rule-based remedies such as data subjects' possibilities to request an injunction from a court,[686] and it introduces the right to be forgotten giving it an *in rem* characteristic.[687] There seems to be a tendency in DPL to provide increasing levels of exclusion, where the newest developments such as the right to be forgotten provide a stronger exclusion power than the more traditional rights.

This increasing level of exclusion is to be expected from the point of view of the framework that was set. In copyright—the branch of law that was seen as the most analogous to DPL—the easier it is to copy a work,

---

[685] See article 7 of the GDRP.
[686] See articles 75(1) and 76(5) of the GDRP.
[687] See article 17 of the GDRP; Jacob Victor, "The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy," *Yale Law Journal* 123 (2013): 513.

the higher the level of protection must be to maintain stable incentives.[688] If the same is to be said about DPL, one should expect increasing levels of protection as long as technology keeps facilitating the collection, storage and dissemination of personal information.

The optimal level of exclusion to be given to privacy entitlements in cyberspace is difficult to define precisely, and largely depends on value judgments. In order to provide a precise answer, it is necessary for a society to decide the weight with which it values each of the elements in the tradeoffs involved, and such weights are likely to vary from one society to the other. The choice among the different options that lie in the spectrum between the absolute disclosure extreme and the no disclosure extreme ultimately depends, largely, on the shape of societal preferences. While one cannot, for this reason, resolve these tradeoffs optimally from a purely theoretical point of view, one can be made aware of which tradeoffs one is dealing with, and one can make the problems inherent in them more visible.

It has been argued that, for data protection, American commentators favor market-based solutions over comprehensive regulations, which are in turn preferred in Europe.[689] DPL in the EU is relatively property-oriented, containing several instances in which consent is needed for information to be transferred. On the other hand, the fair information practices, which are the main tool to protect informational privacy in the US, are harm-based and in such way more liability-oriented than DPL.[690] This has alarmed some European commentators.[691] This

---

[688] See William Landes and Richard Posner, "An Economic Analysis of Copyright Law," *Journal of Legal Studies* 18, no. 2 (1989): 325.

[689] See Pamela Samuelson, "Privacy as Intellectual Property?," *Stanford Law Review* 52, no. 5 (1999): 1125.

[690] See Paul Schwartz, "Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy Control, and Fair Information Practices," *Wisconsin Law Review* 1 (2000): 743. See also Omer Tene and Jules Polonetsky, "To Track or 'Do Not Track': Advancing Transparency and Individual Control in Online Behavioral Advertising," *Minnessota Journal of Law, Science & Technology* 13, no. 1 (2012): 281.

difference, however, is a result that can be expected from a framework that presents tradeoffs whose outcome ultimately depends on societal values and in such way considers that the choices within them does not have one single optimal outcome.

Simultaneously, it has been stated that a regime change towards property rights in the US would increase the control that data subjects have over an already existing market for their personal information, and in such way the change would not be radical.[692] This is especially applicable to establishing general privacy entitlements within American information technology law, since this is a previous step to defining the level of protection within the spectrum for which the creation of an entitlement allows.

In this way, one can give a reasonable account of the persistent regulatory differences between the EU and the US while not abandoning the idea that there are consequences from such differences that can be evaluated from an economic perspective. Once the economic rationale for protecting privacy is clear, one can see which the existing tradeoffs are, and one can see that the two regulatory schemes might just be giving priority to different values within them.

6.4.! Closing Remarks

Concluding the preceding analysis, one can state after the considerations made that it is possible from a law & economics perspective to explain DPL—accounting for the recent trends within it—and to provide policy recommendations for it. Regarding the former, the right to be forgotten and the limits on online tracking are examples on how the law evolves to further exclude others from one's personal information in the context of

---

691 See Lokke Moerel, *Big Data Protection. How to Make the Draft EU Regulation on Data Protection Future Proof* (Tilburg: Tilburg University Press, 2014). Chapter 2.

692 See Pamela Samuelson, "A New Kind of Privacy? Regulating Uses of Personal Data in the Global Information Economy," *California Law Review* 87, no. 3 (1999): 751.

new technologies; this is, to create entitlements for data subjects that did not exist so far. Regarding the latter, one can see that the right to be forgotten should at least be limited to those situations in which informational privacy diverts from traditional privacy problems, and that online tracking regulations should take into account the costs of different types of cookies and be weary with the design of policy defaults.

One should keep in mind, when reading the conclusions set here, that this analysis shows "one side of the Cathedral" of DPL.[693] What is more, this might even not be the most important side. Still, showing this side of the law can produce significant advancements. First, its other sides (deontic, human rights based) have been extensively explored already, and seeing this side is important to have a complete picture of the problems that it involves. Second, seeing this side makes it difficult for scholars who base their results on methodological individualism to say that privacy does not matter—that the cathedral is not there at all. Third, even if a policymaker chooses whether to protect privacy based solely on principled reasons, and abstracting from consequences, this analysis is useful to highlight the secondary effects of such decisions, preventing unintended consequences.

In a much quoted phrase, *Sun* CEO Scott Mcnealy told us that we have no privacy anyway, and that we should get over it.[694] This analysis has shown that the statement is not only untrue, but that there are good reasons why it is so. Failure to protect privacy would lead to an underproduction of information, and that is a scenario that all agents in the interaction would rather avoid.

---

[693] See generally Guido Calabresi and A. Douglas Melamed, "Property Rules, Liability Rules, and Inalienability: One View of the Cathedral," *Harvard Law Review* 85, no. 6 (1972): 1089.

[694] "You have zero privacy anyway. Get over it." First cited in Stephen Manes, "Private Lives? Not Ours!," *PC World*, April 18, 2000.

Bibliography

References

A29WP. "Guidelines on the Implementation of the Court of Justice of the European Union Judgment on 'Google Spain and Inc. v. AEPD and Mario Costeja Gonzalez.'" Brussels, November 26, 2014.

———. "O.J. 03/2013 on Purpose Limitation." Brussels, October 2, 2013.

———. "O.J. 15/2011 On the Definition of Consent." Brussels, July 13, 2011.

———. "O.J. 2/2010 on Online Behavioral Advertising." Brussels, June 22, 2010.

———. "O.J. 8/2010 on Applicable Law." Brussels, December 16, 2010.

Acquisti, Alessandro. "Nudging Privacy: The Behavioral Economics of Personal Information." *Institute of Electrical and Electronics Engineers Security and Privacy Magazine* 7, no. 6 (2009): 82.

———. "Privacy in Electronic Commerce and the Economics of Immediate Gratification." In *Proceedings of the Fifth Association for Computing Machinery Conference on Electronic Commerce*, edited by Jack Breese, Joan Feigenbaum, and Margo Seltzer, 21. New York: Association for Computing Machinery Press, 2004.

Acquisti, Alessandro, Laura Brandimarte, and George Loewenstein. "Privacy and Human Behavior in the Age of Information." *Science* 347, no. 6221 (2015): 509.

Acquisti, Alessandro, and Ralph Gross. "Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook." In *Proceedings of the Sixth Workshop on Privacy Enhancing Technologies*, 1. Cambridge: Robinson College of Cambridge University, 2006.

Acquisti, Alessandro, and Jens Grossklags. "Privacy and Rationality in Individual Decision Making." *Institute of Electrical and Electronics Engineers Security and Privacy Magazine* 3, no. 1 (2005): 26.

———. "Privacy Attitudes and Privacy Behavior." In *The Economics of Information Security*, edited by Jean Camp and Stephen Lewis. Dordrecht: Kluwer, 2004.

———. “What Can Behavioral Economics Teach Us About Privacy ?” In *Digital Privacy: Theory, Technologies and Practices*, edited by Alessandro Acquisti, Stefanos Gritzalis, Costos Lambrinoudakis, and Sabrina di Vimercanti, 363. Boca Raton: Auerbach Publications, 2007.

Acquisti, Alessandro, Leslie John, and George Loewenstein. “The Impact of Relative Standards on the Propensity to Disclose.” *Journal of Marketing Research* 49 (2012): 160.

———. “What Is Privacy Worth?” *Journal of Legal Studies* 42, no. 2 (2013): 249.

Alchian, Armen. “Some Economics of Property Rights.” *Il Politico* 30 (1965): 816.

Allen, Ronald, Mark Grady, Daniel Polsby, and Michael Yashko. “A Positive Theory of the Attorney-Client Privilege and the Work Product Doctrine.” *Journal of Legal Studies* 19, no. 2 (1990): 359.

Amador, Manuel, Ivan Werning, and George-Marios Angeletos. “Commitment vs. Flexibility.” *Econometrica* 74, no. 2 (2006): 365.

Ambrose, Meg, and Jeff Ausloos. “The Right to Be Forgotten Across the Pond.” *Journal of Information Policy* 3 (2013): 1.

American Bar Association. *Model Rules of Professional Conduct*. Chicago: American Bar Association, 2006.

Andolfatto, David. “A Theory of Inalienable Property Rights.” *Journal of Political Economy* 110, no. 2 (2002): 382.

Andrade, Eduardo, Velitchka Kaltcheva, and Barton Weitz. “Self-Disclosure on the Web: The Impact of Privacy Policy, Reward, and Company Reputation.” *Advances in Consumer Research* 29 (2002): 350.

Aquinas, Thomas. *Summa Theologiae*, 1917.

Arendt, Hannah. *The Human Condition*. New York: Anchor, 1959.

Aristotle. “Nicomanean Ethics,” n.d.

———. “Politics,” n.d.

Arndt, Heinz. "The Cult of Privacy." *Australian Quarterly* 21 (1949): 69.

Arrow, Kenneth. "Gifts and Exchanges." *Philosophy & Public Affairs* 1, no. 4 (1972): 343.

Ayres, Ian, and Robert Gertner. "Filling Gaps in Incomplete Contracts: An Economic Theory of Default Rules." *Yale Law Journal* 99, no. 1 (1989): 87.

———. "Strategic Contractual Inefficiency and the Optimal Choice of Legal Rules." *Yale Law Journal* 101, no. 4 (1992): 729.

Ayres, Ian, and Alan Schwartz. "The No-Reading Problem in Consumer Contract Law." *Stanford Law Review* 66 (2004): 545.

Ayres, Ian, and Eric Talley. "Distinguishing between Consensual and Nonconsensual Advantages of Liability Rules." *Yale Law Journal* 105, no. 1 (1995): 235.

———. "Solomonic Bargaining: Dividing a Legal Entitlement to Facilitate Coasean Trade." *Yale Law Journal* 104, no. 5 (1995): 1027.

Azfar, Omar. "Rationalizing Hyperbolic Discounting." *Journal of Economic Behavior & Organization* 38 (1999): 245.

Balkin, Jack. "The Future of Free Expression in a Digital Age." *Pepperdine Law Review* 36 (2008): 427.

Barnett, Randy. "Contract Remedies and Inalienable Rights." *Social Philosophy and Policy* 4 (1986): 179.

Benkler, Yochai. *The Wealth of Networks: How Social Production Transforms Markets and Freedom*. New Haven: Yale University Press, 2006.

Benn, Stanley. "Privacy, Freedom and Respect for Persons." In *Nomos XIII: Privacy*, edited by Ronald Pennock and John Chapman, Vol. 8. New York: Atherton Press, 1971.

Benn, Stanley, and Gerald Gaus. *Public and Private in Social Life*. Kent: Croom Helm, 1983.

Benndorf, Volker, Dorothea Kuebler, and Hans-Theo Normann. "Privacy Concerns, Voluntary Disclosure of Information, and Unraveling: An Experiment." *Forthcoming in European Economic Review*, 2015.

Bennett, Steven. "The 'Right to Be Forgotten': Reconciling EU and US Perspectives." *Berkeley Journal of International Law* 30, no. 1 (2012): 161.

Benoliel, Daniel. "Copyright Distributive Injustice." *Yale Journal of Law & Technology* 10 (2007): 45.

Bensman, Joseph, and Robert Lilienfeld. *Between Public and Private: The Lost Boundaries of the Self*. New York: Free Press, 1979.

Berendt, Bettina, Oliver Günther, and Sarah Spiekermann. "Privacy in E-Commerce." *Communications of the Association for Computing Machinery* 48, no. 4 (2005): 101.

Beresford, Alastair, Dorothea Kübler, and Sören Preibusch. "Unwillingness to Pay for Privacy: A Field Experiment." *Economics Letters* 117, no. 1 (2012): 25.

Bergelson, Vera. "It's Personal But Is It Mine? Toward Property Rights in Personal Information." *UC Davis Law Review* 37 (2003): 379.

Besen, Stanley, and Leo Raskind. "An Introduction to the Law and Economics of Intellectual Property." *Journal of Economic Perspectives* 5, no. 1 (1991): 3.

Besharov, Gregory, and Bentley Coffey. "Reconsidering the Experimental Evidence for Quasi-Hyperbolic Discounting." Duke Department of Economics Working Paper 03-03. Durham, 2003.

Bezanson, Randall. "The Right to Privacy Revisited: Privacy, News and Social Change." *California Law Review* 5, no. 80 (1992): 1133.

Blackstone, William. *Commentaries on the Laws of England*, 1769.

Blanchette, Jean-François, and Deborah Johnson. "Data Retention and the Panoptic Society: The Social Benefits of Forgetfulness." *The Information Society* 18, no. 1 (2002): 33.

Bloustein, Edward. "Privacy Is Dear at Any Price: A Response to Professor Posner's Economic Theory." *Georgia Law Review* 12 (1978): 429.

Bok, Sissela. *Secrets: On the Ethics of Concealment and Revelation*. New York: Vintage, 1989.

Boyd, Virginia. "Financial Privacy in the United States and the European Union: A Path to Transatlantic Regulatory Harmonization." *Berkeley Journal of International Law* 24 (2006): 939.

Bradford, Anu. "The Brussels Effect." *Northwestern University Law Review* 107, no. 1 (2012): 1.

Bradford, David. "Joint Products, Collective Goods, and External Effects: Comment." *Journal of Political Economy* 79, no. 5 (1971): 1119.

Brandimarte, Laura, Alessandro Acquisti, and George Loewenstein. "Misplaced Confidences: Privacy and the Control Paradox." *Social Psychological and Personality Science* 4, no. 3 (2012): 340.

Brenner, Susan. "The Fourth Amendment in an Era of Ubiquitous Technology." *Mississippi Law Journal* 75 (2005): 1.

Breyer, Stephen. "The Uneasy Case for Copyright: A Study of Copyright in Books, Photocopies and Computer Programs." *Harvard Law Review* 84, no. 2 (1970): 281.

Brown, Ian, and Douwe Korff. "Technology Development and Its Effect on Privacy and Law Enforcement. Report for the UK Information Commissioner's Office." Wilmslow: Information Commissioner's Office, 2004.

Brown, Ian, and Christian Marsden. *Regulating Code: Good Governance and Better Regulation in the Information Age*. Cambridge, Mass.: MIT Press, 2013.

Bruyer, Richard. "Privacy: A Review and Critique of the Literature." *Alberta Law Review* 43, no. 3 (2006): 553.

Bull, Hans Peter. *Informationelle Selbstbestimmung. Vision Oder Illusion? Datenschutz Im Spannungsverhältnis von Freiheit Und Sicherheit*. Tubingen: Mohr Siebeck, 2011.

Calabresi, Guido, and A. Douglas Melamed. "Property Rules, Liability Rules, and Inalienability: One View of the Cathedral." *Harvard Law Review* 85, no. 6 (1972): 1089.

Camerer, Colin. "Prospect Theory in the Wild: Evidence from the Field." In *Choices, Values and Frames*, edited by Daniel Kahneman and Amos Tversky, 294. Cambridge: Cambridge University Press, 2000.

Carrascal, Juan Pablo, Christopher Riederer, Vijay Erramilli, Mauro Cherubini, and Rodrigo de Oliveira. "Your Browsing Behavior for a Big Mac: Economics of Personal Information Online." In *Proceedings of the 22nd International Conference on World Wide Web*. Geneva, 2013.

Carroll, Gabriel, James Choi, David Laibson, Brigitte Madrian, and Andrew Metric. "Optimal Defaults and Active Decisions." *Quarterly Journal of Economics* 124, no. 4 (2009): 1639.

Casari, Marco. "Pre-Commitment and Flexibility in a Time Decision Experiment." *Journal of Risk and Uncertainty* 38, no. 2 (2009): 117.

Castellano, Pere Simon. "The Right to Be Forgotten under European Law: A Constitutional Debate." *Lex Electronica* 16, no. 1 (2012): 1.

Christensen, Laurits, Andrea Colciago, Federico Etro, and Greg Rafert. "The Impact of the Data Protection Regulation in the EU." *Intertic Policy Paper 13-1*, 2013.

Citron, Danielle. "Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age." *Southern California Law Review* 80 (2007): 241.

Clarke, Kenneth. "Data Protection (Speech)." London, May 26, 2011.

Clarke, Roger. "Profiling: A Hidden Challenge to the Regulation of Data Surveillance." *Journal of Law, Information and Science* 4 (1993): 403.

Coase, Ronald. "The Problem of Social Cost." *Journal of Law and Economics* 3, no. 1 (1960): 1.

Cohen, David, and Jack Knetsch. "Judicial Choice and the Disparities Between Measures of Economic Values." *Osgoode Hall Law Journal* 30 (1992): 737.

Cohen, Julie. “Examined Lives: Informational Privacy and the Subject as Object.” *Stanford Law Review* 52, no. 5 (2000): 1373.

———. “What Privacy Is For.” *Harvard Law Review* 126 (2013): 1904.

College bescherming persoonsgegevens. “Onderzoek CBP Naar Het Combineren van Persoonsgegevens Door Google. Rapport Definitieve Bevindingen,” November 25, 2013.

Conley, Chris. “The Right to Delete.” In *Intelligent Information Privacy Management*. Palo Alto: Association for the Advancement of Artificial Intelligence, 2010.

“Cookiewet Versoepeld: Verplichte Melding Voor Minder Cookies.” *Volkskrant*, December 20, 2012.

Cornes, Richard, and Todd Sandler. “Easy Riders, Joint Production and Public Goods.” *Economic Journal* 94, no. 375 (1984): 580.

Cornish, William, David Llewelyn, and Tanya Aplin. *Intellectual Property: Patents, Copyright, Trade Marks and Allied Rights*. London: Sweet & Maxwell, 2013.

Costa, Luiz, and Yves Poullet. “Privacy and the Regulation of 2012.” *Computer Law & Security Review* 28, no. 3 (2012): 254.

Crandall, Robert, and John Graham. “Automobile Safety Regulation and Offsetting Behavior: Some New Empirical Estimates.” *American Economic Review* 74, no. 2 (1984): 328.

Dasgupta, Partha, and Eric Maskin. “Uncertainty and Hyperbolic Discounting.” *The American Economic Review* 95, no. 4 (2005): 1290.

De Azevedo Cunha, Mario, Luisa Marin, and Giovanni Sartor. “Peer-to-Peer Privacy Violations and ISP Liability: Data Protection in the User-Generared Web.” *International Data Privacy Law* 2, no. 2 (2012): 1.

De Vattel, Emmerich. *Le Droit de Gens*, 1758.

Debussere, Frederic. “The EU E-Privacy Directive: A Monstrous Attempt to Starve the Cookie Monster?” *International Journal of Law and Information Technology* 13, no. 1 (2005): 70.

Department for Culture Media and Sport. "Open Letter on the UK Implementation of Article 5(3) of the E-Privacy Directive on Cookies." London, May 24, 2011.

Devlin, Patrick. *The Enforcement of Morals: Maccabaean Lecture in Jurisprudence of the British Academy*. New York: Oxford University Press, 1959.

Dickie, John. *Producers and Consumers in EU E-Commerce Law*. Portland: Hart Publishing, 2005.

Downs, Julie, George Loewenstein, and Jessica Wisdom. "Strategies for Promoting Healthier Food Choices." *American Economic Review* 99, no. 2 (2009): 159.

Driessen, Jan, Jan Schinkelshoek, Henry Meijdam, Joris Van Heukelom, Loek Hermans, Julius Minnaar, Ed Nijpels, and Jan-Willem Borsboom. "Verzoek Tot Inhoudelijke Behandeling Wijziging van de Telcommunicatiewet," July 3, 2011.

Dworkin, Ronald. "Lord Devlin and the Enforcement of Morals." *Yale Law Journal* 75, no. 6 (1966): 986.

Easterbrook, Frank, and Daniel Fischel. "The Corporate Contract." *Columbia Law Review* 89 (1989): 1416.

Eckersley, Peter. "How Unique Is Your Web Browser?" In *Privacy Enhancing Technologies Symposium*, edited by Mikhail Atallah and Nicholas Hopper, 1. Berlin: Springer Lecture Notes in Computer Science, 2010.

Engelfriet, Arnoud. "Websites Negeren Massaal de Cookiewet." *Cookierecht*, July 13, 2012.

Epstein, Edna. *The Attorney Client Privilege and the Work Product Doctrine*. Chicago: American Bar Association, 2001.

Etzioni, Amitai. *The Limits of Privacy*. New York: Basic Books, 2008.

European Commission. "A Comprehensive Approach on Personal Data Protection in the European Union." *Communication from the Commission to the European Parliament, the Council, The Economic*

and Social Committee and the Committee on the Regions, November 2010.

———. "Data Protection Reform: Frequently Asked Questions." *MEMO/12/41*, 2012.

———. "Digital Agenda for Europe. A Europe 2020 Initiative," 2015. http://ec.europa.eu/digital-agenda/.

———. "Proposal for a Regulation on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data," 2012.

Federal Communications Commission. "Trends in Telephone Service." Washington, DC, August 7, 2003.

Federal Trade Commission. "Annual Report to Congress for 2003 and 2004 Pursuant to the Do Not Call Registry." Washington, DC, October 4, 2005.

———. "Protecting Consumer Privacy in an Era of Rapid Change. Recommendations for Business and Policymakers." Washington, DC, March 26, 2012.

Fennell, Lee Anne. "Adjusting Alienability." *Harvard Law Review* 122, no. 5 (2009): 1403.

Feri, Francesco, Caterina Giannetti, and Nicola Jentzsch. "Disclosure of Personal Information Under Risk of Privacy Shocks." University of Bologna School of Economics Working Paper 875. Bologna, 2013.

Fernandez-Villaverde, Jesus, and Arijit Mukherji. "Can We Really Observe Hyperbolic Discounting?" Penn Institute for Economic Research Working Paper 02-08. Philadelphia, 2006.

Filmer, Robert. *Patriarcha*, 1680.

Fleischer, Peter. "Foggy Thinking About the Right to Oblivion." *Privacy*, March 2011.

Frederick, Shane, George Loewenstein, and Ted O'Donoghue. "Time Discounting and Time Preference: A Critical Review." *Journal of Economic Literature* 40, no. 2 (2002): 351.

Fried, Charles. “Privacy.” *Yale Law Journal* 77, no. 4 (1968): 475.

Fuller, Elizabeth. “Implied Consent Statutes: What Is Refusal?” *American Journal of Trial Advocacy* 9 (1986).

Furnas, Alexander. “It’s Not All about You: What Privacy Advocates Don't Get about Data Tracking on the Web.” *The Atlantic*, March 15, 2012.

Gavison, Ruth. “Privacy and the Limits of the Law.” *Yale Law Journal* 89, no. 3 (1980): 421.

George, Robert. *Making Men Moral*. New York: Oxford University Press, 1993.

Gerety, Tom. “Redefining Privacy.” *Harvard Civil Rights-Civil Liberties Law Review* 12 (1977): 233.

Gerstein, Robert. “Intimacy and Privacy.” *Ethics* 89, no. 1 (1978): 76.

Gideon, Julia, Serge Egelman, Lorrie Faith Cranor, and Alessandro Acquisti. “Power Strips, Prophylactics , and Privacy, Oh My!” In *Proceedings of the Second Symposium on Usable Privacy and Security*, 133. New York, 2006.

Goodin, Robert, and Frank Jackson. “Freedom from Fear.” *Philosophy & Public Affairs* 35 (2007): 249.

Goodwin, Cathy. “A Conceptualization of Motives to Seek Privacy for Nondeviant Consumption.” *Journal of Consumer Psychology* 1, no. 3 (1992): 261.

Gordon, Wendy. “Asymmetric Market Failure and Prisioner’s Dilemma in Intellectual Property.” *University of Dayton Law Review* 17 (1992): 853.

———. “Fair Use as Market Failure: A Structural and Economic Analysis of the‘ Betamax’ Case and Its Predecessors.” *Columbia Law Review* 82, no. 8 (1982): 1600.

Graham, John, and Steven Garber. “Evaluating the Effects of Automobile Safety Regulation.” *Journal of Policy Analysis and Management* 3, no. 2 (1984): 206.

Grey, Thomas. *The Legal Enforcement of Morality*. New York: Alfred A. Knopf, 1983.

Grimmelmann, James. "Big Data's Other Privacy Problem." University of Maryland Working Paper 14-7. College Park, 2014.

———. "Don't Censor Search." *Yale Law Journal Pocket Part* 48 (2007): 117.

———. "The Google Dilemma." *New York Law School Law Review* 53 (2008): 939.

Groom, Victoria, and Ryan Calo. "Reversing the Privacy Paradox: An Experimental Study." In *Proceedings of the 39th Telecommunications Policy Research Conference*. Schertz, 2011.

Groot, Arnoud. "'Naïeve' Cookiewet Loopt Achter de Feiten Aan." *Emerce*, November 4, 2010.

Habermas, Jürgen. *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society*. Cambridge, Mass.: MIT Press, 1991.

Hagel, John, and Jeffrey Rayport. "The Coming Battle for Consumer Information." *Harvard Business Review* 75, no. 1 (1997): 53.

Halevy, Yoram. "Diminishing Impatience: Disentangling Time Preference from Uncertain Lifetime." University of British Columbia Department of Economics Working Paper 05-17. Vancouver, 2005.

———. "Strotz Meets Allais: Diminishing Impatience and the Certainty Effect." *The American Economic Review* 98, no. 3 (2008): 1145.

Hann, Il-Horn, Kai-Lung Hui, Sang-Yong Lee, and Ivan Png. "Overcoming Online Information Privacy Concerns: An Information-Processing Theory Approach." *Journal of Management Information Systems* 24, no. 2 (2007): 13.

Harbinja, Edina. "Does the EU Data Protection Regime Protect Post-Mortem Privacy and What Could Be the Potential Alternatives?" *SCRIPT-Ed* 10, no. 1 (2013): 19.

Hardy, Trotter. "Property (and Copyright) in Cyberspace." *University of Chicago Legal Forum* 1 (1996): 217.

Hart, Herbert. "Immorality and Treason." *Listener*, July 30, 1959.

———. "Immorality and Treason." In *The Philosophy of Law*, edited by Ronald Dworkin. New York: Oxford University Press, 1977.

———. *Law, Liberty, and Morality*. Stanford: Stanford University Press, 1963.

Hart, Oliver, and John Moore. "Property Rights and the Nature of the Firm" 98, no. 6 (1990): 1119.

Hazard, Geoffrey. "A Historical Perspective on the Attorney-Client Privilege." *California Law Review* 66, no. 5 (1978): 1061.

Helberger, Natali. "Freedom of Expression and the Dutch Cookie-Wall." University of Amsterdam Institute for Information Law Working Paper 13-01. Amsterdam, 2013.

Hendel, John. "Why Journalists Shouldn't Fear Europe's 'Right to Be Forgotten.'" *Atlantic*, January 2012.

Hermstruwer, Yoan, and Stephan Dickert. "Tearing the Veil of Privacy Law: An Experiment on Chilling Effects and the Right to Be Forgotten." Preprints of the Max Planck Institute for Collective Goods. Bonn, 2013.

Hirshleifer, Jack. "Privacy. Its Origin, Function and Future." *Journal of Legal Studies* 9, no. 4 (1980): 649.

Hohfeld, Wesley Newcomb. "Fundamental Legal Conceptions as Applied to Judicial Reasoning." *Yale Law Journal* 26, no. 8 (1917): 710.

———. "Some Fundamental Legal Conceptions as Applied in Judicial Reasoning." *Yale Law Journal* 23, no. 1 (1913): 16.

Hoofnagle, Chris Jay. "Internalizing Identity Theft." *UCLA Journal of Law and Technology* 13 (2009): 1.

Horne, Daniel, and David Horne. "Domains of Privacy: Toward an Understanding of Underlying Factors." In *Direct Marketing Educators' Conference*. San Francisco, 1998.

Hsu, Shi-Ling. "A Two-Dimensional Framework for Analyzing Property Rights Regimes." *University of California Davis Law Review* 36, no. 4 (2003): 813.

Huberman, Bernardo, Eytan Adar, and Leslie Fine. "Valuating Privacy." *Institute of Electrical and Electronics Engineers Security and Privacy Magazine* 3 (2005): 22.

Hui, Kai-Lung, Hock Hai Teo, and Sang-Yong Lee. "The Value of Privacy Assurance: An Exploratory Field Experiment." *Management Information Systems Quarterly* 31, no. 1 (2007): 19.

Hurt, Robert, and Robert Shuchman. "The Economic Rationale of Copyright." *American Economic Review* 56, no. 1 (1966): 421.

Hylton, Keith. "Property Rules, Liability Rules and Immunity: An Application to Cyberspace." *Boston University Law Review* 87 (2007): 1.

Imwinkelried, Edward. "The New Wigmore: An Essay on Rethinking the Foundation of Evidentiary Privileges." *Boston University Law Review* 83 (2003): 315.

Information Commissioner's Office. "Guidance on the Rules on Use of Cookies and Similar Technologies." London, May 2012.

Inness, Julie. *Privacy, Intimacy, and Isolation*. New York: Oxford University Press, 1996.

Jentzsch, Nicola, Sören Preibusch, and Andreas Harasser. "Study on Monetising Privacy: An Economic Model for Pricing Personal Information. Report for the European Network and Information Security Agency." Heraklion, 2012.

Jimenez Cano, Rosa. "Google Comienza a Aplicar El 'Derecho Al Olvido.'" *El País*, July 13, 2014.

John, Leslie, Alessandro Acquisti, and George Loewenstein. "Strangers on a Plane: Context-Dependent Willingness to Divulge Sensitive Information." *Journal of Consumer Research* 37, no. 5 (2011): 858.

Johnson, Eric, Steven Bellman, and Gerald Lohse. "Defaults, Framing and Privacy: Why Opting In-Opting Out." *Marketing Letters* 13, no. 1 (2002): 5.

Johnson, Eric, and Daniel Goldstein. "Defaults and Donation Decisions." *Transplantation* 78 (2004): 1713.

———. "Medicine: Do Defaults Save Lives?" *Science* 302, no. 5649 (2003): 1338.

Johnston, Jason. "Strategic Bargaining and the Economic Theory of Contract Default Rules." *Yale Law Journal* 100, no. 3 (1990): 615.

Joksch, Hans. "Critique of Sam Peltzman's Study: The Effects of Automobile Safety Regulation." *Accident Analysis & Prevention* 8, no. 2 (1976): 129.

Jordan, Robert, and William Warren. "Disclosure of Finance Charges: A Rationale." *Michigan Law Review* 64, no. 7 (1966): 1285.

Kahan, Marcel. "Causation and Incentives to Take Care Under the Negligence Rule." *Journal of Legal Studies* 18, no. 2 (1989): 427.

Kahneman, Daniel, Jack Knetsch, and Richard Thaler. "Anomalies: The Endowment Effect, Loss Aversion, and Status Quo Bias." *Journal of Economic Perspectives* 5, no. 1 (1991): 193.

"Kamer Wil Einde Pop-Ups Door Cookiewet." *NU*, February 13, 2013.

"Kamp (EZ) Gaat Cookievoorstel D66 Bestuderen." *Emerce*, November 22, 2012.

Kamp, Henk. "Kamerbrief over Analytische Cookies En Artikel 11.7a van de Telecommunicatiewet." 's-Gravenhage, December 20, 2012.

Kang, Jerry. "Information Privacy in Cyberspace Transactions." *Stanford Law Review* 50, no. 4 (1998): 1193.

Kapczynski, Amy. "The Cost of Price: Why and How to Get Beyond Intellectual Property Internalism." *UCLA Law Review* 59, no. 4 (2012): 970.

Keller, Punam, Bari Harlam, George Loewenstein, and Kevin Volpp. "Enhanced Active Choice: A New Method to Motivate Behavior Change." *Journal of Consumer Psychology* 21, no. 4 (2011): 376.

Kelley, Patrick, Lucian Cesca, Joanna Bresee, and Lorrie Faith Cranor. "Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach." In *Proceedings of the Association for Computing Machinery Special Interest Group on Computer-Human Interaction Conference*, 1573. New York: Association for Computing Machinery Press, 2010.

Kelley, Patrick Gage, Joanna Bresee, Lorrie Faith Cranor, and Robert Reeder. "A 'Nutrition Label' for Privacy." In *Proceedings of the Fifth Symposium On Usable Privacy and Security*, 4. New York: Association for Computing Machinery Press, 2009.

Keren, Gideon, and Peter Roelofsma. "Immediacy and Certainty in Intertemporal Choice." *Organizational Behavior and Human Decision Processes* 63, no. 3 (1995): 287.

Kesan, Jay, and Rajiv Shah. "Setting Software Defaults: Perspectives from Law, Computer Science and Behavioral Economics." *Notre Dame Law Review* 82, no. 2 (2006): 583.

Kobrin, Stephen. "Safe Harbours Are Hard to Find: The Trans-Atlantic Data Privacy Dispute, Territorial Jurisdiction and Global Governance." *Review of International Studies* 30, no. 1 (2004): 111.

Koops, Bert-Jaap. "Forgetting Footprints, Shunning Shadows: A Critical Analysis of the 'Right to Be Forgotten' in Big Data Practice." *SCRIPT-Ed* 8, no. 3 (2011): 229.

———. "The Inflexibility of Techno-Regulation and the Case of Purpose-Binding." *Legisprudence* 5 (2011): 171.

Korobkin, Russell. "Inertia and Preference in Contract Negotiation: The Psychological Power of Default Rules and Form Terms." *Vanderbilt Law Review* 51, no. 6 (1998): 1583.

———. “The Endowment Effect and Legal Analysis.” *Northwestern University Law Review* 97 (2003): 1227.

———. “The Status Quo Bias and Contract Default Rules.” *Cornell Law Review* 83 (1998): 608.

Kripke, Homer. “Gesture and Reality in Consumer Credit Reform.” *NYU Law Review* 44 (1969): 1.

Kruskal, William. “Terms of Reference: Singular Confusion about Multiple Causation.” *Journal of Legal Studies* 15, no. 2 (1986): 427.

Ku, Raymond. “The Creative Destruction of Copyright: Napster and the New Economics of Digital Technology.” *University of Chicago Law Review* 69, no. 1 (2002): 263.

Kulk, Stefan, and Frederik Zuiderveen Borgesius. “Google Spain v. Gonzalez: Did the Court Forget about Freedom of Expression?” *European Journal of Risk Regulation* 5, no. 3 (2014): 389.

Kurz, Heinz. “Classical and Early Neoclassical Economists on Joint Production.” *Metroeconomica* 38 (1986): 1.

———. “Goods and Bads: Sundry Observations on Joint Production, Waste Disposal, and Renewable and Exhaustible Resources.” *Progress in Industrial Ecology* 3, no. 4 (2006): 280.

Kymlicka, Will. *Contemporary Political Philosophy*. New York: Oxford University Press, 2001.

Landes, William, and Richard Posner. “An Economic Analysis of Copyright Law.” *Journal of Legal Studies* 18, no. 2 (1989): 325.

———. “Multiple Tortfeasors: An Economic Analysis.” *Journal of Legal Studies* 9, no. 3 (1980): 517.

Laudon, Kenneth. “Extensions to the Theory of Markets and Privacy: Mechanics of Pricing Information.” Stern School of Business Working Paper 97-04. New York, 1997.

———. “Markets and Privacy.” *Communications of the Association for Computing Machinery* 39, no. 9 (1996): 92.

Lee, Simon. *Law and Morals*. New York: Oxford University Press, 1986.

Leenes, Ronald, and Eleni Kosta. "Taming the Cookie Monster with Dutch Law. A Tale of Regulatory Failure." *Computer Law & Security Review* 31, no. 2 (2015).

Legarre, Santiago. "The Historical Origins of the Police Power." *University of Pennsylvania Journal of Constitutional Law* 9 (2006): 745.

Lemley, Mark. "Rationalising Internet Safe Harbors." *Journal of Telecommunication and High Technology Law* 6 (2007): 101.

Leon, Pedro Giovanni, Blase Ur, Rebecca Balebako, Lorrie Faith Cranor, Richard Shay, and Yang Wang. "Why Johnny Can't Opt out: A Usability Evaluation of Tools to Limit Online Behavioral Advertising." In *Proceedings of the Association for Computing Machinery Special Interest Group on Computer-Human Interaction Conference*, 589. New York: Association for Computing Machinery Press, 2012.

Lessig, Lawrence. *Code 2.0*. New York: Basic Books, 2006.

———. *Code and Other Laws of Cyberspace*. New York: Basic Books, 1999.

———. "Privacy and Attention Span." *Georgetown Law Journal* 89 (2000): 2063.

———. "The Architecture of Privacy." *Vanderbilt Journal of Entretainment Law and Practice* 1 (1999): 56.

———. "The Law of the Horse: What Cyberlaw Might Teach." *Harvard Law Review* 113, no. 2 (1999): 501.

Leval, Pierre. "Toward a Fair Use Standard." *Harvard Law Review* 103, no. 5 (1990): 1105.

Levmore, Saul. "Probabilistic Recoveries, Restitution, and Recurring Wrongs." *Journal of Legal Studies* 19, no. 2 (1990): 691.

Lichtman, Doug, and Eric Posner. "Holding Internet Service Providers Accountable." *Supreme Court Economic Review* 14 (2006): 221.

Liebowitz, Stan. "Is Efficient Copyright a Reasonable Goal?" *George Washington Law Review* 79, no. 6 (2011): 1692.

Liu, Joseph. "Copyright and Time: A Proposal." *Michigan Law Review* 101, no. 2 (2002): 409.

Locke, John. *Two Treatises of Government*, 1689.

Loerke, Stephan. "The Dutch Find a Lighter Touch on Internet Privacy Laws." *AdAge*, July 3, 2013.

Lunney, Glynn. "Fair Use and Market Failure: Sony Revisited." *Boston University Law Review* 82 (2002): 975.

———. "Reexamining Copyright's Incentives-Access Paradigm." *Vanderbilt Law Review* 49 (1996): 483.

Luzak, Joasia. "Much Ado about Cookies: The European Debate on the New Provisions of the ePrivacy Directive Regarding Cookies." *European Review of Private Law* 21, no. 1 (2013): 221.

———. "Privacy Notice for Dummies? Towards European Guidelines on How to Give 'Clear and Comprehensive Information' on the Cookies' Use in Order to Protect the Internet Users' Right to Online Privacy." *Journal of Consumer Policy* 37, no. 1 (2014): 91.

Madrian, Brigitte, and Dennis Shea. "The Power of Suggestion: Inertia in 401(k) Participation and Savings Behavior." *Quarterly Journal of Economics* 116, no. 4 (2001): 1149.

Manes, Stephen. "Private Lives? Not Ours!" *PC World*, April 18, 2000.

Mantelero, Alessandro. "The EU Proposal for a General Data Protection Regulation and the Roots of the 'right to Be Forgotten.'" *Computer Law & Security Review* 29, no. 3 (2013): 229.

Mayer-Schönberger, Viktor. *Delete: The Virtue of Forgetting in the Digital Age*. Princeton: Princeton University Press, 2009.

Mayes, Tessa. "We Have No Right to Be Forgotten Online." *The Guardian*, March 11, 2011.

McDonald, Aleecia, and Lorrie Faith Cranor. "Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising." In *Proceedings of the 38th Research Conference on Communication, Information and Internet Policy*. Arlington, 2010.

———. “The Cost of Reading Privacy Policies.” *I/S: Journal of Law and Policy for the Information Society* 4 (2008): 543.

McGuire, Joseph, and Joseph Kable. “Decision Makers Calibrate Behavioral Persistence on the Basis of Time-Interval Experience.” *Cognition* 124, no. 2 (2012): 216.

———. “Rational Temporal Predictions Can Underlie Apparent Failures to Delay Gratification.” *Psychological Review* 120, no. 2 (2013): 395.

McKenzie, Craig, Michael Liersch, and Stacey Finkelstein. “Recommendations Implicit in Policy Defaults.” *Psychological Science* 17, no. 5 (2006): 414.

McKinley, Katherine. “Cleaning Up After Cookies Version 1.0.” *Technical Report for ISEC Partners*. San Francisco, 2010.

“Meerderheid Tweede Kamer Wil Einde Aan Cookie-Popups.” *Tweakers*, February 13, 2013.

Mell, Patricia. “Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness.” *Berkeley Technology Law Journal* 11, no. 1 (1996): 26.

Mercado Kierkegaard, Sylvia. “How the Cookies (almost) Crumbled: Privacy & Lobbyism.” *Computer Law & Security Review* 21, no. 4 (2005): 310.

Merrill, Thomas, and Henry Smith. “Making Coasean Property More Coasean.” *Journal of Law and Economics* 54, no. 4 (2011): 77.

———. “What Happened to Property in Law and Economics.” *Yale Law Journal* 111, no. 2 (2001): 357.

Milgate, Murray. “Goods and Commodities.” Edited by Lawrence Blume and Steven Durlauf. *The New Palgrave Dictionary of Economics*. New York: Macmillan, 2008.

Mill, John Stuart. *On Liberty*, 1859.

———. *Principles of Political Economy: With Some of Their Applications to Social Philosophy*. Longmans, Green, 1865.

Milne, George, and Mary Culnan. "Strategies for Reducing Online Privacy Risks: Why Consumers Read (or Don't Read) Online Privacy Notices." *Journal of Interactive Marketing* 18, no. 3 (2004): 15.

Ministry of Security and Justice and the Central Bureau of Statistics. "Safety Monitor 2012," 2013.

"Mislukte Cookiewet Is Een Wijze Les." *NetKwesties*, April 11, 2013.

Mitchell, Basil. *Law, Morality and Religion in a Secular Society*. New York: Oxford University Press, 1968.

Mitrou, Lilian. "The Impact of Communications Data Retention on Fundamental Rights and Democracy." In *Surveillance and Democracy*, edited by Kevin Haggerty and Minas Samatas, 127. London: Routledge, 2010.

Mitrou, Lilian, and Maria Karyda. "EU's Data Protection Reform and the Right to Be Forgotten: A Legal Response to a Technological Challenge?" In *Proceedings of the Fifth International Conference of Information Law and Ethics*, 29. Corfu, 2012.

Moerel, Lokke. *Big Data Protection. How to Make the Draft EU Regulation on Data Protection Future Proof*. Tilburg: Tilburg University Press, 2014.

Murphy, Richard. "Property Rights in Personal Information: An Economic Defense of Privacy." *Georgetown Law Journal* 84, no. 1 (1995): 2381.

Naghavi, Alireza, and Günther Schulze. "Bootlegging in the Music Industry: A Note." *European Journal of Law and Economics* 12, no. 1 (2001): 57.

Nissenbaum, Helen. "Privacy as Contextual Integrity." *Washington Law Review* 19 (2004): 119.

Noam, Eli. "Privacy and Self-Regulation: Markets for Electronic Privacy." In *Privacy and Self-Regulation in the Information Age*, edited by Barbara Wellbery, 21. Washington, DC: National Telecommunications and Information Administration, 1997.

Norberg, Patricia, Daniel Horne, and David Horne. "The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors." *Journal of Consumer Affairs* 41, no. 1 (2007): 100.

O'Brien, David. *Privacy, Law, and Public Policy*. New York: Praeger Publishers, 1979.

O'Donoghue, Ted, and Matthew Rabin. "Choice and Procrastination." *Quarterly Journal of Economics* 116, no. 1 (2001): 121.

———. "Doing It Now or Later." *The American Economic Review* 89, no. 1 (1999): 103.

OPTA. "Veelgestelde Vragen over de Cookieregels," February 2013.

"Opta Overtreedt Eigen Cookie-Regels." *NU*, October 26, 2012.

Parent, William. "A New Definition of Privacy for the Law." *Law and Philosophy* 2, no. 1980 (1983): 305.

———. "Privacy, Morality, and the Law." *Philosophy & Public Affairs* 12, no. 4 (1983): 269.

Payne, John, James Bettman, and Eric Johnson. *The Adaptive Decision Maker*. New York: Cambridge University Press, 1993.

Peltzman, Sam. "A Reply to Robertson." *Journal of Economic Issues* 11, no. 3 (1977): 672.

———. "Offsetting Behavior, Medical Breakthroughs, and Breakdowns." *Journal of Human Capital* 5, no. 3 (2011): 302.

———. "The Effects of Automobile Safety Regulation." *Journal of Political Economy* 83, no. 4 (1975): 677.

Peng, Weihong, and Jenniffer Cisna. "HTTP Cookies. A Promising Technology." *Online Information Review* 24, no. 2 (2000): 150.

Plant, Arnold. "The Economic Aspects of Copyright in Books." *Economica* 1 (1934): 167.

———. *The New Commerce in Ideas and Intellectual Property*. London: Athlone Press, 1953.

Posner, Richard. "An Economic Theory of Privacy." *American Enterprise Institute Journal of Government and Society (Regulation)* 2 (1978): 19.

———. “Privacy.” Edited by Peter Newman. *The New Palgrave Dictionary of Economics and the Law*. New York: Macmillan, 1998.

———. “Privacy, Surveillance, and Law.” *The University of Chicago Law Review* 75, no. 1 (2008): 245.

———. “The Economics of Privacy.” *The American Economic Review* 71, no. 2 (1981): 405.

———. “The Right of Privacy.” *Georgia Law Review* 12, no. 3 (1978): 393.

———. “When Is Parody Fair Use?” *Journal of Legal Studies* 21, no. 1 (1992): 67.

Post, Robert. “The Social Foundations of Privacy: Community and Self in the Common Law Tort.” *California Law Review* 77 (1989): 957.

———. “Three Concepts of Privacy.” *Georgetown Law Journal* 89 (2000): 2087.

Prins, Corien. “Property and Privacy: European Perspectives and the Commodification of Our Identity.” In *The Future of the Public Domain*, edited by Lucie Guibault and Bernt Hugenholtz, 223. Alphen aan den Rijn: Kluwer Law International, 2006.

———. “The Propertization of Personal Data and Identities.” *Electronic Journal of Comparative Law* 8, no. 3 (2004): 1.

———. “When Personal Data, Behavior and Virtual Identities Become a Commodity: Would a Property Rights Approach Matter?” *SCRIPT-Ed* 3, no. 4 (2006): 270.

Purtova, Nadezhda. “Illusion of Personal Data as No One’s Property.” *Law, Innovation and Technology* 7, no. 1 (2015): 83.

———. “Property in Personal Data: A European Perspective on the Instrumentalist Theory of Propertisation.” *European Journal of Legal Studies* 2 (2010): 3.

———. *Property Rights in Personal Data: A European Perspective*. Tilburg: Proefschrift ter verkrijging van de graad van doctor aan de Universiteit van Tilburg, 2011.

Rachels, James. "Why Privacy Is Important." *Philosophy & Public Affairs* 4, no. 4 (1975): 323.

Raskind, Leo. "A Functional Interpretation of Fair Use: The Fourteenth Donald C. Brace Memorial Lecture." *Journal of the Copyright Society* 31 (1983): 601.

Read, Daniel. "Is Time-Discounting Hyperbolic or Subadditive?" *Journal of Risk and Uncertainty* 23, no. 1 (2001): 5.

Read, Daniel, and Peter Roelofsma. "Subadditive versus Hyperbolic Discounting: A Comparison of Choice and Matching." *Organizational Behavior and Human Decision Processes* 91, no. 2 (2003): 140.

Reding, Viviane. "Data Protection Reform: Restoring Trust and Building the Digital Age Single Market." *Speech 13/720 at the Fourth Annual European Data Protection Conference*. Brussels, September 17, 2013.

———. "The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age." *Speech 12/26 at the Innovation Conference: Digital, Life, Design*. Munich, January 24, 2012.

———. "The Upcoming Data Protection Reform for the European Union." *International Data Privacy Law* 1 (2011): 3.

Regan, Priscilla. *Legislating Privacy: Technology, Social Values, and Public Policy*. University of North Carolina Press, 1995.

Reiman, Jeffrey. "Privacy, Intimacy and Personhood." *Philosophy & Public Affairs* 6, no. 1 (1976): 26.

Richards, Neil. "The Dangers of Surveillance." *Harvard Law Review* 126, no. 1 (2013): 1934.

Richards, Neil, and Daniel Solove. "Privacy's Other Path: Recovering the Law of Confidentiality." *Georgetown Law Journal* 96 (2007): 124.

Robertson, Leon. "A Critical Analysis of Peltzman's 'The Effects of Automobile Safety Regulation.'" *Journal of Economic Issues* 11, no. 3 (1977): 587.

Robinson, Glen. "Multiple Causation in Tort Law: Reflections on the DES Cases." *Virginia Law Review* 68, no. 4 (1982): 713.

Robinson, Neil, Hans Graux, Maarten Botterman, and Lorenzo Valeri. "Review of EU Data Protection Directive. Report for the UK Information Commissioner's Office." London, 2009.

Rodrigues, Ruben. "Privacy on Social Networks." In *The Offensive Internet*, edited by Saul Levmore and Martha Nussbaum, 237. Cambridge, Mass.: Harvard University Press, 2010.

Romanosky, Sasha, and Alessandro Acquisti. "Privacy Costs and Personal Data Protection: Economic and Legal Perspectives." *Berkeley Technology Law Journal* 24, no. 3 (2009): 1061.

Ronellenfitsch, Michael. "Bull, Hans Peter, Informationelle Selbstbestimmung-Vision Oder Illusion? Datenschutz Im Spannungsverhältnis von Freiheit Und Sicherheit." *Die Verwaltung: Zeitschrift Für Verwaltungsrecht Und Verwaltungswissenschaften* 44, no. 4 (2011): 601.

Rose-Ackerman, Susan. "Inalienability and the Theory of Property Rights." *Columbia Law Review* 85, no. 5 (1985): 931.

Rosen, Jeffrey. "The Right to Be Forgotten." *Stanford Law Review Online* 64 (2012): 88.

———. *The Unwanted Gaze: The Destruction of Privacy in America*. New York: Vintage Books, 2001.

Rosenberg, David. "The Causal Connection in Mass Exposure Cases: A 'Public Law' Vision of the Tort System." *Harvard Law Review* 97, no. 4 (1984): 849.

Rosenblum, Nancy. *Another Liberalism: Romanticism and the Reconstruction of Liberal Thought*. Cambridge, Mass.: Harvard University Press, 1987.

Rule, James. *Privacy in Peril: How We Are Sacrificing a Fundamental Right in Exchange for Security and Convenience*. New York: Oxford University Press, 2007.

Rule, James, and Lawrence Hunter. "Towards Property Rights in Personal Data." In *Visions of Privacy: Policy Choices for the Digital Age*, edited by Colin Bennett and Rebecca Grant, 168. Toronto: University of Toronto Press, 1999.

Samuelson, Pamela. "A New Kind of Privacy? Regulating Uses of Personal Data in the Global Information Economy." *California Law Review* 87, no. 3 (1999): 751.

———. "Privacy as Intellectual Property?" *Stanford Law Review* 52, no. 5 (1999): 1125.

Samuelson, Paul. "The Pure Theory of Public Expenditure." *Review of Economics and Statistics* 36 (1954): 387.

Samuelson, William, and Richard Zeckhauser. "Status Quo Bias in Decision Making." *Journal of Risk and Uncertainty* 1 (1988): 7.

Sartor, Giovanni. "Providers' Liabilities in the New EU Data Protection Regulation: A Threat to Internet Freedoms?" *International Data Privacy Law* 3, no. 1 (2013): 3.

Sartor, Giovanni, and Mario de Azevedo Cunha. "The Italian Google-Case: Privacy, Freedom of Speech and Responsibility of Providers for User-Generated Contents." *International Journal of Law and Information Technology* 18, no. 4 (2010): 356.

Savin, Andrej. *Research Handbook on EU Internet Law*. Cheltenham: Edward Elgar, 2014.

Schaumann, Niels. "Copyright Infringement and Peer-to-Peer Technology." *William Mitchell Law Review* 28, no. 3 (2002): 1001.

Schneier, Bruce. *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. New York: Norton & Company, 2015.

Schwartz, Paul. "Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy Control, and Fair Information Practices." *Wisconsin Law Review* 1 (2000): 743.

———. "Privacy and Democracy in Cyberspace." *Vanderbilt Law Review* 52 (1999): 1607.

———. “Privacy Inalienability and the Regulation of Spyware.” *Berkeley Technology Law Journal* 20 (2005): 1269.

———. “Property, Privacy, and Personal Data.” *Harvard Law Review* 117, no. 7 (2004): 2056.

———. “The EU-US Privacy Collision: A Turn to Institutions and Procedures.” *Harvard Law Review* 126 (2013): 1966.

Schwartz, Paul, and Daniel Solove. “PII Problem: Privacy and a New Concept of Personally Identifiable Information, The.” *NYU Law Review* 86 (2011): 1814.

Schwartz, Paul, and William Treanor. “The New Privacy.” *Michigan Law Review* 101 (2003): 2163.

Scott, Gini Graham. *Mind Your Own Business: The Battle for Personal Privacy*. Cambridge, Mass.: Perseus Books, 1995.

Sergent, Randolph. “A Fourth Amendment Model for Data Networks and Computer Privacy.” *Vanderbilt Law Review* 81 (1995): 1181.

Shah, Rajiv, and Jay Kesan. “Policy through Software Defaults.” In *Proceedings of the National Conference on Digital Government Research*, 265. New York: Association for Computing Machinery Press, 2006.

Shils, Edward. “Privacy: Its Constitution and Vicissitudes.” *Law and Contemporary Problems* 31, no. 2 (1966): 281.

Shostack, Adam, and Paul Syverson. “What Price Privacy? (and Why Identity Theft Is about Neither Identity nor Theft).” In *Economics of Information Security,* edited by Jean Camp and Stephen Lewis, 129. Norwell: Kluwer, 2004.

Sloan, Robert, and Richard Warner. “Big Data and the ‘New’ Privacy Tradeoff.” Chicago-Kent College of Law Research Paper 13-33, 2013.

———. *Unauthorized Access: The Crisis in Online Privacy and Security*. Boca Raton: CRC Press, 2013.

Slobogin, Christopher. “Transaction Surveillance by the Government.” *Mississippi Law Journal* 75 (2005): 139.

Smith, Adam. *Lectures on Jurisprudence*, 1764.

Smith, Robert. *Ben Franklin's Web Site: Privacy and Curiosity from Plymouth Rock to the Internet*. Washington, DC: Sheridan Books, 2000.

Solove, Daniel. "A Tale of Two Bloggers: Free Speech and Privacy in the Blogosphere." *Washington University Law Review* 84 (2006): 1195.

———. "Conceptualizing Privacy." *California Law Review* 90, no. 4 (2002): 1087.

———. "The First Amendment as Criminal Procedure." *NYU Law Review* 82 (2007): 112.

———. "'I've Got Nothing to Hide'and Other Misunderstandings of Privacy." *San Diego Law Review* 44 (2007): 745.

———. *The Digital Person*. New York: New York University Press, 2004.

———. "The Virtues of Knowing Less: Justifying Privacy Protections against Disclosure." *Duke Law Journal* 53, no. 3 (2003): 967.

Solove, Daniel, Marc Rotenberg, and Paul Schwartz. *Privacy, Information and Technology*. New York: Aspen Publishers, 2006.

Sony Online Entretainment Press Release. "Sony Online Entretainment Announces Theft of Data from Its Systems," 2011.

Sovern, Jeff. "Opting In, Opting Out, or No Options at All: The Fight for Control of Personal Information." *Washington Law Review* 74 (1999): 1033.

Sozou, Peter. "On Hyperbolic Discounting and Uncertain Hazard Rates." *Proceedings of the Royal Society of Biological Sciences* 265, no. 1409 (1998): 2015.

Spiekermann, Sarah, Jens Grossklags, and Bettina Berendt. "E-Privacy in 2nd Generation E-Commerce: Privacy Preferences versus Actual Behavior." In *Proceedings of the Third Association for Computing Machinery Conference on Electronic Commerce*, edited by Michael Wellman and Yoav Shoham, 38. New York: Association for Computing Machinery Press, 2001.

Steinglass, Matt. “Dutch Cookie Law May Lead to Online Exodus.” *TechHub*, June 21, 2011.

Stigler, George. “An Introduction to Privacy in Economics and Politics.” *Journal of Legal Studies* 9, no. 4 (1980): 623.

Sunstein, Cass. “Acceptance Speech for the Title of Honorary Doctor at Erasmus University Rotterdam.” November 8, 2013.

———. “Believing False Rumors.” In *The Offensive Internet*, edited by Saul Levmore and Martha Nussbaum, 91. Cambridge, Mass.: Harvard University Press, 2010.

———. “Choosing Not to Choose.” Harvard Public Law Working Paper 14-07. Boston, 2014.

———. “Impersonal Default Rules vs. Active Choices vs. Personalized Default Rules: A Triptych.” Harvard Law School Working Paper 13-01. Boston, 2013.

———. *On Rumors. How Falsehoods Spread, Why We Believe Them, What Can Be Done*. New York: Farrar, Straus and Giroux, 2009.

———. “Switching the Default Rule.” *NYU Law Review* 77 (2002): 106.

———. *Why Societies Need Dissent*. Cambridge, Mass.: Harvard University Press, 2003.

Sunstein, Cass, and Richard Thaler. “Libertarian Paternalism Is Not an Oxymoron.” *The University of Chicago Law Review* 70, no. 4 (2003): 1159.

Swire, Peter, and Robert Litan. *None of Your Business: World Data Flows, Electronic Commerce and the European Privacy Directive*. Washington, DC: Brookings Institution Press, 1998.

Tabarrok, Alex, and Tyler Cowen. “The End of Asymmetric Information.” *Cato Unbound*, April 6, 2015.

Tene, Omer, and Jules Polonetsky. “Privacy In The Age Of Big Data: A Time For Big Decision.” *Stanford Law Review Online* 64 (2012): 63.

———. “To Track or ‘Do Not Track’: Advancing Transparency and Individual Control in Online Behavioral Advertising.” *Minnessota Journal of Law, Science & Technology* 13, no. 1 (2012): 281.

Thaler, Richard. “Some Empirical Evidence on Dynamic Inconsistency.” *Economics Letters* 8 (1981): 201.

Thaler, Richard, and Cass Sunstein. “Libertarian Paternalism.” *American Economic Review* 93, no. 2 (2003): 175.

Toulson, Roger, and Charles Phipps. *Confidentiality*. London: Sweet & Maxwell, 2007.

Tsai, Janice, Serge Egelman, Lorrie Faith Cranor, and Alessandro Acquisti. “The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study.” *Information Systems Research* 22, no. 2 (2011): 254.

Turow, Joseph. “Americans and Online Privacy: The System Is Broken.” *The University of Pennsylvania Annenberg Public Policy Center Report*. Philadelphia, 2003.

Turow, Joseph, Lauren Feldman, and Kimberly Meltzer. “Open to Exploitation: American Shoppers Online and Offline.” *The University of Pennsylvania Annenberg Public Policy Center Report*. Philadelphia, 2005.

Turow, Joseph, Jennifer King, Chris Jay Hoofnagle, Amy Bleakley, and Michael Hennessy. “Americans Reject Tailored Advertising and Three Activities That Enable It.” *The University of Pennsylvania Annenberg Public Policy Center Report*. Philadelphia, 2009.

Ur, Blase, Pedro Giovanni Leon, Lorrie Faith Cranor, Richard Shay, and Yang Wang. “Smart, Useful, Scary, Creepy: Perceptions of Online Behavioral Advertising Perceptions of Online Behavioral Advertising.” In *Proceedings of the Symposium On Usable Privacy and Security*. New York: Association for Computing Machinery Press, 2012.

Van Blarkom, GW, John Borking, and Jacobus Olk. *Handbook of Privacy and Privacy-Enhancing Technologies*. The Hague: College bescherming persoonsgegevens, 2003.

Van der Ploeg, Irma. "Keys to Privacy." In *The Machine-Readable Body*, edited by Irma Van der Ploeg, 15. Maastricht: Shaker, 2005.

Van der Sloot, Bart. "Je Geld of Je Gegevens: De Keuze Tussen Privacybescherming En Gratis Internetdiensten." *Nederlands Juristenblad* 86, no. 23 (2011): 1493.

Van Hittersum, Robert. "Dutch Political Parties Violate Their Own Cookie Law." *FleishmanHillard*, June 7, 2012.

Van Hoboken, Joris. *Search Engine Freedom. On the Implications of the Right to Freedom of Expression for the Legal Governance of Web Search Engines*. Alphen aan den Rijn: Kluwer Law International, 2012.

Varian, Hal. "Economic Aspects of Personal Privacy." In *Cyber Policy and Economics in an Internet Age. Topics in Regulatory Economics and Policy Series.*, edited by William Lehr and Lorenzo Pupillo, 127. Norwell: Springer, 2002.

Verkerke, Rip. "Legal Ignorance and Information-Forcing Rules." *William and Mary Law Review* 56 (2015): 833.

Victor, Jacob. "The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy." *Yale Law Journal* 123 (2013): 513.

Viscusi, Kip. "Consumer Behavior and the Safety Effects of Product Safety Regulation." *Journal of Law and Economics* 28, no. 3 (1985): 527.

———. "The Lulling Effect: The Impact of Child-Resistant Packaging on Aspirin and Analgesic Ingestions." *American Economic Review* 74, no. 2 (1984): 324.

Viscusi, Kip, and Wesley Magat. "Informational Regulation of Consumer Health Risks: An Empirical Evaluation of Hazard Warnings." *RAND Journal of Economics* 17, no. 3 (1986): 351.

"Voorstel Voor Ruimere Cookiewet." *NU*, November 21, 2012.

Vos, Freek. "Waar Maakt Iedereen Zich Zo Druk over? Leve de Cookies!" *Volkskrant*, October 17, 2012.

W3C Tracking Protection Working Group. "W3C Last Call Working Draft." *Tracking Preference Expression (DNT)*, April 24, 2014.

Wang, Yang, Pedro Giovanni Leon, Kevin Scott, Xiaoxuan Chen, Alessandro Acquisti, and Lorrie Faith Cranor. "Privacy Nudges for Social Media: An Exploratory Facebook Study." In *Proceedings of the Twenty Second International Conference on World Wide Web Companion*, 763, 2013.

Warman, Matt. "EU Fights 'Fierce Lobbying' to Devise Data Privacy Law." *The Telegraph*, February 9, 2012.

Warren, Samuel, and Louis Brandeis. "The Right to Privacy." *Harvard Law Review* 4, no. 5 (1890): 193.

Wathieu, Luc, and Allan Friedman. "An Empirical Approach to Understanding Privacy Valuation." Harvard Business School Working Paper 07-75. Boston, 2007.

Weber, Bethany, and Gretchen Chapman. "The Combined Effects of Risk and Time on Choice: Does Uncertainty Eliminate the Immediacy Effect? Does Delay Eliminate the Certainty Effect?" *Organizational Behavior and Human Decision Processes* 96, no. 2 (2005): 104.

Weber, Rolf. "The Right to Be Forgotten More Than a Pandora's Box?" *Journal of Intellectual Property, Information Technology and E-Commerce Law* 2 (2011): 120.

Werro, Franz. "The Right to Inform v. the Right to Be Forgotten: A Transatlantic Clash." In *Haftungsbereich Im Dritten Millennium (Liability in the Third Millennium)*, edited by Aurelia Colombi Ciacchi, Christine Godt, Peter Rott, and Lesley Smith, 285. Baden: Nomos, 2009.

"Wetgever Maakt Surfen Onmogelijk." *Financieel Dagblad*, June 11, 2010.

Whitford, William. "The Functions of Disclosure Regulation in Consumer Transactions." *Wisconsin Law Review* 2 (1973): 400.

Whitman, James. "The Two Western Cultures of Privacy: Dignity versus Liberty." *Yale Law Journal* 113, no. 6 (2004): 1151.

Wigmore, John. *Wigmore on Evidence*, 1940.

Willis, Lauren. "When Nudges Fail: Slippery Defaults." *University of Chicago Law Review* 80, no. 3 (2013): 1155.

———. "Why Not Privacy By Default?" *Berkeley Technology Law Journal* 29, no. 1 (2014): 61.

Wolfenden, John. "Report of the Committee on Homosexual Offences and Prostitution." London, 1957.

World Economic Forum. "Personal Data: The Emergence of a New Asset Class. Report for the 'Rethinking Personal Data' Project." Geneva, 2011.

Yan, Jun, Ning Liu, Gang Wang, Wen Zhang, Yun Jiang, and Zheng Chen. "How Much Can Behavioral Targeting Help Online Advertising?" In *Proceedings of the Eighteenth International Conference on World Wide Web*, 261. New York: ACM, 2009.

Zinser, Alexander. "The Safe Harbor Solution: Is It an Effective Mechanism for International Data Transfers Between the United States and the European Union?" *Oklahoma Journal of Law & Technology* 1 (2004): 11.

Zittrain, Jonathan. *The Future of the Internet. And How to Stop It*. New Haven: Yale University Press, 2008.

Zwenne, Gerrit-Jan, and Maxime Verhagen. "Dutch Cookie Law to Affect Businesses Outside Holland." *E-Commerce Law & Policy* 13, no. 17 (2011): 1.

!

Legislation

2005 Act on the specific provisions for the protection of individuals in relation to the processing of personal data in the electronic communications sector (Luxemburg).

Act CVII of 2011 on Communications (Hungary).

Act No. 101/2000 Coll. (Czech Republic).

Act No. 169 (Act on Electronic Communications Networks and Services, Denmark).

Act of 6 January 1978 (France).

Act on Electronic Communications (Slovakia).

Besluit Universele Dienstverlening en Eindgebruikersbelangen (Decision on Universal Services and End-user Interests, The Netherlands).

Data Protection Code (Italy).

Directive 1995/46/EC (EU).

Directive 2000/31/EC (EU).

Directive 2002/58/EC (EU).

Directive 2009/136/EC (EU).

Electronic Communications Act (Belgium).

Electronic Communications Act (Estonia).

Electronic Communications Networks and Services (Ireland).

Electronic Messages Act (Bulgaria).

Henkilötietolaki 1999/523 (Personal Data Act, Finland).

Law 3471/2006 (Greece).

Law 4070/2012 (Greece).

Law 41/2004 (Portugal).

Law 506/2004 (Portugal).

Law 46/2012 (Portugal).

Law 34/2002 (Information Society and Electronic Commerce Law, Spain).

Law on Electronic Communications (Lithuania).

Law on Information Society Services (Latvia).

Legal Notice 239 of 2011 (Malta).

Ordinance 13/2012 (Portugal).

Privacy and Electronic Communications Regulations of the United Kingdom (PECR, UK).

Proposal for a Regulation on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Regulation Proposal, EU).

Regulation of Electronic Communication and Postal Services Law (Cyprus).

Royal Decree 13/2012 (Spain).

Sw. lagen om elektronisk kommunikation 2003:389 (Electronic Communications Act, Sweden).

Telecommunicatiewet (Telecommunications law, The Netherlands).

Telecommunications Act (Austria).

Telecommunications Act (Germany).

Telecommunications Law (Poland).

Zakon o elektroničkim komunikacijama (Electronic Communications Act, Croatia).

ZEKom-1 (Electronic Communications Act, Slovenia).

Cases

Bodil Lindqvist v. Åklagarkammaren i Jönköping, ECJ C-101/01 (2003).

Briscoe v. Reader's Digest Association Inc., 483 P.2d 34 (Cal. 1971).

Deutscher Apothekerverband eV v. DocMorris NV and Jacques Waterval, ECJ C-322/01 (2003).

Ex Parte Jackson, 96 US 727 (1877).

Florida Star v. B.J.F., 491 U.S. 524 (1989).

Fredrik Neij and Peter Sunde Kolmisoppi v. Sweden, ECHR 40397/12 (2013).

Gertz v. Roberts Welch, 418 U.S. 323 (1974).

Google Spain SL and Google Inc. v. AEPD and Mario Costeja González, CJEU C-131/12 (2014).

Home Office v Wainwright, EWCA Civ. 2081 (2001).

Melvin v. Reid, 112 Cal.App. 285, 297 P. 91 (1931).

New York Times Co. v. Sullivan, 376 U.S. 254 (1964).

Piergiorgio Gambelli and Others, ECJ C-243/01 (2003).

Prince Albert v. Strange, 2 De G, & Sm 652 (1859).

Rosenbloom v. Metromedia Inc., 403 U.S. 29, 91 S. Ct. 1811, 29 L. Ed. 2d 296 (1971).

Sindell v. Abbott Laboratories, 26 Cal. 3d 588 (1980).

Time Inc. v. Hill, 385 U.S. 374 (1967).

US v. Antoine Jones, 132 S. Ct. 945 (2012).

US v. Maynard, 615 F.3d 544 (DC Cir. 2010).

Volker und Markus Schecke GbR and *Hartmut Eifert* (joined cases), CJEU C-92/09 and C-93/09 (2010).

Summary

Technological changes, particularly in the context of big data, have made surveillance by public and private parties easier than ever before: they have reduced the costs of gathering, storing and disseminating information. This has been coupled with a decentralization in internet content creation. Together, these changes modify the interactions involving privacy and personal information exchanges and, to that extent, they force us to reconsider the scope of protection that we grant them. This reconsideration has been done from the perspective of human rights, while the economic incentives involved remain underexplored.

In the process of doing this, the thesis evaluates whether data protection law can be justified from an economic perspective. Given that people face privacy costs by disclosing personal information, entitlements created by data protection affect the incentives for generating information in the context of decentralized content creation; hence, these entitlements can lead to greater information production in the long run. Due to this, privacy and access to information are often complementary rights. Determining the efficient protection level for these entitlements, however, becomes complex, as both property rules and liability rules introduce additional problems. An intermediate protection level is hence suggested.

Following this, the thesis gives an explanation of why people sometimes disclose their personal information for low compensations despite the high value that they attach to their privacy, based on the uncertain probability of privacy breaches. This explanation can account for user behavior within a rational-choice framework in a way that fits intuitively with both consumers' demands for transparency and contemporary policy debates on privacy. It also reverses the prevalent behavioral model's policy conclusions and accounts for current trends in data protection law—particularly the right to be forgotten.

The right to be forgotten is then analyzed focusing on its formulation in the General Data Regulation Proposal. The right creates large social costs, mainly by reducing freedom of expression and access to information. Due to its implementation difficulties, it could also introduce a risk-compensation mechanism in which people engage in more risky behavior than before. From this perspective, *Google v. Spain* does not rule on the right to be forgotten but on the liability of search engines; and in doing so, it fails to offer a consistent balance between privacy and freedom of expression.

The second major policy debate analyzed is the limitations placed on online tracking by the Electronic Communications Framework Directive, which changes the default system for tracking to an opt-in. A comparative study of the directive's implementation across member states is presented, with special attention to The Netherlands and the United Kingdom. Drawing from the behavioral economics literature on default rules, policy changes that would avoid the incentive problems present in these regulations are suggested.

The thesis makes the dynamics of the tradeoffs involving privacy more visible; both theoretically and in two of the main policy debates in European data protection law. It offers an explanation for data protection law from an economic perspective and, in doing so, provides a new basis for the evaluation of further data protection measures.

Samenvatting

Dankzij technologische veranderingen, met name in het kader van big data, is het voor publieke en particuliere partijen eenvoudiger dan ooit om toezicht uit te oefenen doordat de kosten voor het verzamelen, opslaan en delen van informatie zijn gedaald. Dit ging gepaard met decentralisatie bij de creatie van internetcontent. Deze combinatie van veranderingen leidt tot een gewijzigde wisselwerking tussen privacy en de uitwisseling van persoonlijke informatie en dwingt ons als zodanig de geboden mate van bescherming inzake deze punten te heroverwegen. Deze heroverweging heeft plaatsgevonden vanuit het perspectief van de mensenrechten, terwijl de economische prikkels die hierbij een rol spelen onderbelicht blijven.

Daarbij wordt in het proefschrift geëvalueerd of de wetgeving inzake gegevensbescherming vanuit een economisch perspectief kan worden gerechtvaardigd. Aangezien mensen privacy inleveren wanneer ze persoonlijke informatie verstrekken, zijn aanspraken voortvloeiend uit het recht op gegevensbescherming van invloed op de prikkels bedoeld om binnen de context van een gedecentraliseerde creatie van content informatie te genereren; mogelijk leiden deze aanspraken op lange termijn dan ook tot een hogere informatieproductie. Hierdoor zijn privacy en toegang tot informatie vaak complementaire rechten. Het wordt evenwel een complexe aangelegenheid om een efficiënt beschermingsniveau voor deze aanspraken te bepalen, aangezien zowel eigendomsregels als aansprakelijkheidsregels bijkomende problemen veroorzaken. Om die reden wordt een gemiddeld beschermingsniveau voorgesteld.

Hierna wordt in het proefschrift een verklaring gegeven voor het feit dat mensen soms in ruil voor een lage tegenprestatie persoonlijke informatie verstrekken hoewel ze veel waarde aan hun privacy hechten, uitgaande van de onzekere waarschijnlijkheid dat er inbreuken op de privacy zullen worden gepleegd. Hierbij wordt het gedrag van gebruikers in het kader van de *rational choice* benadering verklaard op een wijze die intuïtief aansluit bij de roep om transparantie door consumenten en de huidige beleidsdebatten over privacy. Hiermee worden ook de heersende beleidsconclusies over het gedragsmodel onderuitgehaald en de huidige trends op het gebied van wetgeving inzake gegevensbescherming verklaard — met name het recht om te worden vergeten. Vervolgens wordt het recht om te

worden vergeten geanalyseerd, waarbij de formulering van dit recht in het voorstel voor een algemene verordening gegevensbescherming centraal staat. Dit recht brengt hoge maatschappelijke kosten met zich mee, vooral doordat de vrijheid van meningsuiting en de toegang tot informatie worden beperkt. Vanwege de moeilijkheden bij de tenuitvoerlegging ervan kan de verordening ook leiden tot een risico-compensatiemechanisme waarbij mensen riskanter gedrag gaan vertonen dan daarvoor. Vanuit dit perspectief blijkt dat in de zaak *Google v. Spanje* geen uitspraak wordt gedaan over het recht om te worden vergeten maar over de aansprakelijkheid van zoekmachines; dit betekent dat er geen consistent evenwicht wordt geboden tussen privacy en de vrijheid van meningsuiting.

Het tweede belangrijke beleidsdebat dat wordt geanalyseerd, betreft de beperkingen inzake *online tracing* zoals voorzien in de kaderrichtlijn inzake elektronische communicatie, als gevolg waarvan de standaardinstelling voor tracering wordt gewijzigd in een keuze-instelling. Er wordt een vergelijkend onderzoek naar de tenuitvoerlegging van de richtlijn in de lidstaten gepresenteerd, met bijzondere aandacht voor Nederland en het Verenigd Koninkrijk. Uitgaande van wat in de literatuur over gedragseconomie wordt geschreven over standaardregels, worden beleidsveranderingen voorgesteld om de problemen inzake prikkels waarvan in deze verordeningen sprake is, te vermijden.

Het proefschrift maakt de dynamiek van de privacy-afwegingen zichtbaarder, zowel vanuit een theoretisch oogpunt als in twee van de belangrijkste beleidsdebatten over de Europese wetgeving inzake gegevensbescherming. Het biedt een verklaring voor wetgeving inzake gegevensbescherming vanuit een economisch perspectief en biedt daarmee een nieuwe basis voor de evaluatie van verdere maatregelen inzake gegevensbescherming.