Property rights in personal data

Purtova, N.N.

Publication date:
2011

PROPERTY RIGHTS IN PERSONAL DATA:
A EUROPEAN PERSPECTIVE

PROPERTY RIGHTS IN PERSONAL DATA: A EUROPEAN PERSPECTIVE

Proefschrift ter verkrijging van de graad van doctor

aan de Universiteit van Tilburg,

op gezag van de rector magnificus, prof. dr. Ph. Eijlander,

in het openbaar te verdedigen ten overstaan van een

door het college voor promoties aangewezen commissie

in de aula van de Universiteit

op woensdag 16 februari 2011 om 16:15 uur

door

Nadezhda Nickolayevna Purtova

geboren op 11 april 1981 te Yoshkar-Ola, Rusland

Promotores:

Prof. mr. J.E.J. Prins
Prof. dr. P.J.A. de Hert

ISBN 978-90-8891-235-1

Cover design: J.A. Groenendijk
Printed by: Proefschriftmaken.nl || Printyourthesis.com
Published by: Uitgeverij BOXPress, Oisterwijk

Маме и папе с любовью
To my parents with love

Contents:

Chapter 1: Introduction

1. Subject matter, research question and aim of this study

This study considers the familiar idea to introduce property rights in personal data against a backdrop of developments in the modern European concept of property rights and new applications of information technology not yet accounted for in the existing debate. The principal question that this book attempts to answer is whether, from a legal perspective, the propertisation of personal data is a realistic option in Europe in terms of further development of the European approach to data protection. The research question implies the two sub-questions: firstly, to what extent, if at all, is the propertisation of personal data legally possible; and secondly, if, and to the extent that it is possible, what would be the benefits and limitations thereof when it comes to resolving the personal data problem?

This research started off with an assumption, based on European literature on privacy, that the idea of the propertisation of personal data was a Bad Idea. Indeed, in European discourse propertisation was often used interchangeably with commodification both of personal data and a human right to data protection. Hence, the search for a European perspective on the issue began, based on Popper's idea of falsification, as an attempt to refute the hypothesis that propertisation is a good solution to the data protection problem in Europe, by finding evidence of possible harmful effects of propertisation and identifying further arguments against it.

Nevertheless, the results of the research into the concept of property in European law, as well as a closer examination of modern data processing, were convincing enough for the author to take another look at the propertisation debate. As it turned out, the analysis was not able to reject the hypothesis that propertisation *might* be a solution. In Popperian terms, this does not mean that the hypothesis is proven - i.e., that propertisation *should* be introduced. At the same time, the results of this study have strengthened the case for propertisation considerably by its failed attempt at falsification. This study presented propertisation as a legitimate and promising tool in a new generation of data protection which is certainly worth further consideration.

Personal data, at least in the European legal lexicon, is not a conventional object of property rights; the transfer of ownership is not how we usually regard the act of telling people about ourselves. Yet, property talk has entered a policy discourse around personal data. Firstly, regardless of the actual legal circumstances, lively markets in personal data have become a reality. The so-called information industry routinely collects and deals in databases containing the personal details of people as both citizens and consumers, and appear to regard this data as its property.

Moreover, individuals also treat the data pertaining to them as 'their own,' and habitually disclose it in exchange for money, goods, or services.

In the early 1970s, US scholars were the first to propose that personal information should be formally recognized as an object of property rights.[1] Propertisation would acknowledge the existing phenomenon of the commodification of, or the attribution of a high market value to, personal data. It would also return to individuals control over the personal information that had become lost in the course of the Information Revolution.[2] In addition, natural rights theory was also invoked to support property claims for personal information, implying an inherent connection between an individual and the data pertaining to him.[3] Other commentators saw the benefits of propertisation in terms of the rhetorical value of property talks.[4] Nevertheless, one of the most discussed approaches to the protection of personal data as property has come from an economic perspective, especially against the backdrop of the shortcomings that are specific to the US data protection system.

Notably, however, although the American debate on the propertisation of personal data has since passed its peak,[5] in Europe such property talk has only recently extended beyond lay circles.[6] One cannot help but notice the growing attention now paid by European academics and policymakers towards 'privacy by design' as a data protection tool, i.e. technology which increases an individual's control and negotiating powers with regard to the collection and use of his personal data. The idea of property-like control over personal information has also received

---

[1] Alan F. Westin, *Privacy and Freedom* (London, Sydney, Toronto: the Bodley Head, 1967).

[2] E.g. Ibid., p. 7; Daniel J. Solove, "Privacy and Power: Computer Databases and Metaphors for Information Privacy," *Stan. L. R.* 53 (2001)., p. 1428

[3] Ibid., p. 1446 (although Solove does not develop the natural law argument further); Vera Bergelson, "It's Personal, but Is It Mine? Toward Property Rights in Personal Information," *U.C. Davis L. Rev.* 37(2003)., p. 430; Margaret Jane Radin, "Property and Personhood," *Stanford Law Review* 34, no. 5 (1982)., p. 959

[4] "Property talk is just how we talk about matters of great importance" (Lawrence Lessig, "Privacy as Property," *Social Research: An International Quarterly of Social Sciences* 69, no. 1 (2002)., p.247); "If you could get people (in America, at this point in history) to see [a] certain resource as property, then you are 90 percent to your protective goal." (Lessig, "Privacy as Property.")

[5] Indeed, the reader will find only few relevant works after 2004 (e.g. James Rule, *Privacy in Peril: How We Are Sacrificing a Fundamental Right in Exchange for Security and Convenience* (Oxford University Press, 2007)., Lawrence Lessig, *Code 2.0* (New York: Basic Books, 2006)., a new edition of ———, *Code and Other Laws of Cyberspace* (New York: Basic Books, 1999).

[6] Among the few European authors writing about property in personal data are Colette Cuijpers, "A Private Law Approach to Privacy: Mandatory Law Obliged? ," *SCRIPT-ed* 4, no. 4 (2007)., J.E.J. Prins, "Property and Privacy: European Perspectives and the Commodification of Our Identity," in *The Future of the Public Domain, Identifying the Commons in Information Law*, *Information Law Series* (Kluwer Law International, 2006)., Antoinette Rouvroy, Poullet, Yves, "The Right to Information Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy," in *Reinventing Data Protection?*, ed. Serge Gutwirth, et al. (Berlin: Springer, 2009)., Niels Van Dijk, "Property, Privacy and Personhood in a World of Ambient Intelligence," *Ethics Inf Technol* 12 (2009).

renewed attention at the EU level. For instance, in a 14th April 2009 video message, Vivian Reding, the EU Commissioner for Information Society and Media, said that "Europeans must have the right to control how their personal information is used, and […] that the Commission would take action wherever EU Member States failed to ensure that new technologies such as behavioural advertising, RFID 'smart chips' or online social networking respected this right."[7] The property in data is one of the tools at the disposal of the law when it comes to providing individuals with the desired degree of control.[8]

Despite the amount of literature available on propertisation by American authors, and a growing interest in the concept by European scholars, the current debate has three major flaws. Firstly, it lacks structure and a systematic approach. There has been no comprehensive study in either Europe or the US which compares the substance of a personal data problem that propertisation would resolve with an assessment of what property as a legal instrument has on offer. The arguments for or against propertisation mostly focus only on individual aspects of the personal data problem, such as the commodification of personal information, and ignore others, or approach the concept of property one-sidedly, e.g. arguing that propertisation will induce, not limit, (uncontrolled) personal data transfers,[9] whereas a general analysis of the concept of property may show that it is not always the case. As a result, the propertisation debate so far has been displaying selective vision, losing sight of the forest behind the trees.

Secondly, the existing literature on propertisation does not specify which of many possible perspectives on property form the basis of the authors' understanding of this concept. As a result, there is significant disagreement among participants to the discourse on what property is and what effects it has when it comes to personal data. This confusion about the basic assumptions regarding property makes it difficult for the debate to achieve any constructive results.[10]

Finally, new developments in information technology and a resulting new structure of the personal data flow have received virtually no attention in the propertisation discourse in either the US or Europe.

Consequently, the aim of this study is to provide an answer to the research question in a way which tackles the limitations of the existing debate.

---

[7] "Citizens' privacy must become priority in digital age, says EU Commissioner Reding" available online at <http://ec.europa.eu/information_society/newsroom/cf/itemlon>

[8] For recent evaluations and proposals for the improvement of the 1995 Data Protection Directive see, e.g. Neil Robinson, Graux, Hans, Botterman, Maarten, Valeri, Lorenzo, "Review of the European Data Protection Directive: Technical Report Prepared for the Information Commissioner's Office," (Santa Monica: RAND, 2009).

[9] E.g. Jessica Litman, "Information Privacy / Information Property," *Stan. L. R.* 52(2000).

[10] For more on this see Chapter 4

2. Perspective of this study

2.1. Legal perspective

An inquiry into the subject of property rights in personal data may benefit from utilizing a range of auxiliary disciplines such as legal studies, ethics, law and economics, the philosophy of law, legal history and legal sociology. Firstly, the notion of property is at the core of the research at hand, and significant arguments concerning the concept have been made from both economic and philosophical perspectives. Secondly, the economic, ethical and philosophical analyses involve normative standards against which the idea of the propertisation of personal data may be evaluated, such as whether it is just, ethical, effective, and efficient. This way the different perspectives facilitate the making of normative choices that are relevant to propertisation. In addition, although the current research does not focus on revealing any causal connections, it still can benefit from the discipline of the sociology of law, which introduces awareness of the fact that no institution operates in isolation in a social (including a legal) system. Legal history may also be helpful, since the modern institution of property, as well as its effects and rationales, is better understood in light of the historical development of this concept.

These are only a few illustrations of the opportunities and benefits of a multi-disciplinary study on the matter of property in personal data, in which each perspective provides a unique insight. However, how far this study can go is limited by both the time available for the PhD project and the training of the author. Indeed, full-scale sociological, economic, or philosophical research on the topic would probably demand a degree in each discipline and then the writing of a separate dissertation on each matter. Accordingly, the present work will be a study in the area in which the author is trained – the law. By the legal perspective this study means the perspective focused on the system, content and relationship of legal rules and their binding effect. Other non-legal aspects and consequences of propertisation, e.g. from the fields of economics or ethics, are beyond the scope of this book, although certainly worthy topics for other studies.

2.2. European perspective

As well as being a study of the law, this book also approaches the issue of the propertisation of personal data from a European perspective. The European perspective means the perspective of the European Union (EU) and Council of Europe (CoE). Focusing on these two European entities is more promising when it comes to developing a common approach to the central issue of this book. Despite still present and numerous differences between EU member states, they share

significant common interests such as creation of the common market, traditions of regulation and human rights and aspirations, e.g. to guarantee respect for human rights. Crucially, they also share a common policy on data protection expressed, *inter alia*, in: the Council of Europe Convention No. 108 for the protection of individuals with regard to the automatic processing of personal data, adopted by the Council of Europe Committee of Ministers on 28 January 1981 (Convention 108); and the EC Directive on the protection of individuals with regard to the processing of personal data and the free movement thereof (Directive 95/46/EC (OJ L281, 23.11.1995, 31), adopted by the European Parliament and the Council on 24 January 1995 (the 1995 Directive or the Data Protection Directive).

Moreover, both the EU and the Council of Europe have institutions which represent and formulate the common interests of their member states. In certain areas, the EU speaks for the member states as one voice in, for example, negotiations with the US and other non-European states. This latter role is of increasing significance in light of the growing internationalization of data transfers and the data protection debate. Consequently, it is legitimate to conclude that, provided proper account is given to the differences that are still present between the individual member states, defining Europe as the EU and the CoE offers a good chance of developing a coherent approach to the notion of propertisation.

2.3. Perspective of the individual

To maintain the balance between the completeness and feasibility of this research, and given that the research question is, in part, normative, this study will adopt a normative perspective against which the notion of property in personal data will be evaluated. Such a perspective is that of an individual's interests. Namely, the propertisation will be defended because it improves the position of a data subject to exercise control with regard to his/her personal data by creating tools of accountability, monitoring and enforcement of the data protection rights. The perspective of the data subjects' interests distinguishes this study from those on property and personal data that are conducted from the perspective of the intellectual property rights of the organizations constituting the information industry.[11]

[11] Niels Van Dijk, "Intellectual Rights as Obstacles for Transparency in Data Protection," in *Mobile Marketing in the Perspective of Identity, Privacy and Transparency, Future of Identity in the Information Society (Fidis), D.11.12.*, ed. A. Deuker (2009).

3. Theoretical framework

3.1. Legal pragmatism

The answer to the research question is largely influenced by legal pragmatism - the position of the author of this book regarding the law. To explain briefly the essence of this teaching, I borrow from Butler's essay on legal pragmatism where he nicely sums up the main points:[12]

> *Law is contextual: it is rooted in practice and custom, and takes its substance from existing patterns of human conduct and interaction. To an equal degree, law is instrumental, meant to advance the human good of those it serves, hence subject to alteration toward this end. Law so conceived is a set of practical measures for cooperative social life, using signals and sanctions to guide and channel conduct."*

In the context of the present study this mainly means two things. Firstly, 'property' – one of the main legal concepts in the discussion herein – may not only matter in terms of how it is defined by law and legal doctrine, but also as it is understood both in legal practice and non-legal discourse. Both legal and non-legal uses and meanings of property are relevant for a legal pragmatist. For instance, from a purely legal perspective the propertisation of personal data may be a promising alternative to resolving the personal data problem, However, it may also be the case that the symbolic meaning of the term e.g. to a layman, or in national legal discourse, is not the same as the European law approach that is discussed further in Chapter 4. The term 'property' may appear to be so highly loaded with market ideology that its application to objects such as personal data may confuse rather than clarify the situation, resulting in the resistance of national legal elites and, ultimately, the loss of any possible advantages of propertisation, making it impractical. However, this aspect of the legal pragmatism approach requires studies in the sociology or psychology of law. Since this study only concerns the law, it will, therefore, omit the first implication of legal pragmatism and instead focus on the second.

The second implication of legal pragmatism for this study is that the pros and cons of introducing property rights in personal data have to be evaluated against a background of the instrumental nature of property as a legal concept. Legal pragmatism dictates that property rights in personal data should be introduced, if at all, as a *tool* and *practical measure* with which to achieve a particular goal set by society. Naturally, the propertisation of personal data is only justified when it

---

[12] Brian E. Butler, "Legal Pragmatism: Banal or Beneficial as a Jurisprudential Position?," *Essays in Philosophy* 3, no. 2 (2002).

achieves such a goal more completely or better in other respects than the other tools employed for this purpose.

3.2. Evolutionary approach to data protection

As the reader may have already anticipated from the section on legal pragmatism, the vision of property as an instrument to achieve a certain goal will be prominent in the analysis to come. Therefore, another theoretical framework is important for the purposes of this study – the evolutionary approach to data protection legislation. This approach has been adopted in different forms by *inter alia* Bennett,[13] Mayer-Schönberger,[14] and others.[15] The main idea behind it is that policies and legislation in the field of personal data in different countries are bound to go through the same sequential stages of development:

> *Data protection, above and beyond national idiosyncrasies, can be viewed as an informally co-ordinated international process in which nations might be at different stages of legislative development but cannot resist a general evolutionary trend within data-protection norms (especially [N.P. but not only] in Europe).*[16]

Moreover, however advanced the latest personal data regime is, as information technologies and practices move on the public's perceptions of the related problems shift and give rise to the need for policies and legislation of a new, more advanced 'generation'.

While sharing the basic idea of there being a correlation between societal, technological, and data protection developments, the proponents of the evolutionary approach disagree somewhat on the number, exact timing and some of the details of the substantial characteristics of generational systems. Trying to address these disagreements and develop a new consistent taxonomy is unnecessary for the

---

[13] Colin J. Bennett, *Regulating Privacy - Data Protection and Public Policy in Europe and the United States* (1992).

[14] Viktor Mayer-Schőnberger, "Data Protection in Europe," in *Technology and Privacy: The New Landscape*, ed. P.E. Agre, Rotenberg, Marc (The MIT Press, 1997).

[15] See, for instance, Yves Poullet, "The Directive 95/46/EC: Ten Years After," *Computer Law & Security Report* 22 (2006). In his article, Poullet *inter alia* observes the necessity of the emergence of the third generation of data protection coupled with technological developments (p. 215).

[16] In Mayer-Schőnberger, "Data Protection in Europe."; for criticism of the generational interpretation of the evolutionary approach see, e.g. Lee A. Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits*, vol. 10, Information Law Series (Kluwer Law International, 2002). Bygrave distinguishes not generations but 'certain regulatory trends' of data protection. He rejects the generational interpretation as "the analytical utility of employing such fixed chronological categories is diminished by the fact that the trends concerned are often more gradual than the categories indicate. Concomitantly, use of the categories can easily result in ambiguous or misleading generalisations in which distinctions are overstated." (pp. 87-88)

purposes of this research, and it is enough to choose one of the existing classifications as a point of departure. Accordingly, the taxonomy of choice of this study is that developed by Mayer-Schönberger.

Mayer-Schönberger distinguishes four waves of the development of information technology as well as four corresponding generations of concerns and types of data protection legislation. Preceding the first generation was the emergence and spread of mainframe computers in the 1960s. These made the processing of personal data faster, the storage easier, and ensured that the retrieval of information about individuals could be achieved in a matter of seconds. These technological developments, coupled with government initiatives to create centralized, national databanks of their citizens' personal details, gave rise to fears of databases and the possibility that information about an individual could be retrieved instantly, giving governments the tools with which to control society. In brief, the problem was seen to be the very fact of computerized data processing. As a result of this perception, processing itself had to be controlled. Consequently, the first generation of data protection involved the government regulation of databases in form of the organizational rules such as data security, accuracy, secrecy, and source-code integrity. Sometimes, data security was maintained by controlling physical access to a database, and given that there were expected to be only a few databanks, the data protection norms were linked to these. The first generation of data protection did not employ abstract rules or the language of privacy. No individual data protection rights were envisaged. Instead, supervisory authorities ensured the databanks' compliance with data protection standards.[17]

The second generation data protection regime appeared in the 1970s, when technological developments suddenly advanced. Small-sized computers were increasingly available and began to dominate. Consequently, the number of actors processing personal data increased and came to include thousands of private organizations, each of which maintained a database and became impossible to control with the individually targeted technical regulations characteristic of the first generation approach. The response was a shift to individual privacy rights with which citizens could protect their own interests. The right to consent to the processing of one's data, thus, emerged, enabling the individual to decide whether or not to disclose his personal details. However, these data protection rights were only negative and did not extend beyond establishing the control over disclosure.[18]

In the 1980s, when it became clear that participation in modern society was impossible without revealing personal information for processing in databases, the third generation of data protection rules was introduced, whereby an individual's freedom to hold on to his personal data was replaced with a more participatory right

[17] Mayer-Schőnberger, "Data Protection in Europe.", p. 225
[18] Ibid., pp. 227-228

to information self-determination. This implied the existence of positive individual rights beyond non-disclosure, and these equated to having control over one's personal information and a say in each stage of data processing, including collection, use and retention. Individuals were therefore entrusted with the responsibility to exercise information self-determination over their data. Data protection thus relied on private (i.e. via individual complaints) enforcement.[19]

However, since the negotiating powers were unequal between individuals and data collection institutions, the social price for exercising self-determination was too high for many. This meant that very few were actually able to enjoy the right to control and negotiate about the processing of their data. Accordingly, the fourth generation data protection approach came into being. The 1995 EU Directive on data protection is the fruit of this most recent evolutionary move in Europe. Its rationale is the restoration of the balance of power between individuals and data processing actors, and, once this has been achieved, the reliance is yet again on individual participatory rights. As a consequence, fourth generation data protection legislation returned to the method of state regulation employed by the first generation approach, but also retained the individual participatory rights introduced by the third. It is now a mix of individual positive and negative rights and positive and negative obligations of data processing organizations, the latter of which are enforced both privately and by supervisory government agencies. Moreover, as the contexts of data processing became increasingly different, the fourth generation of data protection rules became more sectoral and includes special norms for particular types of information processing.[20]

In 1997, Mayer-Schönberger concluded that the evolution of the approaches to data protection was an ongoing process, and went on to state that "in a couple of years" fifth and sixth generation mechanisms may well emerge.[21] In the year 2011 one cannot help but wonder whether the circumstances concerning data protection have again shifted. Given that the key fourth generation data protection instrument – the 1995 Directive - is still in force and has not undergone any fundamental changes, is there really a need for a fifth generation approach? Technology has certainly moved forward. Radio Frequency Identification Technologies (RFIDs) have enabled the even greater integration of computers into daily life, leading to the possible introduction of ambient intelligence and an internet of things.[22] When implemented, these technologies will operate on the basis of the constant collection and processing

[19] Ibid., pp. 229-232
[20] Ibid., pp. 232-235
[21] Ibid., p. 235
[22] As De Hert defines it, "in a world of [an] "Internet of things," computing is enabled to melt invisibly into the fabric of our […] life. In a world of [an] "Internet of things", it will be easier to establish new relationships, but also to identify people, since all possible everyday objects will be part of a network." see Paul De Hert, "A Right to Identity to Face the Internet of Things?"

of personal information. Social online networks like Facebook or Twitter have also now largely taken over the personal communication task, subverting in popularity personal e-mails or blogs. In these networks people are willingly, and often indiscriminately, sharing personal information with dozens or hundreds of their online 'friends' or even complete strangers. In these circumstances, this book tries to shed some light on whether, legally speaking, property rights in personal data could be part of the future of the European data protection in the face of the recent wave of development of the information technology and practices.

4. Method of functional equivalence

It has already been made clear earlier in this chapter that the idea to tackle concerns vis-à-vis data processing by the means of property rights in personal data emerged across the Atlantic, in the United States. Naturally, the propertisation discourse has, thus, largely been shaped by the US legal system. Although the focus of this book is on the European legal order, much can be learned from US discourse and the original propertisation debate as it unfolded there. Consequently, and also bearing in mind that legal pragmatism is the theoretical background of this book, functional comparative law seems to be the most appropriate research method.

According to the outlines of the approaches to comparative law set out in *The Oxford Handbook of Comparative Law*[23] and *An Introduction to Comparative Law* by Zweigert, Kötz and Weir,[24] the main principle upon which this method relies is that of functional equivalence. This principle, and the validity of the method in general, are based on the assumption that "despite the great differences in their historical development, conceptual structure, and style of operation,"[25] a number of the world's legal systems face, essentially, the same problems. Although the ways to resolve these issues may differ, it is common for divergent means to achieve similar results.[26] For this reason, the different national legal institutions should be considered from the position of the functions they perform, i.e. without reference to the concepts of any national legal system,[27] but from the perspective of a particular

[23] Mathias Reimann, *The Oxford Handbook of Comparative Law*, Reinhard Zimmermann ed. (Oxford University Press, 2006).
[24] Konrad Zweigert, Kötz, Hein, Weir, Tony, *Introduction to Comparative Law* (Oxford [etc.]: Clarendon Press, 1998).
[25] Ibid., p. 40
[26] See, however: "It is true that there are many areas of social life which are impressed by especially strong moral and ethical feelings, rooted in the particularities of the prevailing religion, in historical tradition, in cultural development, or in the character of the people. These factors differ so much from one people to another that one cannot expect the rules which govern such areas of life to be congruent." These areas are "mainly to be found in family law and in the law of succession." (Zweigert et al, *Introduction to Comparative Law*., pp.39-40)
[27] Ibid., p.34

societal need that the legal institution addresses. In adopting such an approach, the same functions of the different legal norms then become criteria for comparison and evaluation. As a result, functionalist comparative law becomes a tool of 'better-law comparison' – "the better of several laws is that which fulfils its function better that the others".[28]

The principle of functionality means that the comparative law method is perfectly suited to the circumstances of this study. Firstly, the functional method makes otherwise incomparable systems and institutions comparable; functionalism overcomes doctrinal discrepancies between divergent legal systems, with different national institutions being reduced to their functions and, as a result, becoming "functionally irrelevant."[29] For the purposes of our research this means that a comparison of the US and Europe, which are otherwise extremely different legal orders, is possible provided that the focus is on the common problem of the protection of personal data and privacy. For the same reason, the facts that, firstly, the US and some European jurisdictions utilize the common law, while the rest of Europe applies continental law, and, secondly, that these countries belong to different legal families, also lose their significance. A functional approach also resolves the problem of different concepts of property, or their equivalents, being applied throughout the jurisdictions compared.

Secondly, a functional equivalence approach considers a particular legal institution as "one [possible, but not necessarily appropriate – N.P.] contingent solution amongst several possibilities."[30] This extends the outlooks of legal scholars beyond the boundaries of their own legal systems to a discovery of alternative solutions to a familiar problem. Accordingly, functionalism widens the choices available to law and policymakers, develops critical attitudes to one's own legal system, and, as a result, provides a sustainable basis for 'better law' political and legislative choices. According to Zweigert, Kötz and Weir, this international focus, which is made possible by the functional approach, is the only instrument enabling the exchange of ideas between jurisdictions, thus making legal studies a true science.[31] This book will benefit from functionalism because its very purpose is to broaden the outlooks of European policy and lawmakers to alternative approaches to data protection. In particular, the focus on the American idea of property rights in personal data will promote a critical attitude to, and accord a fresh look at, European data protection mechanisms and vice versa. Critical thinking and a fresh look at our

---

[28] Reimann, *Oxford Handbook*., p. 342. For the same idea see also Esser, Josef, *Grundsatz und Norm in der richterlichen Rechtsfortbildung* (1956), cited in the Oxford Handbook, p.346 (unfortunately, no English translation is available); Gordley, James, Is Comparative Law a Distinct Discipline? (1998) 46 *AJCL* 607-15

[29] Reimann, *Oxford Handbook*., p. 358

[30] Ibid., p. 358

[31] Zweigert, *Introduction to Comparative Law*., p. 15

own system from a foreign perspective will, ultimately, enable an informed choice to be made as to propertisation of personal data and possible alterations to the system which is already in place in Europe.

The discovery of a 'better law' from a wide range of models is the third benefit of the functional approach to the present study. Indeed, as well as its theoretical-descriptive role revealing "how and why certain legal systems are different or alike",[32] functional comparative law can also be utilized in its 'applied' version which suggests "how a specific problem can most appropriately be solved under the given social and economic circumstances."[33]

5. The key message of this study

The key message this study hopes to convey is that it is impossible to give a simple "yes" or "no," "1" or "0" answer to the questions on the possibility of and need for propertisation. Where a multi-faceted and fluid notion such as property is concerned, one should first reflect on precisely what meaning is being attributed to the concept. From a legal perspective, what matters is not the "property" label but the actual content of the implied rights and their legal effects. The European discussion on propertisation should take into account the many meanings that property has in different forums, both inside and outside the legal debate. In particular, the introduction of property rights in personal data may serve both market and non-market or protective functions. More on this issue will follow in Chapter 4.

Moreover, and consistent with the logic of legal pragmatism and the fluidity of the concept of property, whether property is invoked in its market or non-market form depends on the function that policy-makers choose for it to carry out.

Finally, Europeans should decide on the scope of the rights they would prefer to have with regard to personal data, and then see if they have to describe these in terms of 'property' or not, since it is not the label but the actual content of the rights granted that matters.

6. Structure of the argument

The book is divided into three parts Part I 'sets the stage' for the analysis that follows. Based on the logic of legal pragmatism and perception of property as an instrument to achieve societal goals, Chapters 2 and 3 identify the problem that the propertisation of personal data is intended to tackle. The substance of that problem is defined as a combination of developments and concerns with regard to personal

[32] Ibid., p. 11
[33] Ibid.

data. Special attention is paid to recent developments in information technology and practices and the resulting complex structure of the modern data flow (Chapter 2). Since these advances put current data protection mechanisms under ever more pressure, the need to deal with these new challenges, possibly, by introducing a new generation of data protection tools is discussed in Chapter 3.

Chapter 4 is an introduction to the wider property debate. It contains some basic statements concerning property in general that are vital for the further analysis of the idea of property in personal data. Simultaneously, the chapter reveals that among the numerous possible outlooks on property, the legal perspective has its own distinct meaning which is the basis of this study's approach. The chapter also addresses some of the reservations and concerns regarding the propertisation of a novel object such as personal data, particularly given the seeming impossibility of extending property rights beyond the traditional borders to include such an unconventional object of property rights. Finally, the principle of market alienability as an allegedly inevitable aspect of propertisation is also considered and rejected.

The goal of Part II is to look back at the original US propertisation debate and learn the lessons that are appropriate for a European reader. In particular, the aim of Chapter 5 is to prepare the ground for the European reader to see the idea of the propertisation of personal data as a logical development in the interplay of various factors, including the state of US information privacy law and the *conceptualis*ation of the personal data problem. Chapter 6, in turn, contains an outline of the most common arguments for and against the concept of property in personal data, with the purpose being to make the reader aware of the variety of perspectives in existence, with each being defended from a different standpoint, bearing a different, often non-legal, meaning and performing a different function.

Part III is devoted to developing a European perspective on property rights in personal data. It begins in Chapter 7 with an analysis of how the current European approach to data protection copes with the new complexities of the modern data flow and whether there is any room for improvement. The chapter concludes that although the normative choices embodied in the substantive principles of data protection are still valid, their implementation is not without flaws. In other words, the system of accountability, monitoring and enforcement is not achieving its goals.

Part III further includes the analysis of the possibility of propertisation in the EU legal order under the 1995 Directive (Chapter 8) and the permitted scope of property rights under Article 8 ECHR (Chapter 9). Particularly in view of the flexible content of property rights, which can be adapted to achieve goals of a policy-maker, and given that the formal use of the actual term "property" is not vital, Chapter 8 concludes that nothing in the Directive prevents the – limited – propertisation of personal data, whether formally or informally, at least as long as the principle of information self-determination remains. Chapter 9 concludes that ECHR

jurisprudence on the waiver of rights imposes a limit on the alienation of personal data and also on the market side of propertisation.

Chapter 10 completes the European perspective on the idea of property rights in personal data. After reaching conclusions on the possibility of the propertisation of personal information in the European legal order, the chapter examines the potential that the introduction of property rights in personal data has and some limitations thereof, when it comes to making a positive difference in addressing the personal data problem in the modern flow of personal data. The conclusion is reached that the key to using property rights to create a better system of accountability, compliance, monitoring and enforcement lies in their *erga omnes* effect.

Part I: Setting the Stage

Chapter 2: The personal data problem: the developments raising personal data related issues

1. Introduction

According to the logic of functional equivalence, "despite the great differences in their historical development, conceptual structure, and style of operation,"[34] a variety of the world's legal systems have to deal with essentially the same problems, albeit they cope with them in different ways. Simultaneously, the evolutionary approach to data protection assumes that the content of data protection legislation has been always tied to how people regard the issue.[35] It, therefore, comes as no surprise that the question of the substance of the personal data problem appears to be central in the literature that is proposing new ways to deal with personal data processing. The purpose of this study is to examine property rights as a possible tool with which to tackle the personal data problem in Europe. Accordingly, it is only logical to begin the analysis of the idea of propertisation with a description of the problem.

The choice of terminology is important. Labelling the issue in question as 'a data protection problem' will, unavoidably, have normative implications; it will mean that 'protecting data' in itself is the goal of personal data related policies, whereas the exact targets of data protection are yet to be established in this and the next chapter. The preference, therefore, is to use as neutral a term as possible. As a consequence, for the purposes of this study and to avoid the probable normative implications, the problem at hand will be referred to as a data processing problem, or, alternatively, as a personal data problem – with both terms broadly referring to the subject that is being regulated, i.e. personal data and anything done with it.

The personal data problem should be understood as a combination of developments and concerns with regard to personal information. This chapter provides an overview of the relevant developments. Chapter 3 reviews the concerns and offers the analysis thereof, based on the current public and academic debate in Europe and the United States.

The relevant developments can be provisionally grouped into the technological, institutional, market (or market-related) and societal, and will be addressed in this order. The analysis will also touch upon the developments that have occurred in the overall structure of personal data flow and are characteristic of the 2000s. This overview of the personal data related developments is provisional because – although the categories in question are quite distinct – it is sometimes

---

[34] Zweigert, *Introduction to Comparative Law*., p. 40

[35] Mayer-Schőnberger, "Data Protection in Europe."

difficult to draw a clear line between them. In any event, a precise classification is not important for the goal that is set for this chapter; a rough overview of personal data related developments will be enough to give an impression of what processes there have been in the field in light of the evolutionary approach to data protection described in the introductory chapter.

2. Developments

2.1. General technological developments

By the term 'technological developments,' this study means advances in the field of Information Technology, both hardware and software, as well as in other types of technology that are related in some way to personal data. When writing about technology as a defining factor of the personal data problem, it would be wrong to explain the latter solely by reference to the former. The relationship between the thirst for personal data and the development of technology is a two-way street.[36] Robins and Webster, for instance, point out that new forms of the functioning of public and private organisations, which - among other factors - cause appetite for information, are not led by technology; they could exist just as well within the non-technological context of human mega-machines, e.g. an army.[37] On the other hand, the two – the technology and a demand in personal data - could not have achieved their present scale if they were not interlinked. For instance, it is easy to agree with a connection that Regan makes between the US government's record keeping and the history of IBM.[38] The system of punch cards introduced by Herman Hollerith for the 1890 census in the United States evolved into the multi-billion corporation that IBM is now.[39] The government was won over by the speed at which the punching machine processed data, and even more so by the mainframe computers in the 1960s. Computerization brought data collection by government agencies to an entirely new level, making it easier to manage, match and exchange data, as well as "retain records over a long period of time and … retrieve a particular record from a large system of records."[40] IBM was, however, too dependent on state purchases; given the high price of their machines only a major client could afford them. Moreover, the company almost certainly lobbied its interests in order to receive new government

[36] Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits*., p. 97
[37] Kevin Robins, Webster, Frank, "History of the Inforation Revolution," in *The Information Society Reader*, ed. Raimo Blom Frank Webster, Erkki karvonen, Harri Melin, Kaarle Nordenstreng, Ensio Puoskari (London and New York: Routledge, 2004).
[38] Priscilla Regan, *Legislating Privacy: Technology, Social Values, and Public Policy* (The University of North Carolina Press, 1995)., pp. 69-70
[39] Ibid.
[40] Ibid.

contracts, as well as making sure that the machines the government actually did purchase were only compatible with IBM software.[41] The same co-dependence can be seen now, half-a-century later, between the government and the corporations developing, for example, new biometric identification and location tracking systems, along with other empowering technologies.

An important advance in hardware development, which has made information technology accessible to, and usable by, actors from outside government agencies, is miniaturization. A comparison between the first mainframe computers, which could easily fill a room, and a modern 'smart phone' that fits into the palm of a hand, speaks for itself. Smaller and better saleable computers are also cheaper and, therefore, more affordable, not only by private corporations, but also by private households and individual users. First, hospitals, schools, banks and similar organizations were able to computerize their records, leading to the emergence of medical, educational, financial and other computer databanks. Now individual users are equipped with mobile devices, meaning that they are able to use online services 'on the go,' make themselves constantly available for communication, and otherwise receive and share information. Increasing miniaturization and the ubiquity of such technology have been characteristic of the developments in hardware up to the present day, making it possible to 'implant' a small computer chip in almost everything from a mobile phone to a teddy bear.[42] Miniaturization also enables a vision of embedded intelligence to come to life. Indeed, the viability of embedded intelligence and the Internet of Things will depend on computers[43] to shrink in size in order to be placed in every object around us that is connected to a network of other intercommunicating objects.[44]

The operation of computers on such a small scale (from virtually every household to, possibly, almost every object) means that a wider range of, among others, personal data[45] will be available for collection, and will not require questionnaires to be filled in first. Instead, simply keeping records of activities performed on a computer is sufficient. Developments in other fields of technology such as biometrics have also enabled greater penetration by technology and data processing of our private lives.

Linked to miniaturization and the increasing private use of information technology, is a truly critical development in the field of personal data - the

---

[41] Robins, "History of the Inforation Revolution."

[42] E.g. the iTeddy idea "Combining stable play patterns with modern technology to create interactive techno-toys for the 21st century child, promoting passive learning through play" <http://www.iteddy.com/home.aspx>

[43] The word 'computer' is used here in the widest sense of the word.

[44] David Wright, Gutwirth, Serge, Friedewald, Michael, de Hert, Paul, Langheinrich, Marc, Moscibroda, Anna, "Privacy, Trust and Policy-Making: Challenges and Responses," *Computer Law and Security Review* 25 (2009): 70.

[45] The Internet of Things does not always require the data be personalized.

emergence of and the proliferation of the Internet, a "global system of interconnected computer networks."[46] Originally developed in the 1960s as a military project, this system became commercialized as a global network in the mid 1990s.[47] With a personal computer in virtually every household in the United States and Europe, an estimated quarter of the Earth's population now uses the World Wide Web and services such as: electronic mail and online instant messaging systems; file transfers and sharing; online gaming; Voice over Internet Protocol (VoIP) person-to-person communication via sound and video; online social networking sites; news portals; and online shops.[48]

Due to the architecture of the Internet, Daniel Solove has described it as "the hub of [the] personal information market."[49] Firstly, the Internet is an effective tool with which to aggregate and consolidate information. Due to the enormous data storage capacities available, little on the Internet takes place without leaving a trace of information behind. Even when the information is deleted or altered, it never really disappears. Secondly, the Internet eliminates the difficulties caused by the physical distances previously associated with communicating information. As a result, records that were once scattered across wide-ranging territories can now be accessed from anywhere in the world. This has made the peddling and purchasing of data much easier.

The most characteristic feature of cyberspace, according to Solove, is the non-static, or interactive, nature of web-pages, which has created a revolution for the targeted marketing industry.[50] This non-static nature of a web-page enables the collection of both more and a wider range of data pertaining to identifiable individuals, including civil identity information.[51]As Leenes explains, most of the content of the Internet is provided by corporations with commercial interests, and represents a business model based on advertising. Following the law of targeted marketing, for instance, and in the case of the Google search engine, the more personalized advertisements that Google presents to a visitor, the greater the likelihood that one of them will be clicked on. Accordingly, a search engine provider (among other service and content providers on the Internet) needs to know who its users are.[52] This is achieved in three ways, the first of which is managed by requiring a user to establish a personal account with a log-in and a password, which is often linked to his or her civil identity. This is certainly the case with online shops where,

---

[46] "Internet" at <http://en.wikipedia.org/wiki/Internet>

[47] History of the World Wide Web on the website of the World Wide Web Consortium (W3C) <http://www.w3.org/History.html>

[48] "Internet" at <http://en.wikipedia.org/wiki/Internet>

[49] Solove, "Privacy and Power: Computer Databases and Metaphors for Information Privacy.", p. 1409

[50] Ibid., p. 1410

[51] Ibid., p. *1411*; Ronald Leenes, "Do You Know Me? Decomposing Identifiability," *TILT Law & Technology Working Paper Series*, no. 006/2008 (2008).

[52] Ibid., p. 6

to place an order, a customer has to reveal his name, payment details (credit card or bank account number), as well as a shipping address. The second and third means of identification are cookies and IP addresses.

A cookie is a small file that is stored in the user's web browser when he visits a search engine (or another online service) for the first time containing the address of the cookie provider.[53] Additional cookies may contain data on, e.g. the last time the user visited a web-site or his language preferences. Cookies are read by the service provider every time the user visits the website, and the search engine or web-shop then knows that it has been visited by this user before. In addition, cookies can also be used to link information about a current visit to data pertaining to previous interactions with the website.[54] When it comes to IP (Internet Protocol) addresses, these are assigned to an individual computer when it connects to the Internet and are stored by search engines along with the queries made.[55]

The existence of the Internet has introduced a new type of personal data known as clickstream, which is a record of what a computer's user clicks on while browsing the Internet or using another software application. Any action is logged and may then be retrieved and used for personalization purposes.[56] It is here where the implications of the profiling and data mining techniques become clear. Similar to the case of data markets described further on,[57] in the scenario of personalized services, enhanced knowledge about consumers is vital for a successful business. By virtue of its architecture, the Internet provides a great deal of data about consumer behaviour. The techniques of profiling and data mining arguably are able to transfer the 'noise' of ever-expanding amounts of generated data into actual knowledge of what the consumer wants.[58]

Another Internet-related development that is relevant to the personal data problem is the phenomenon of cloud computing. The term refers to a body of web-based - as opposed to on-premises - services, such as providing storage capacity and applications for customer, healthcare records, and employee database management.[59] Cloud computing is often presented to businesses as a cheaper way of delivering IT services; instead of maintaining the expensive, complete IT infrastructure that is required for the on-premises execution of relevant information processes, customers

---

[53] Ibid., p. 7

[54] Ibid.

[55] Ibid.

[56] For more on the use of clickstream data see Wendy W. Moe and Peter S. Fader, "Capturing Evolving Visit Behavior in Clickstream Data," *Journal of Interactive Marketing* May (2003). For the privacy implications of the use of clickstream data see Tal Z. Zarsky, "Desparately Seeking Solutions: Using Implementation-Based Solutions for the Troubles of Information Privacy in the Age of Data Mining and the Internet Society," *Maine Law Review* 56, no. 1 (2004).

[57] Section 2.4.

[58] More on profiling and data mining will follow in section 2.2.

[59] For more details on cloud computing see, e.g. Richard Martin, J., Hoover, Nicholas, "Guide to Cloud Computing," in *Information Week: the business value of technology* (2008).

of cloud computing vendors[60] pay only for the services they consume. Cloud computing is also widely available for private use. Examples include web-based email services, photo storage, online backup and file transfer services such as YouSendIt, online medical record storage such as Microsoft's HealthVault, and applications associated with social networking sites.[61] Yet when customers store their data with a vendor's hardware, they lose both sight of it and a large element of control over the fate of that data, including its protection from hacker attacks and transfers to the marketing industry and government agencies.[62]

Technology continues to develop as we speak, providing opportunities to constantly be online and alternatives to staying at home behind a computer. In particular, media-centric cell phones have become popular, not only allowing easy access to the Internet and the technology to take photos and make videos, but "accelerating humanity toward this vision of 'augmented reality,' where data from the network overlays your view of the real world."[63] Although not yet being marketed, the technology is already there to retrieve information about objects and people around you by simply holding up a cell phone and using a camera.

2.2. Profiling

Profiling is a process of creating and applying profiles, a sort of 'portraits' which are used to characterize an individual, a demographic group, a marketing segment, or any other group of individuals formed by any other criterion. A profile does not merely describe an individual or a group, but also predicts their behaviour based upon what is typical for the individual or group in question. Profiling is not a completely new phenomenon and is not exclusive to information technologies. Hildebrandt refers to a successful application of forensic profiling long before the first computer was created.[64] This study, however, focuses only on automated

---

[60] Vendors of cloud computing services include Amazon Web Services, Google App Engine, Salesforce, etc.

[61] PrivacyRightsClearinghouse, "The Privacy Implications of Cloud Computing ".

[62] The personal data related concerns resulting from cloud computing will be addressed in more detail later on in this chapter. Meanwhile, see e.g. Ann Cavoukian, "Privacy in the Clouds - a White Paper on Privacy and Digital Identity: Implications for the Internet " (Information and Privacy Commissioner of Ontario, 2008).; Robert Gellman, "Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing," (The World Privacy Forum, 2009).

[63] Brian X. Chen, "If You're Not Seeing Data, You're Not Seeing," *Wired*, no. August 25, 2009 (2009), http://www.wired.com/gadgetlab/tag/augmented-reality/.; A video of the Augmented Reality technology Application for iPhone < http://www.youtube.com/watch?v=5M-oAmBDcZk >

[64] Mireille Hildebrandt, "Defining Profiling: A New Type of Knowledge?," in *Profiling the European Citizen: Cross-Disciplinary Perspectives*, ed. Mireille Hildebrandt, Gutwirth, Serge (Dordrecht: Springer, 2008).

profiling, which is a product of data mining,[65] a process "by which large databases are mined by means of algorithms for patterns of correlations between data. These correlations indicate relation[s] between data, without establishing causes or reasons. /…/ [Profiling by means of data mining will] provide prediction, based on past behaviour."[66] Profiling may be both direct and indirect. The former occurs when a profile is applied to an individual based on data concerning his own past behaviour, while the latter, in contrast, relies on the past behaviour of others[67] being applied to an individual – the object of the profiling – and is based on one or several characteristics that the individual in question shares with the group. To illustrate how automated direct and indirect profiling works in practice, both Leenes and Zarsky have used an example of an online shop.[68] Zarsky's illustration offers up two scenarios: scenario A is when a male customer, Mr A, from a particular area, enters an online shoe shop searching for a present for his wife. He browses through the content of the site quickly and, having little idea of the price-quality relationship with regard to shoes, buys some low quality footwear for a price that is higher than what is reasonable. A log of his behaviour is kept and a consumer profile is made which describes him as falling into a category of male professionals, probably with high income, who have little free time, do not search for bargains and have little knowledge about shoes. The next time he logs in, the web-shop recognizes a cookie it has inserted in Mr A's browser, identifies him as a returning customer and does not advertise any special offers, maintaining in plain view only expensive shoes of poor quality. This is an example of direct profiling. Scenario B, on the other hand, concerns another male, Mr B, who lives in the same area as Mr A and visits the same web-shop for the first time. Based on his IP-address (linked to the ZIP code), the shop's server recognizes Mr B as a customer living in the same locale as Mr A (since Mr A gave his home address as his shipping address) and automatically puts him in the same category of male professionals who have little free time, do not search for bargains and have limited knowledge of shoes. This occurs because data mining algorithms employed by the web-shop's market research department linked Mr. B's place of residence to this particular marketing segment.[69] Accordingly, as the example of Mr

---

[65] Ibid. Mireille Hildebrandt, Gutwirth, Serge, ed. *Profiling the European Citizen: Cross-Disciplinary Perspectives* (Dordrecht: Springer,2008).

[66] Hildebrandt, "Defining Profiling: A New Type of Knowledge?.", ———, ed. *Profiling the European Citizen: Cross-Disciplinary Perspectives*.

[67] Thierry Nabeth, "Reply: Further Implications?," in *Profiling the European Citizen: Cross-Disciplinary Perspectives*, ed. Mireille Hildebrandt, Gutwirth, Serge (Dordrecht: Springer, 2008)., p. 40

[68] Leenes, "Do You Know Me? Decomposing Identifiability." Zarsky, "Desparately Seeking Solutions: Using Implementation-Based Solutions for the Troubles of Information Privacy in the Age of Data Mining and the Internet Society."

[69] Zarsky, "Desparately Seeking Solutions: Using Implementation-Based Solutions for the Troubles of Information Privacy in the Age of Data Mining and the Internet Society."; for more examples of profiling in marketing see Charles W. Lamb, Hair, Joseph F. Jr., McDaniel, Carl *Marketing*, 10 ed.

A and Mr B demonstrates, the application of profiles is not always accurate or fair. These and other concerns associated with profiling are addressed later in this chapter.[70]

2.3. Institutional developments

By institutional developments this study means developments that are related to the operation of both public and private organizations. The main such advance, which raises a great number of personal data related issues, is the ever growing reliance of both public and private organizations on information about individuals, whether they be citizens, customers, or consumers. Let us look at the public bodies first. One cannot overestimate the role that a modern state, as the largest public organization around, has been playing with regard to our personal data. Although record-keeping by public institutions has been very common throughout the centuries, before the modern state came into existence these records were very unsystematic and limited, both in their purpose and the way they were built.[71] More centralized and complex public record-keeping systems have only emerged over the last 300 years, a period in which state power and functions have expanded[72] from the mere extraction of domestic revenue to top-down governance. These developments were coupled with the emergence of a state bureaucracy.[73] Eventually, the state developed 'infrastructural powers',[74] namely "the capacity to actually penetrate civil society and implement political decisions throughout the realm."[75] With the industrialization of society, the state-citizen relationship has taken on the shape of mutual

---

(South Western Educational Publishing, 2008). P. 240 (chart of profiles based on age and marital status)

[70] See section 3 on Concerns.

[71] Bennett, *Regulating Privacy - Data Protection and Public Policy in Europe and the United States*., p. 18; Robert Ellis Smith, Ben Franklin's Web Site: Privacy and Curiosity from Plymouth Rock to the Internet 12 (2000) referred to in Solove, "Privacy and Power: Computer Databases and Metaphors for Information Privacy.", p. 1400; *Records, Computers, and the Rights of the Citizens*, p. 2

[72] Bennett, *Regulating Privacy - Data Protection and Public Policy in Europe and the United States*., p. 18

[73] Charles Tilly, *Coercion, Capital, and European States, Ad 990-1990.* (Oxford: Blackwell Publishers, 1998)., p. 75; this is how the theorists of state formation describe this process: Initially, the preparation for interstate wars resulted in the necessity to extract domestic revenue (Anthony Giddens, *The Nation-State and Violence* (Berkeley: University of California Press, 1985)., p. 311). Effective tax collection and the conquest of new territories required expanded and well-organized state administration which eventually materialized into "a modern bureaucracy: courts, treasuries, tax systems, regional administrations, and public assemblies." (Tilly, *Coercion, Capital, and European States, Ad 990-1990.*, p. 75)

[74] Simultaneously with a gradual loss of state *despotic powers*, i.e. "the range of actions the state elite is empowered to undertake without routine, institutionalized negotiations with civil society groups." (Joel Migdal, *Strong Societies and Weak States. State-Society Relations and State Capabilities in the Third World* (Princeton, NJ: Princeton University Press, 1988)., p. 5)

[75] Tilly, *Coercion, Capital, and European States, Ad 990-1990.*, p. 75.

responsibilities. For instance, as Westin and Baker summarize, since the 1930s, 40s and 50s, the state administration in the United States has become more regulation-, licensing-, and entitlement-orientated.[76] In Europe, too, regulation and, since compulsory social insurance was introduced in Germany in 1883, the welfare state have played a prominent role in the modernization of society.[77] Examples of welfare state policies include unemployment and child support benefits, as well as public healthcare and education. Although the reach of welfare policies differs from state to state, it is common in both Europe and the United States to have at least a basic safety net maintained by a government in order to take care of its weak and disadvantaged. The European Union plays an increasingly important part in forming more uniform social policies.[78]

The effective performance of the tasks referred to above requires a state to have at least minimal knowledge of the situation it aims to tackle – and this knowledge is often drawn from various kinds of personal data. For instance, fighting crime is more successful when law-enforcement officials have some information about the individuals with a criminal record, which is contained in police databases with names, photographs, details of committed offences, fingerprints and, more recently, DNA. Likewise, the execution of an unemployment benefit programme is not possible without information about individuals in need of this help, such as their name, address, bank account number, and, depending on the kind of benefit, some data about their financial and family circumstances, and employment prospects, etc. Such data are used both to assess the position of an applicant with regard to the eligibility to receive benefits, as well as to identify him or her in order to execute transfers. As Garrett observes in the context of the UK, "[s]ocial work […] from its inception has endeavoured to maximize information on 'clients', to sift that information and to classify, divide and demarcate these 'clients' into particular groups and categories. […] [For instance, the] history of the Charity Organization Society (COS) reveal[s] how its leaders tried to construct giant […] filing cabinets on the 'deserving' and 'undeserving' population of neighbourhoods."[79] These are only a few examples of how a government obtains the personal data of its citizens. On a more general level, Alan Westin classifies government records into three distinct

---

[76] Westin & Baker, Databanks in a Free society: Computers, Record-keeping, and Privacy (1972), at 220-23

[77] Maurizio; Rhodes Ferrera, Martin "Recasting European Welfare States: An Introduction," *West European Politics* 23, no. 2 (2000).

[78] See, for instance, an overview of EU activities in Employment, Social Policy, Health and Consumer Affairs for the year 2009 at <
http://www.consilium.europa.eu/App/NewsRoom/loadBook.aspx?id=351&lang=1&bid=79&infotarget=&target=>

[79] Paul Michael Garret, "Social Work's 'Electronic Turn': Notes on the Deployment of Information and Communication Technologies in Social Work with Children and Families," *Critical Social Policy* 25, no. 4 (2005)., p. 535

categories depending on their purpose and manner of collection: (1) administrative records, generated as a result of some sort of 'transaction', like a birth or marriage, and from personal data which is self-reported or gathered openly; (2) intelligence records drawn from administrative records or compiled on the basis of the testimony of informants and the observations of investigators; and (3) statistical records based on data gathered as a result of a survey. The more numerous and complex state policies become, the more information about its citizens that a government needs.[80] This is the development that Daniel Solove characterized as "an insatiable thirst for information about individuals."[81]

This thirst for information, both in Europe and the United States, is partially rooted in New Public Management (NPM) – a relatively new ideology of public administration dating back to the 1980s. Customer-orientated and striving, among other things, for budget cuts, the decentralization of decision-making, accountability for performance, performance auditing, and privatization,[82] NPM served as the ideological basis for the greater use of information technology, e.g. from case management and the transition of public services, to one-stop-shops which provide many services in one place. The one-stop shop initiative that has been enabled by the Internet is commonly referred to as e-government[83] and is an instance of the NPM. To cite the EU website, "e-government is the use of Information & Communication Technologies (ICTs) to make public administrations more efficient and effective, promoting growth by cutting red tape."[84] Individuals can upload on-line the personal data that is necessary for interaction with the government on e-government web-sites, these data including social security,- driver's licence,- passport- and bank account numbers, and medical and tax data.[85]

What is more, the e-government initiatives are also taken with a view to enhancing the transparency of government operations and decision-making, as well as e-democracy.[86] On the EU level, several projects have been funded to achieve these

---

[80] Ibid.

[81] Solove, "Privacy and Power: Computer Databases and Metaphors for Information Privacy.", p. 1401

[82] Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits*., p. 99. For more on New Public Management see G. Gruening, "Origin and Theoretical Basis of New Public Management," *International Public Management Journal* 4 (2001).

[83] One of the recent examples of the one-stop shop created by use of information technology is the Personal Internet Page (PIP) initiative of the Dutch government: "MijnOverheid.nl is the internet page where after logging in with [a] personal social service number an individual can arrange government-related matters, check her personal data in an easy and safe way." (translated from Dutch into English by the author, see http://www.e-overheid.nl/sites/pip/). For a similar initiative in the US, see <http://www.usa.gov/Citizen/Services.shtml> the Get It Done Online page

[84] < http://ec.europa.eu/information_society/tl/soccul/egov/index_en.htm >

[85] J.E.J. Prins, "E-Overheid: Evolutie of Revolutie?," *Nederlands Juristenblad* 76, no. 11 (2001).

[86] Kuno Schedler and Isabella Proeller, "The New Public Management: A Perspective from Mainland Europe," in *New Public Management: Current Trends and Future Prospects*, ed. Stephen P Osborne Kathleen McLaughlin, and Ewan Ferlie (Routledge, 2001). 165

goals, e.g. the EuroPetition project,[87] the VOICE project which enables "ordinary people to find out about and understand EU laws, procedures and debates, [… and to] have a say in how policy is decided,"[88] and the VEP "The Virtual European Parliament," which creates "a virtual European Parliament in which young citizens can participate via mobiles and Web 2.0 technologies and tools."[89]

As well as the growth in the amount of personal data held by various types of organizations, another feature of institutional life in Europe and the United States is the integration of these data into centralized data banks. In the early stages of this development in the US during the 1960s, there were proposals to establish centralized population registers. There were also plans by several European governments to conduct a national population census in and around the 1970s. The European initiatives were accompanied by an attempt to introduce common criteria (e.g. multi-purpose personal identification numbers (PINs)) for the quick referencing of stored data.[90] Both in the United States and Europe, the initiatives to create all-inclusive public sector data banks did not receive public support. However, smaller – compared to the originally proposed - government databases have been created, also using a national identifier, e.g. a social security number in the United States, a Burgerservicenummer (BSN)[91] in the Netherlands, and the INSEE code in France, which is used as a social insurance number and a national identification number for the purposes of taxation and employment, etc.[92]

The state function of ensuring national security took a new twist in relation to personal information after the September 11th 2001 attacks in the United States, the Madrid July 2004 train bombings, and the 7th July 2005 London suicide attacks on public transport. The US government and the governments of a number of European countries regarded this ever so real terrorist threat and the interests of national security as a justifiable reason for taking (albeit controversial) measures affecting personal data. The US Congress passed the USA Patriot Act, which was widely criticised for threatening "fundamental freedoms by giving the government the

---

[87] Aimed at "coordinating and submitting a pan-EU petition involving over 4.9 million citizens." (<http://ec.europa.eu/information_society/activities/egovernment/implementation/prep_action/index_en.htm >)

[88] < http://ec.europa.eu/information_society/apps/projects/factsheet/index.cfm?project_ref=EP-07-01-034 >

[89] < VEP 'The Virtual European Parliament': creates a virtual European Parliament in which young citizens can participate via mobiles and web2.0 technologies and tools. >

[90] Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits*., p. 94

[91] Citizen's Service Number

[92] According to the results of a study described in Benoit Otjacques, Hitzelberger, Patrik, Feltz, Ferdant, "Interoperability of E-Government Information Systems: Issues of Identification and Data Sharing," *Journal of Management Information Systems* 23, no. 4 (2007)., in part, with an eye to ensuring the interoperability of the e-government information systems, there is a tendency in the European Union "towards acceptance of single, multipurpose identifiers. […] Germany is now the only country of the 15 original EU members that does not have and does not want to install a single identifier in the future. Hungary, a new member, shares this attitude." (p. 48)

power to access to your medical records, tax records, information about the books you buy or borrow without probable cause, and the power to break into your home and conduct secret searches without telling you for weeks, months, or indefinitely."[93] In the UK, the Anti-Terrorism, Crime and Security Act 2001 was passed as a part of a series of anti-terrorism legislation, with Parts III (Disclosure of Information) and XI (Retention of communications data) being of special relevance for the field of personal data. Another implication of the developments in the national security arena is that the private sector becomes an agent of the state.[94] This is well-illustrated by the recent EU-US debate concerning the obtaining of Passenger Name Record (PNR) data from airlines and details of bank transfers via SWIFT (the Society for Worldwide Interbank Financial Telecommunication).[95]

The anti-terrorism and security measures introduced after 9/11, though outstanding in their nature, are only one part of a recent and more general trend seen in the last 20 years for a modern state to pursue absolute public safety, eliminate fear, and prevent damage and anti-social behaviour.[96] Steps taken towards this goal include street and indoor video surveillance, traffic cameras with the functions of number-plate and face recognition,[97] and youth file programmes aimed at the prevention of child abuse and youth anti-social behaviour. As an illustration, in the autumn of 2003, in the Green Paper, Every Child Matters, the UK government published a plan to introduce local databases containing "a list of all children living in the area" as well as other "basic details," the latter of which would include not only a child's name, address and details on parents, carers and education, but also data about "any cause of concern in relation to a child."[98] Such tagging was proposed "for preventive purposes, without the consent of the child or their carers. We [the government] would also welcome views on whether warning signs should reflect factors within the family such as imprisonment, domestic violence, mental health or substance misuse problems amongst parents and carers."[99]

---

[93] For one of many examples of public criticism of the USA Patriot Act, see the American Civil Liberties Union at <http://www.aclu.org/safefree/resources/17343res20031114.html>

[94] Hans Graux Neil Robinson, Maarten Botterman, Lorenzo Valeri, "Review of the European Data Protection Directive: Technical Report Prepared for the Information Commissioner's Office," (Santa Monica: RAND, 2009). 14

[95] Digital Civil Rights in Europe, "Final Agreements between EU and USA on Pnr and Swift."

[96] David Garland, *The Culture of Control: Crime and Social Order in Contemporary Society* (The University of Chicago Press, 2001).

[97] "In London, a system for "congestion charging" uses a sophisticated number plate recognition system to charge motorists who drive into central London during business hours. It was revealed that the system was organized in cooperation with the intelligence services that use it with facial recognition systems to monitor the drivers of the cars" (Privacy International at < http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559479>); Mark Townsend and Paul Harris, "Security Role for Traffic Cameras," *The Observer* (2003).

[98] Garret, "Social Work's 'Electronic Turn': Notes on the Deployment of Information and Communication Technologies in Social Work with Children and Families." 536

[99] Chief Secretary to the Treasury, 2003: 53-4, cited in Ibid.538, emphases added by Garrett.

While the state cannot fulfil many of its functions without obtaining the personal data of its citizens, private sector organizations also continuously collect and process personal data pertaining to their employees. The purpose of this is, first, to assess and organize work performances in a more efficient way. In addition, in the course of an employer-employee relationship other information is also needed (e.g. a name and address to conclude an employment contract, a bank account number to pay a salary, education to confirm professional qualifications, etc). Personal information is also collected as a consequence of workplace surveillance (for fraud and general crime prevention purposes).[100]

Another common feature of modern life that is intertwined with public and private institutions is the fact that to benefit from public or private services, people are often put in a position where they have to disclose their personal information or otherwise face a reality of having no access to services and being excluded from other aspects of public life.[101] As a result, an average person can barely live his life without leaving a substantial trail of records behind him.[102]

Another development that is common to both public and private organizations is the increasing automation of decision-making processes. Computers are beginning to analyze the information required for making decisions which were previously in the domain of human discretion, e.g. credit ratings, insurance premiums, or social welfare entitlement.[103] This (partially) automated decision-making is facilitated by the "increasingly routine and extensive sharing of personal data across traditional institutional boundaries. … [This leads to the 're-use' or 'secondary use' of data] that already exist in [a] structured format in databases maintained by themselves or other organizations,"[104] and for purposes other than those for which the data were originally collected. This implies both the commercial use of government data, as well as the utilization of privately built data banks for public purposes.[105]

The last, but by no means the least, of the selected few institutional developments that are relevant to the personal data problem, is the process of internationalization. Given the strong commercial and institutional ties that bind

---

[100] For more on surveillance in the work place see, e.g. Berend R. de Vries Sjaak Nouwt, Corien Prins, ed. *Reasonable Expectations of Privacy?: Eleven Country Reports on Camera Surveillance and Workplace Privacy* Information Technology and Law (Asser Press,2005).

[101] Wright et al, "Privacy, Trust and Policy-Making: Challenges and Responses."

[102] In 2009 it was reported that a Dutch citizen is listed in 250 to 500 public and private databases (B. and Wagemans Schermer, T., *Onze Digitale Schaduw. Een Verkennend Onderzoek Naar Het Aantal Databases Waarin De Gemiddelde Nederlander Geregistreerd Staat* (Amsterdam: Considerati, 2009)., pp. 40-41).

[103] Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits*., p. 96

[104] J. Bing, "Informatics of Public Administration: Introducing a New Academic Discipline," *Informatica ediritto* 1-2 (1992).

[105] See Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits*., p. 95 and the footnotes at pp. 95-96.

countries together in a modern world, one could at least speculate that but for the position of a given country or countries in an international or supranational organization, along with the mere interplay of mutual co-dependencies, some personal-data-related policies or data practices would not have been adopted or taken on the shape they have now. Examples of direct international and supranational influence on data protection policies are some of the instruments of public international and European law. These include:[106] non-binding, but significant, UN guidelines concerning Computerized Personal Data Files of 14 December 1990;[107] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data;[108] the 1981 Council of Europe Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data;[109] the European Convention on Human Rights;[110] and the EC Data Protection Directive.[111] Each of the named instruments relies on varying degrees of consensus on the acceptable standards for data protection practices[112] and, therefore, implies a higher or lower degree of harmonisation of national policies vis-à-vis personal data.

In addition to the general human rights' and regional data protection instruments referred to above, there have also been calls for an international legal

---

[106] The influence of international and, particularly, European law on personal-data related policies may also be indirect, i.e. the influence stems from a legal instrument containing no direct personal-data related obligations. See, for instance, C.M.K.C. Cuijpers, Koops, Bert-Jaap, "Het Wetsvoorstel 'Slimme Meters': Een Privacytoets Op Basis van Art. 8 Evrm.," (2008).
Koops and Cuijpers discuss a Dutch legislative proposal to implement the EC Directive on energy efficiency (Directive 2006/32/EC) by making 'smart energy meters' mandatory for each end-user. The meters are 'smart' because they are designed to provide data on the actual use of energy. The use of these meters generates new types of personal data (on patterns of consumption of energy, types of electric equipment, presence in the house, holiday periods, etc.) as well as opening up opportunities for abuse of this information. Koops and Cuijpers arrived at the conclusion that the Directive does not require implementation in the form of the mandatory introduction of smart meters. Moreover, such a measure is contrary to Article 8 of the ECHR's guarantees of privacy. The point that is, however, relevant for this study is that the initiative of the Dutch government, although it touched on personal data protection interests, resulted from a European law instrument that, on the face of it, is not dealing with the data protection issue, since it related to energy efficiency.

[107] UN Doc E/CN.4/1990/72 adopted in Strasbourg, 28.I.1981

[108] Adopted on 23 September 1980.

[109] ETS 108 adopted on January 28, 1981.

110 Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) Art 8.

[111] Directive 95/46/EC of the European Parliament and Council dated 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement thereof.

[112] The example of the 1995 Directive illustrates how difficult it can be to achieve consensus on the regional let alone the international level. At the stage of discussing the 1990 draft, which was strongly based on German and French proposals, the UK was against an approach to data protection as a fundamental right because it was too abstract. For more details on building consensus in the course of the adoption of the 1995 Data Protection Directive see, for instance, Dorothee Heisenberg, *Negotiating Privacy: The European Union, the United States, and Personal Data Protection* (London: Lynne Rienner Publishers, 2005)., starting on p.51.

framework for privacy and data protection. For instance, Christopher Kuner reports that in 2005, at the 27th International Conference of Data Protection and Privacy Commissioners, the 'Montreux Declaration' was agreed, which appealed to the United Nations "to prepare a binding legal instrument which clearly sets out […] the rights to data protection and privacy as enforceable human rights".[113]This plea has been repeated at different forums ever since,[114] including jointly by some private sector companies like Google, which in 2007 argued for 'Global Privacy Standards'.[115] Moreover, in 2009, the Spanish Data Protection Authority came up with an initiative to draft an international legal instrument on data protection to be submitted for adoption at the United Nations level.[116]

As Kuner argues, due to the lack of a global agreement on the one right approach to privacy and data protection, the time may not yet be ripe for such a worldwide data protection standard.[117] However, existing data protection instruments do have an international harmonizing impact despite the disagreements referred to. The harmonizing effect at times extends beyond the borders of the international and supranational organizations in question. Article 25 of the 1995 Data Protection Directive is a remarkable case, prohibiting the transfer of personal data to other countries unless they provide "an adequate level of protection".[118] According to Heisenberg, almost all of the countries affected by such a prohibition – particularly those with direct investments in the EU and those where EU member states have invested in them - have adopted data protection mechanisms that are generally compliant with the Directive.[119] The US, which is the EU's biggest trading partner, did not pass such legislation; instead, an alternative public-private "hybrid regulation"[120] was introduced in the form of the Safe Harbor Agreement of 2000.

---

[113] Christopher Kuner, "An International Legal Framework for Data Protection: Issues and Prospects," *Computer Law & Security Review* 25, no. 4 (2009)., p. 307 citing the 27th International Conference of Data Protection and Privacy Commissioners, The protection of personal data and privacy in a globalised world: a universal right respecting diversities (2005), <www.privacyconference2005.org/fileadmin/PDF/montreux_declaration_e.pdf>.

[114] Ibid., p. 307-308

[115] Ibid., p. 307 citing <http://googlepublicpolicy.blogspot.com/2007/09/call-for-global-privacy-standards.html>

[116] Ibid., p. 307

[117] Ibid., p. 317

[118] Article 25(1) reads as follows: "The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection." For in-depth analysis of the 'long arm' of the EU data protection law see Lokke Moerel, "The Long Arm of EU Data Protection Law: Does the Data Protection Directive Apply to Processing of Personal Data of EU Citizens by Websites Worldwide?," *International Data Privacy Law*, no. November (2010).

[119] Heisenberg, *Negotiating Privacy: The European Union, the United States, and Personal Data Protection*, 101, 04.

[120] Ibid., p. 73

Despite much criticism, it allows for the transatlantic transfer of the personal data of Europeans by and to American companies which - on a voluntary basis - adhere to certain principles of data processing that are similar to those in the European directive.[121]

2.4. Market-related

By market-related developments this study means both general market processes that are relevant in the field of personal data, and developments that are related to actual data markets.

It has already been demonstrated that both public and private organizations have come to depend a great deal on information pertaining to individuals. In the case of private organizations, this interest has gone beyond the issue of employees' data; the development of new marketing and advertising techniques on both sides of the Atlantic have resulted in an ever-increasing need for consumer data.

The push for the growth of privately held databanks of consumer data was given an impetus by a shift from the mass production that was characteristic of the 1950s, and aimed at "the nameless, faceless American customer",[122] to targeted marketing where the production of goods and services was "directed to discrete individuals or groups."[123] The use of targeted marketing means that the market is determined not by the industry, as it used to be, but is instead attuned to customer preferences. The law of targeted marketing is: the greater the knowledge of the targeted group, the higher its rate of purchasing.[124] Accordingly, the businesses of today are searching for whatever consumer information they can get hold of, which is not limited to actual customers,[125] and often extends beyond consumers' views on

---

[121] For more details on the Safe Harbor Agreement see the website of the US Department of Commerce <http://www.export.gov/safeharbor/index.asp>; for criticism of the agreement, see e.g. Duncan H. Brown, Blevins, Jeffrey Layne, "The Safe-Harbor Agreement between the United States and Europe: A Missed Opportunity to Balance the Interests of E-Commerce and Privacy Online," *Journal of Broadcasting & Electronic Media* 46, no. 4 (2002).

[122] Solove, "Privacy and Power: Computer Databases and Metaphors for Information Privacy.", p. 1404

[123] Ibid. See also J.E.J. Prins, Van der Hof, Simone, "Personalization and Its Influences on Identities, Behaviour and Social Values," in *Profiling the European Citizen: Cross-Disciplinary Perspectives*, ed. Mireille Hildebrandt, Gutwirth, Serge (Dordrecht: Springer, 2008).

[124] "The effectiveness and profitability of targeted marketing depend upon data, and the challenge is to obtain as much of it as possible." (Solove, "Privacy and Power: Computer Databases and Metaphors for Information Privacy.", p. 1407); Arthur M. Hughes, the Complete Database Marketer: Second generation strategies and techniques for tapping the power of your customer database 51 (2d ed. 1996), pp. 267-68 referred to in ———, "Privacy and Power: Computer Databases and Metaphors for Information Privacy.", p. 1405

[125] "In addition to isolating a company's most profitable customers, marketers studied them, profiled them, and then used that profile to hunt for similar customers. This … demanded not only information about existing customers, but the collection of data about prospective customers as well." (Solove, "Privacy and Power: Computer Databases and Metaphors for Information Privacy.", p. 1405)

the product to information of a much more intimate nature, like more general opinions, attitudes, beliefs, detail of lifestyles and "even a full-scale psychological profile."[126]

Based on such a profile, a customer is offered goods or services that he or she is likely to be interested in.[127] This is also referred to as personalization,[128] or one-to-one marketing.[129]

An element of data-sharing on the institutional level, which was mentioned in the previous section, has transformed into a personal data market. Given the huge profits that personal data brings when new marketing techniques are used, as well as the effort and expense associated with acquiring this data, marketers soon realized that they did not always have to research and collect all of this information from scratch, but could simply borrow it from the already existing databases of other enterprises, retail records, client lists, and even government records.[130] Nowadays, collections of personal data are traded for between a few cents and a dollar per name.[131] Along with companies selling information on their clients, which was collected as a by-product of their primary activities, a new branch of the information industry – database builders - has emerged, and is devoted exclusively to the collection of data. The personal information industry brings in annual revenues measured in the billions of dollars.[132] This phenomenon of the high market value attributed to personal data is often referred to as commodification.

Another aspect of the commodification process is that individuals themselves have come to consider data pertaining to them as 'their property,'[133] and habitually

---

[126] Ibid., p. 1404

[127] Section 2.2. elaborates further on profiling practices and profiling-enabling techniques.

[128] Prins and vd Hof, "Personalization and Its Influences on Identities, Behaviour and Social Values." Hildebrandt, ed. *Profiling the European Citizen: Cross-Disciplinary Perspectives*.

[129] The purpose of one-to-one marketing is to sell more products to each customer. One-to-one marketing aims to build a long-lasting relationship with a customer by using her personal information. (Lamb, *Marketing*, 249-50.)

[130] See Nicole Van der Meulen, *Fertile Grounds: The Facilitation of Financial Identity Theft in the United States and the Netherlands* (Wolf Legal Publishers, 2010)., Section 7.1 "Information Brokers"

[131] "Individual credit card details have been sold for as little as 30p." For a recent report on personal data sales, see Murad Ahmed, Burgess, Kaya "Four Million British Identities Are up for Sale on the Internet," *TimesOnline,* no. July, 18 (2009), http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article6718560.ece.

[132] See, for instance, Dave Wieneke, "Is Linkedin for Sale? Does That Mean Your Personal Information Is, Too?," *UsefulArts.us: Online Law Blog: How trademark, copyright, privacy and politics shape the Web.*(2008), http://usefularts.us/2008/06/18/is-linkedin-for-sale-does-that-mean-your-personal-inforamtion-is-too/., reporting in June 2008 that "Bain Capital has bought a 53 million stake in the social networking site LinkedIn. This would bring the total valuation for LinkedIn to just above $1 billion."

[133] The Internet is full of examples of laymen advocating in one or another, more or less organised way for recognition of their property in personal data: a post on the wall of a Facebook group "Stop Facebook To Publish Network-Data Without Permission" – "My data is my property and they have to

disclose it in exchange for money, bargains, or services. Good examples are a supermarket loyalty card, which enables customers to benefit from discounts and special offers, or a free-of-charge e-mail account created 'in exchange for' information about its holder.

2.5. Societal developments

Societal developments are a provisional umbrella term used to cover the processes that are characteristic both for individual members of the populations of Europe and the United States, as well as European and American societies as collectivities.

A prominent societal factor that is relevant to the field of personal data is the fact that people – as social animals - have always had an interest in learning about their neighbours and telling others about themselves. In the last decade, this willingness to share personal information has been met with the emergence of search engines like Google, or the Dutch "people search engine" Wie-O-Wie,[134] as well as Web 2.0 that is aimed at the sharing of information: e.g. blogs, wikis, photo and video sharing websites, and online social networking sites like Facebook, MySpace or Twitter. Indeed, after meeting someone new, it has become common to type their name and any other details into the search bar and be presented with an extensive list of personal information. Companies have been reported to use personal information found on the web to discover what their current or potential employees are 'really like' and then recruit on the basis of what they learn.[135] A shocking example of how easy it can be to collect exhaustive data on an individual is the case of the US Supreme Court Justice, Antonin Scalia. Reported as a blog post on the Above the Law site, it was revealed that for a course assignment a class of Joel Reidenberg managed to obtain on the web "a 15-page dossier on Scalia, including his home address, the value of his home, his home phone number, the movies he likes,

---

protect it."; "The Act Concerning the Right of Property in Personal Data - Draft Proposal for US Legislation" at <http://www.dogchurch.org/dogpac/data.html>

[134] < http://wieowie.nl/>. The engine allows a user to search by full name, as well as a nickname, on the websites of online social networks like Facebook, Twitter, the professional social network LinkedIn, profiles on Yahoo!, Wikipedia, Google and others.

[135] Amy S. Clark, "Employers Look at Facebook, Too: Companies Turn to Online Profiles to See What Applicants Are Really Like," *CBS Evening News*, no. June 20, 2006 (2006), http://www.cbsnews.com/stories/2006/06/20/eveningnews/main1734920.shtml.; "The CareerBuilder survey also shows how quickly social network searches have become an integral part of the recruitment process: overall, nearly half (45 percent) of survey respondents said they were checking new hires' social media profiles, up from just 22 percent last year." (Tameka Kee, "Survey: More Employers Use Facebook to Vet New Hires Than Linkedin," *paidContent.Org: The Economics of Content*, no. 19 August 2009 (2009), http://paidcontent.org/article/419-more-employers-scanning-facebook-for-new-hires-than-linkedin/., original emphasis)

his food preferences, his wife's personal e-mail address, and 'photos of his lovely grandchildren.'"[136]

Desire to communicate is now also facilitated by new means of communication and building relationships. Social network sites have taken over a large element of personal online communication, subverting in popularity personal e-mails and web-pages in the process. After establishing an account with a particular social network site, people willingly and often indiscriminately share information about themselves with dozens or hundreds of their online 'friends', and often complete strangers. Acquisti and Heintz discovered that "CMU users of Facebook provide an astonishing amount of information,"[137] with 39.9% of them disclosing a phone number, while the majority of users set out dating preferences, political views, and their relationship status.[138]

The new way to communicate and relate to people shows itself in the fact that some personal information, like photographic and video images, is made publicly available online not by an individual himself, but by others.[139] The most common example is uploading to a social network profile, and then tagging, photos and videos containing images of friends. Some civil action or 'do-it-yourself-justice' groups have, however, been using the same strategies to fight crime or antisocial behaviour.[140]

A fundamental cause of such a deep invasion of technology into previously technology-free societal phenomena – the building and maintenance of social relationships - is genuine human interest or, as Bygrave puts it, "human fascination for the 'technically sweet' in the form of advanced, push-button gadgetry."[141] The fascination with 'gadgetry' goes beyond online networking services and also includes other technical innovations like a new model of a mobile phone, navigation devices, wireless technology, you name it. Research in the field of marketing suggests that consumers can experience strong emotions during the initial use of innovations.[142] As well as making people happy, these devices, one way or another,

---

[136] Kashmir Hill, "Justice Scalia Responds to Fordham Privacy Invasion!," *Above the Law: A Legal Tabloid*, no. Wednesday, April 29 (2009), http://abovethelaw.com/2009/04/justice_scalia_responds_to_for.php.; the dossier has never been made public.

[137] Alessandro Acquisti, Gross, Ralph, "Information Revelation and Privacy in Online Social Networks (the Facebook Case)," in *ACM Workshop on Privacy in the Electronic Society (WPES)* (2005).

[138] Ibid.

[139] J.E.J. Prins, "Name, Shame and Everlasting Blame," *NJB* 84, no. 3 (2009).

[140] http://perverted-justice.com/index.php or http://hollabacknyc.blogspot.com/. The latter is used by New York women to fight against sexual harassment by posting photo and video images of men who have harassed them, and <http://www.stopkinderpornonu.com/> which reports the areas in Belgium and the Netherlands (in a radius of a few hundred meters around a street) where convicted and suspected paedophiles live.

[141] Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits*., p. 98

[142] Stacy L. Wood, Moreau, C. Page, "From Fear to Loathing? How Emotion Influences the Evaluation and Early Use of Innovations," *Journal of Marketing* 70, no. 3 (2006).

expose the personal information of their users to the rest of the world. Developments in the field of augmented reality promise that all data will soon be available, not only on the web, but also by simply putting an object or individual of interest on one's cell phone that is enabled with a camera and an appropriate application.[143]

2.6. The transformation of the structure of the data flow

This section describes the changes that have occurred in the *overall structure* of personal data flow and are characteristic of the 2000s. The changes have been enabled by a variety of technological, market, institutional and societal factors and have invaded various aspects of modern life. It would be erroneous to try to fit these developments under the five umbrella labels just used above. Therefore, the structural developments in the field of modern data flow are addressed in a separate section. The developments in question are particularly related to the phenomena of chain informatisation, cloud computing, and ambient intelligence.

2.6.1. Chain informatisation

Chain informatisation is a part of the phenomena of organizational cooperation and data base aggregation. It refers to the automated sharing of information between both private sector organizations and government agencies, and is argued to aid the speedy, smooth and customer-friendly provision of services. In practice it means that many small databases are effectively merged into one big database. For instance, an individual, when referring to a state organ or a private entity, does not need to supply them with documented proof of the facts necessary for a particular decision to be made; the relevant entity already has access to all necessary data supplied via the chain of databases of other bodies. Multiple actors are involved in the operation of such a database; some collect personal data first-hand, others process it and others still use it. The actors who collect information do not always end up using it, and the ones making decisions on the basis of that data are not the ones who originally collected it. As well as customer convenience, chain informatisation is said to improve levels of cooperation between various private and public agencies and also addresses complex situations, like child welfare issues and the prevention of child abuse.[144] The complexity of a real-life situation is dealt with by breaking it into separate segments, each of which is then handled by a separate body or authority. Each authority collects or requires data to carry out its share of work. This leads to

---

[143] E.g. Chen, "If You're Not Seeing Data, You're Not Seeing." For more information on augmented reality, see Section 2.1.

[144] "De Burger in De Ketens: Verslag van Nationale Ombudsman over 2008," (Dutch National Ombudsman, 2008).

multiple actors possessing and exchanging relevant information. The 2003 UK Green Paper, *Every Child Matters,* mentioned earlier, proposes a model of data sharing that constitutes chain informatisation. When the data forming that database comes from, or is accessible through, other government agencies or private organizations, chain informatisation is in action.

The longer the chain, the more actors it includes, and the more actors involved, the greater the likelihood that something will go wrong in the process. For instance, there is a danger of incorrect records getting into the system. Although the incorrect data may be used for lawful purposes, it could, nevertheless, have harmful consequences for a citizen or consumer. Indeed, the Dutch ombudsman has referred to an example of an entrepreneur who was mistakenly 'given' a criminal record and was suffering the consequences thereof for 13 years.[145] In cases of children welfare files, the possibility of taking children away from their parents 'by mistake' can not be excluded. Say, a child is merely more active and clumsy in comparison to an average child of the same age and as a result visits the emergency room regularly. Responsible medical personnel may 'flag' the child and a social worker, without going deeper into the details of the situation, may interpret the flags in the system to conclude that the child is being physically abused.

2.6.2. Cloud computing

The phenomenon of cloud computing has been briefly touched upon earlier in this chapter,[146] and refers to the body of web-based – as opposed to on-premises – services, such as an online storage capacity and applications including customer and healthcare records and employee database management.[147] Cloud computing - like chain informatisation - is often presented to businesses as a cheaper way of delivering IT services. Cloud computing is also widely available for private use in the form of web-based email services, photo storage facilities, social networking sites, etc.[148] However, when customers store their data with a cloud computing vendor's hardware, they lose both sight of it and a large element of control over its fate, including its protection from hacker attacks and transfers to the marketing industry and government agencies.[149]

---

[145] Ibid.

[146] Section 2.1.

[147] For more details on cloud computing see, e.g. Martin, "Guide to Cloud Computing."

[148] PrivacyRightsClearinghouse, "The Privacy Implications of Cloud Computing ".

[149] The personal data related concerns resulting from cloud computing will be addressed in more detail later on in this chapter. Meanwhile, see e.g. Cavoukian, "Privacy in the Clouds - a White Paper on Privacy and Digital Identity: Implications for the Internet ".; Gellman, "Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing."

2.6.3. Ambient intelligence

Ambient intelligence (AmI) refers to an architecture whereby computers "melt invisibly into the fabric of our […] life."[150] From a technological point of view, ambient intelligence is enabled by data communication tools, e.g. RFIDs that are 'planted' into various items: household objects, clothes, personal communication devices, goods, etc,[151] which, as a result, become 'smart' and communicate information about or around themselves and 'act' in accordance with this data. For instance, this technology can be used to monitor the supply of goods and provide for their immediate delivery.[152] It also can be used to observe and identify people, "since every possible everyday object will be part of a network."[153] Various 'intelligent' objects have already been marketed. In a Japanese 'intelligent bathroom' the users' blood pressure, weight, and sugar levels are measured and their urine analyzed; the test results are then transferred to a home network and displayed on a computer spreadsheet, accompanied by advice on diet and exercise, and all without any human intervention. The CNN web-site reported in 2005 that 100 of such bathrooms were already sold.[154] Now, imagine the benefits if all these data were also transferred to your GP. In fact, 'smart' wrist bands have already been used to monitor the condition of chronically ill patients from a distance, reporting to a hospital if an individual has had a seizure. The notion of a full-scale ambient intelligence response to every individual's need may sound like science fiction, but one can get a sense of how close this future actually is after checking, e.g, the Phillips' research website, which is reporting progress in this area.[155] Indeed, Wikipedia predicts that AmI will become a reality in the period 2010-2020.[156]

Ambient intelligence is not yet as contemporary a phenomenon as chain informatisation and cloud computing. Nevertheless, it has similar features: a growing number of 'smart objects' collect personal information, not only in the home, but also on the streets and in supermarkets, etc. Indeed, it is present in ever increasing areas of human life, and is connected into a network controlled by various and multiple actors, including goods and service providers, software and hardware maintenance services and an individual himself (the computer controlling the 'smart bathroom' is located in the home).

---

[150] Paul de Hert, "A Right to Identity to Face the Internet of Things?."
[151] H. Rolf Weber, "Internet of Things - New Security and Privacy Challenges," *Computer Law & Security Report* 26, no. 1 (2010). at 23
[152] Ibid.
[153] de Hert, "A Right to Identity to Face the Internet of Things?."
[154] "Health Checks from Your Doctor Could Be Replaced by Visits to the Bathroom, Thanks to a Smart Toilet Developed by a Japanese Company.," *CNN.com* 2005, no. June 28 (2005), http://www.cnn.com/2005/TECH/06/28/spark.toilet/index.html.
[155] http://www.research.philips.com/newscenter/pictures/systsoft-ambintel.html
[156] http://en.wikipedia.org/wiki/Ambient_intelligence

2.6.4. The new structure of relationships within the data flow

The quality that is common to the three phenomena set out above, and which distinguishes them from earlier developments in data processing, is the growing number of actors involved and of the relationships between them. On the one hand, this is a step further along the line of the earlier tendency for information technology to become more widely applied and the number of data processing actors to increase. On the other, if the currently-in-force fourth generation data protection regime is aimed at regulating relatively simple sequences of relationships between these actors, the relationships that are now characteristic of chain informatisation, cloud computing and, in the future, ambient intelligence, are on a completely different scale of complexity.

More specifically, the data flow in the 1990s, although already involving more and more participants, was relatively easy to map. After being collected, personal data was retained by the initial collector for his needs, or was transferred to several other parties for processing on the orders of the collector or for other uses. Indeed, despite a growing number of transfers, the flow of data remained relatively linear with just a few branch lines. With the advances in information technology and practices of the 2000s, especially the developments in Internet use enabling data clouds and chains and the Internet of things, the number of actors involved in data flow has multiplied in geometric progression, as have the number of relationships between them. The latter go beyond simple chains to form a massive structure comparable to a three-dimensional spider's web. In fact, research has revealed that the paths that packets of information take as they travel across the Internet form a dandelion-like structure.[157]

A data subject is at the centre of the web. Each node in the structure represents a data processing actor. Every actor is connected to other actors in the same chain of data flow as well as also being interconnected, by means of cloud computing, to other actors in many other chains. The links connecting the nodes represent the paths that data pertaining to the data subject take, i.e. relationships within the data flow.

The web in fact represents several independent databases, but they also can function as one large database where a piece of data can move from actor X to actor Y by taking a multiplicity of shorter or longer paths, with fewer or more steps and a greater or smaller number of actors involved. This new structure of the flow of data takes the relationships between the data subject and data processing actors to a new, ever greater, level of complexity.

---

[157] Daniel Kane, "Digital Dandelions: The Flowering of Network Research," *USCD News Center*, no. August, 31 (2007). Available at http://ucsdnews.ucsd.edu/newsrel/science/08-07DigitalDandelionsDK-.asp; for similar conclusions about the structure of relationships and communication on social network sites see Caroline Haythornthwaite, "Social Networks and Internet Connectivity Effects," *Information, Communication, and Society* 8, no. 2 (2005).

3. Conclusion

The purpose of this chapter was to look at one side of the personal data problem – the developments that have taken place in technology, public and private institutions and markets and marketing strategies, as well as the way people function, communicate and build relationships in the modern information society. The developments are many and various. Nonetheless, two trends appear more prominently. The first is the constantly growing thirst for information, both in the public and private sector. The state and businesses want more personal information, allegedly, in order to be more efficient and serve citizens or customers better, but also to control the population and channel human behaviour into a desired direction, whether it is greater obedience of the law, more respect for social rules and better security, or other, less noble, forms of manipulation. People's private lives have also become more dependent on sharing personal data; we are always reachable via e-mail and mobile technology, we give access to our personal information to acquaintances or 'friends' via social network profiles, and keep people 'posted' with updates in our status, etc. A failure to adapt to this online lifestyle is likely to lead to social exclusion. The second trend is the growing capacity of technology to accommodate the desire for more information, personalisation and better communication. Hardware has also decreased in size and price, making technology more accessible, invading more aspects of human life and reporting on it. Software has also been developed to perform short of any type of imaginable analysis of personal data.

Although this study does not aim to establish any cause-and-effect relationships, one cannot help but conclude that the unquenchable thirst for personal data and the development of enabling technology are interrelated.[158]

Although technology and the desire for information began as relatively independent phenomena, they have now become so intertwined that there are, without a doubt, causal connections between them. For a non-sociological study such as this one, it is difficult to see what causes what: whether the need for data triggers technological developments, or whether the latter, as seen in the section on the new structure of data flow, have gained a momentum of their own, making more data available, with the supply creating the demand. In this 'chicken-and-egg' situation, involving major institutional, market and social processes with lives of their own, what remains to be seen is whether an individual who, on the one hand, has triggered the processes in question, has, on the other, in many ways also become their hostage. The following chapter will, therefore, consider these and the other concerns raised by personal data related developments.

---

[158] Other studies, however, show that technology has "natural" tendency to erode privacy (Ronald Leenes, Koops, Bert-Jaap, "'Code': Privacy's Death or Saviour?," *International Review of Law, Computers, and Technology* 19, no. 3 (2005).)

Chapter 3: The personal data problem: concerns

1 Introduction

The concerns raised as a result of new personal data related developments comprise the second part of the personal data problem. Given the increased scope and, often, the sensitivity of the personal information processed as a result of institutional, market, societal and technological developments, it comes as no surprise that the actual and potential effects of data processing raise numerous concerns in academic and political circles, as well as among the general public. To be fair, new data practices have, in many ways, brought a lot of benefits to the Western, post-industrial societies we live in, and it is hard to now imagine doing without them.[159] However, the focus of this book is on propertisation as a remedy for the negative effects of personal data related developments. Therefore, the following discussion will only address the downsides, or 'concerns'.

As well as describing the concerns, the end goal of this exercise is to get a clear idea of what is seen as problematic about the current ways in which personal data is handled in Europe. The value of such a descriptive exercise is well-explained by John Dewey: "The way in which the problem is conceived decides what specific suggestions are entertained and which are dismissed; what data are selected and which rejected; it is the criterion for relevancy and irrelevancy of hypotheses and conceptual structures."[160] It will become clear in the subsequent parts of this book that the way in which the personal data problem has been *conceptualis*ed often channels and, therefore, explains the choice of tools available to tackle it, *i.e.* the instruments of personal data protection employed at present, as well as the proposed alternative tools, of which the propertisation of personal data is one example.[161] The respective conclusions reached should lay the groundwork for the subsequent chapters to examine if the introduction of property rights in personal data could be a way to achieve the goals that are desirable with regard to the European personal data regime – to tackle the concerns most prominent of which are presented further.

The concerns are many and various. There is, however, no agreement regarding their nature and validity, despite a vast amount of attention being devoted to the transformation of information practices and the development of information

---

[159] For an account of the benefits of data processing and limits of privacy see, e.g. Amitai Etzioni, *The Limits of Privacy*, 1 ed. (Basic Books, 2000).

[160] John Dewey, Logic: The Theory of Inquiry 108 (1938) cited in Solove, "Privacy and Power: Computer Databases and Metaphors for Information Privacy.", p. 1399

[161] e.g., Chapter 5, section 3 explaining how conceptualisation of privacy as secrecy of information determined the development of the US *Information Privacy Law*.

technology since the 1960s. Indeed, as Colin Bennett accurately points out, "it is not immediately obvious … what harm results from the computerized collection, use, and disclosure of personal data."[162]

Moreover, an adequate *conceptualis*ation of the problem that is linked to relatively recent and rapid developments in technology, requires not merely an in depth analysis, but also time. The time is needed for the actual consequences of the constantly evolving information practices to become more apparent, and for the parties involved to familiarize themselves with the problems' ever-changing spectrum. The aim of this research is, however, to examine (one of) the solutions to the *already articulated* aspects of the personal data problem, not to express it differently or discover new sides thereof. The following analysis will specifically focus on reviewing what other scholars have had to say about the concerns related to personal data. Since there is an enormous body of writing on the topic, the literature review will not be comprehensive, but will instead be detailed enough to provide an overall impression of the subject.

To bring some order to the analysis of the multiplicity of personal data concerns, it is helpful to consider them against a theoretical backdrop. The theory of choice in this study is the one articulated by Tal Zarsky in his article *Desperately Seeking Solutions: Using Implementation-Based Solutions for the Troubles of Information Privacy in the Age of Data Mining and the Internet Society.*[163] In it, Zarsky distinguishes three elements of the personal data flow - collection, analysis, and the implementation of data - and suggests that solutions to personal data problems are dependent on the stage at which the problems occur.[164] Following this logic, the subsequent sections will group each particular concern according to stages in the personal data flow.

---

[162] Bennett, *Regulating Privacy - Data Protection and Public Policy in Europe and the United States.*, p. 12

[163] Zarsky, "Desparately Seeking Solutions: Using Implementation-Based Solutions for the Troubles of Information Privacy in the Age of Data Mining and the Internet Society." Alternative approaches to the classification of relevant concerns are possible. See, for instance, Solove's classification of privacy harms inDaniel J. Solove, "Conceptualizing Privacy," *Cal. L. Rev.* 90 (2002)., and ———, "A Taxonomy of Privacy," *U. Pa. L. Rev.* 154 (2006). Moreover, Zarsky's theory as a backdrop for the present analysis has its weaknesses. To name a few of these, the classification of certain data practices by Zarsky as belonging to a particular stage of data flow is, at times, questionable, and his theory also has a normative perspective (some may interpret the division of the data flow into collection, analysis, and implementation as already implying a solution). However, the decision to adopt Zarsky's approach has been guided by pragmatic considerations to bring order to the chaos in the discourse on personal data related concerns and the theory seems to cope with the task well.

[164] Zarsky, "Desparately Seeking Solutions: Using Implementation-Based Solutions for the Troubles of Information Privacy in the Age of Data Mining and the Internet Society.", p. 15

2. Data collection: secrecy, misbalance of power, freedom, autonomy, etc.

Concerns related to the first phase of the flow of information – the collection or disclosure of personal data - were the first to take the stage in the data protection debate. Personal data is collected via different types of surveillance, such as with security cameras, the monitoring of online activities, the taping of phone conversations, etc.

These collection-related concerns demonstrated themselves in calls to protect individual privacy, privacy being understood as the Warren and Brandeis' right to be let alone,[165] and to experience social isolation, solitude and withdrawal. At the heart of these concerns lies the notion that the secrecy of (certain types of) personal information has a value of its own and must be protected. An individual requires an element of secrecy around which to develop his personality, process and express emotions, and build relationships, etc.[166] The infringement of privacy as secrecy by the disclosure of private facts, or surveillance, threatens the violation of personal security, "inhibition, self-censorship, embarrassment, and damage to reputation."[167]

In the United States, the personal data problem has long been *conceptualis*ed as a problem of the secrecy of information, the disclosure of confidential data, and surveillance.[168] Ever since the 1960s, the policy and academic debate has been dominated, in Solove's words, by the "mantra of 'privacy'"[169] and "the protection of our individual right to be let alone."[170] Priscilla Regan points out that "a new technology might allow for observation of actions regarded as 'private,' listening in on conversations thought to be 'private', collection and exchange of information thought to be 'private', or interpretation of psychological responses viewed as 'private.'"[171]

The opposite of "information privacy," *i.e.* the absolute transparency of our personal lives, has been captured in a metaphor of Big Brother.[172] The metaphor comes from George Orwell's novel *Nineteen Eighty-Four,* which describes a totalitarian state able to constantly watch and control every move of its citizens. The metaphor brings up another implication of the violation of privacy as secrecy,

---

[165] See Samuel Warren, Louis Brandeis, "The Right to Privacy," *Harvard Law Review* 4 (1890).

[166] Yves Poullet, "Data Protection Legislation: What Is at Stake for Our Society and Democracy?," *Computer Law & Security Report* 25 (2009)., p. 113-114 and footnotes.

[167] Solove, "Privacy and Power: Computer Databases and Metaphors for Information Privacy."

[168] Ibid., p. 1431

[169] Ibid. See e.g., Regan, *Legislating Privacy: Technology, Social Values, and Public Policy*., pp. 3, 15; P. Blok, *Recht Op Privacy* (Boom, 2002)., p. 245; Report "Federal databanks and Constitutional Rights," p. ix, etc.

[170] Senate Floor debates, reprinted in US Senate and House Committees on Government Operations, Legislative History of the Privacy Act of 1974, s. 3418 (PL 93-579), 94th Cong., 2d sess. (Washington, D.C.: Government Printing Office, 1976), p. 775

[171] Regan, *Legislating Privacy: Technology, Social Values, and Public Policy*., p. 2

[172] Solove, "Privacy and Power: Computer Databases and Metaphors for Information Privacy.", p. 1413

namely an upsetting of the balance of powers between individuals and data collectors - public and private organizations. As Regan explains, with advances in information technology, organizations acquire new power that is derived from gaining "access to information about individuals' histories and activities, the content and patterns of their communications, and their thoughts and proclivities."[173] So far as a power balance between a citizen and a government is concerned, Lessig has articulated a common US presumption that "privacy is meant as a substantive limit on the government's power. Understood this way, privacy does more than protect dignity or limit intrusion; privacy limits what government can do."[174]

Related to the concern of the upset balance of powers is a fear that surveillance and the free availability of personal data, especially in relation to opinions, behaviour, and other characteristics that are different from those of the majority, may prevent citizens from speaking up,[175] instead making them engage in self-censorship and inhibiting eccentric or other behaviour that deviates from the norm.[176] The result is the undermining of individual autonomy. Fear of raising a voice in protest or expressing oneself undermines the existence of civil society[177] and participatory democracy.[178] The current advances in data processing technology enable "the power of the dominant community to norm others into oblivion."[179]

---

[173] Regan, *Legislating Privacy: Technology, Social Values, and Public Policy*., p. 2

[174] Lessig, *Code 2.0*., p. 213

[175] Rouvroy, "The Right to Information Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy.", Paul M. Schwartz, "Privacy and Participation: Personal Information and Public Sector Regulation in the United States," *Iowa L. Rev.* 80 (1995).

[176] This point has been made in the 1983 census decision of the German Constitutional Court (BVerfG, Karlsruhe, Dec. 15, 1983, EuGRZ, 1983, p. 171 and ff.); see also Serge Gutwirth, de Hert, Paul, "Regulating Profiling in a Democratic Constitutional State," in *Profiling the European Citizen: Cross-Disciplinary Perspectives*, ed. Mireille Hildebrandt, Gutwirth, Serge (Dordrecht: Springer, 2008).

[177] "Civil society refers to the arena of uncoerced collective action around shared interests, purposes and values. In theory, its institutional forms are distinct from those of the state, family and market, though in practice, the boundaries between state, civil society, family and market are often complex, blurred and negotiated. Civil society commonly embraces a diversity of spaces, actors and institutional forms, varying in their degree of formality, autonomy and power. Civil societies are often populated by organizations such as registered charities, development non-governmental organizations, community groups, women's organizations, faith-based organizations, professional associations, trade unions, self-help groups, social movements, business associations, coalitions and advocacy groups." ("What is civil society?". Centre for Civil Society, London School of Economics. 2004-03-01. http://www.lse.ac.uk/collections/CCS/what_is_civil_society.htm. Retrieved 2006-10-30.)

[178] "Participatory democracy strives to create opportunities for all members of a political group to make meaningful contributions to decision-making, and seeks to broaden the range of people who have access to such opportunities." Wikipedia <http://en.wikipedia.org/wiki/Participatory_democracy>

[179] Lessig, *Code 2.0*., p. 219

3. Analysis of data: fear of errors, misrepresentation, dehumanization, and 'perfect knowledge'

The 'analysis' is everything that happens to data between its collection and implementation, including, but not limited to, making, storing and maintaining records, building and mining databases, and deducing knowledge from datasets. The diversity of these processes gives rise to quite different concerns.

The obvious weak point of the stage of analysis is that a record might contain errors, or a dossier may be outdated or incomplete. If that happens, a false image of an individual that is taken from the faulty record may be used to make decisions which seriously affect this person's life. The negative consequences of data analysis gone wrong go far beyond damage to reputations. Recall the case of Mr Arar: a Syrian-born Canadian national was stopped and detained at New York JFK airport on suspicion of terrorist activities. He was then questioned by US authorities, with all of these events being based on documents obtained from the Canadian police and intelligence services. He was finally extradited to Syria, where he was subjected to torture. Eventually, it transpired that the intelligence collected by the Canadian authorities and used as a ground for detention and extradition was not, in fact, true.[180]

A fear of a more intangible nature is that of dehumanization, both of an individual in his capacity as a citizen or consumer, and of the decision-making process. The former concern relates to the fact that, as a result of the automated analysis of personal data, private business and government clerks will not perceive an individual who they are dealing with as a human being but as a file. The file will be a substitute for a personality and will determine an individual's future. This fear was expressed in US legislative hearings in the 1970s by Representative Cornelius Gallagher: "'The Computerized Man,' as I see him, would be stripped of his individuality and privacy. Through the standardization ushered in by technological advance, his status in society would be measured by the computer, and he would lose his personal identity. His life, his talent, and his earning capacity would be reduced to a tape with very few alternatives available."[181]

The second dimension of dehumanization relates to a bureaucratic process of handling personal records, which is often uncontrolled and chaotic, with little transparency and accountability. Indeed, among others, Solove,[182] Bennett,[183] and

---

[180] For more detail on Arar's case see "Privacy International Case Report," (London: Privacy International). at <http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-543297&als[theme]=Anti%20Terrorism>)

[181] Cited in Regan, *Legislating Privacy: Technology, Social Values, and Public Policy*., p. 72

[182] Solove, "Privacy and Power: Computer Databases and Metaphors for Information Privacy.", p. 1439

[183] Bennett, *Regulating Privacy - Data Protection and Public Policy in Europe and the United States*.

Westin,[184] link the essence of the data processing problem to bureaucratic processes. According to Weber's classification, these bureaucratic processes are highly routinized, and above all prioritize efficiency, the standardization of decisions, and the cultivation of specialization and expertise.[185] The major threat of bureaucracy is its predisposition to dehumanize in an attempt to eliminate "love, hatred, and all purely personal, irrational, and emotional elements which escape calculation."[186] On the other hand, in Solove's view, bureaucracy often fails to pay adequate attention to an individual – "not because […] officials are malicious but because they are busy, face extreme stress, must act within strict time constraints, have limited training, and are often not encouraged (or even authorized) to respond to idiosyncratic situations creatively."[187]

The final concern, which is related to the stage of analysis, has to do with the aggregation of personal data. There are two sides to the problem of aggregation. Firstly, most of the information about individuals is not sensitive, embarrassing, or kept secret for any other reason. The damage from disclosing one's grocery shopping list is also minimal. What *is*, however, disturbing, in the age of the Internet and data warehouses is that these arbitrary pieces of information have been aggregating. One random record of Sunday shopping may be innocent. But when nearly *every* piece of information is recorded and stored, the body of data resulting from such aggregation has the potential to reveal some deeper and more sensitive knowledge about the individual to whom these records pertain.[188] Indeed, the Internet enables the aggregation of a wide range of personal information; everything done online leaves traces.

A related concern is expressed by Lessig. The existence of a large and virtually all-inclusive database that is open to searches brings to zero a pre-internet era "benefit of innocence;"[189] innocent facts when taken out of context may be interpreted as compromising, which is an imperfection of the system of "perfect knowledge."[190]

---

[184] Westin, *Privacy and Freedom*.

[185] Solove, "Privacy and Power: Computer Databases and Metaphors for Information Privacy.", p. 1421-22

[186] Weber, "Internet of Things - New Security and Privacy Challenges.", p. 216

[187] Daniel J. Solove, "The Darkest Domain: Deference, Judicial Review, and the Bill of Rights," *Iowa L. Rev.* 84 (1999): 1017. At 1017

[188] This point is made, among others, in Solove, "Privacy and Power: Computer Databases and Metaphors for Information Privacy." Acquisti states that it is possible to 'guess' a social security number with a high degree of accuracy knowing only a person's gender, zip-code and date of birth – the data not that sensitive and casually revealed when taken separately (Acquisti, "Information Revelation and Privacy in Online Social Networks (the Facebook Case)."

[189] Lessig, *Code 2.0.*, p. 218

[190] To illustrate the loss of the benefit of innocence, Lessig uses an example of a man walking out of a hotel in the company of a woman young enough to be his daughter; taken alone this observation is implicating the man in, possible, infidelity, or the manipulation of a younger woman, possibly his

Another, wider consequence of data aggregation relates to the fact that there is an enormous database out there already combining smaller databases which, in the age of universal data sharing, are somehow interconnected. Such a state of affairs takes the control of personal information out of the hands of an individual; we can never be sure that the piece of data that we refuse to disclose, or want to remove from one database, is not stored by another and, therefore, accessible to anyone sharing that second data bank.

Such 'hyperavailability' of personal information in part undermines the idea of *personal* data protection. Indeed, thanks to profiling, an individual does not need to reveal *his* personal information to be subjected to personal data related treatment, like price discrimination. As long as there is enough data to build a profile about people *like* the individual in question, a very small piece of data, such as an IP address, is enough to identify a citizen or a consumer with a group profile and treat him accordingly. So, Lessig writes: "Companies don't spend money collecting data about you. They want to know about people like you. […] What the merchants want is a way to discriminate – only in the sense of being able to tell the difference between sorts of people."[191]

4. The implementation of data: discrimination, manipulation, inequality

Implementation in Zarsky's classification means every use that personal data is put to after its collection and analysis. How certain kinds of personal information are used has always been a matter of concern. Sensitive data in particular, such as ethnic origin, race, or political opinions, may be a reason for unjust persecution, social exclusion, and discrimination. The Holocaust, political repression in the former Soviet bloc and apartheid in South Africa are only a few recent examples of the devastating power that sensitive personal data has when put to unjust use. These dangers have, however, been present ever since people learned to discriminate and they are still valid today. What has changed, though, with the advance of information technologies is that any data – automatically coupled with other data and analyzed – may give rise to unjust treatment. Specifically, these concerns relate to profiling, which draws upon many bits and pieces of information scattered across multiple databases, then builds an image of an individual as a citizen or consumer and applies that image to make predictions about his future.

Some people may be happy with the results of applying to them, for instance, consumer profiles. 'Smart' websites show individuals only selected advertisements and save time and effort by separating useless commercials from information about

---

employee, into having a relationship with him, an older man. The least serious blame is being a part of an obvious mismatch; in reality, the woman *is* his daughter. (Ibid.)

[191] Ibid., p. 217

desired products.[192] However, some authors warn us that such practices may lead to manipulation, stigmatization, price- and other sorts of discrimination, and inequality in general. Lessig wonders - when the system is 'smart' and seems to know what we want better and more quickly than we do - how can we be sure that these wishes are genuinely ours.[193] Zarsky refers to this phenomenon as an 'autonomy trap.'[194] The point is that an individual's autonomy to make choices – even very simple ones like what book to read next - is questionable when the range of options and the context of the choice are being controlled by others.

The profiling of consumers is said to have the potential to lead to economic segregation; it helps online businesses to fine-tune their services in order to attract some and force out other customers based on social and economic criteria.[195] Related to the concerns about economic segregation is the possibility of price discrimination. Wealthier customers, or those less concerned about what they spend, are more likely to pay a higher price for a product, whereas others are always looking for a discount. To achieve greater profits, online businesses relying on these two profiles, divide their customers into two groups and may alter their pricing in such a way that the former receive discount offers once in a while – with the purpose of rewarding their loyalty – whereas the latter are not shown any offers. Since the two types of customers rarely sit next to each other while making online purchases, it is difficult to demonstrate that price discrimination ever took place.[196]

The profiling techniques that provide in-depth knowledge about groups of people may also reveal other characteristics which may lay the groundwork for a broader range of discriminatory policies in both the private and the public sector. For example, insurance companies are reported to discriminate against people based on genetic screaning or family history of a genetic disease such as Huntington's;[197] in the absence of detailed information about every individual, racial and religious *group profiling* is used as a security measure and leads to religious and racial

---

[192] Leenes uses an example of a winter tires' advertisement in California. See Leenes, "Do You Know Me? Decomposing Identifiability."

[193] Lessig, *Code 2.0.*, p. 219; also in Lawrence Lessig, "The Law of the Horse: What Cyberlaw Might Teach," *Harvard Law Review* 113 (1999).

[194] Zarsky, "Desparately Seeking Solutions: Using Implementation-Based Solutions for the Troubles of Information Privacy in the Age of Data Mining and the Internet Society."

[195] Lessig, *Code 2.0.*, p. 220

[196] Leenes uses an example of Amazon and its price discrimination policies in Leenes, "Do You Know Me? Decomposing Identifiability."

[197] A 2009 study at the University of British Columbia, the first study of genetic discrimination in Canada, shows that "Canadians at risk of developing Huntington's disease frequently experience unfair treatment based on genetic information." (see http://www.med.ubc.ca/media/Canadians_at_risk_for_Huntington_s_disease_suffer_genetic_discrimination.htm) See also the same study published on June 10 2009 online in the British Medical Journal at www.bmj.com.; but see Aad Tibben, "Genetic Discrimination in Huntington's Disease," *BMJ* 338 (2009). "Genetic testing gives people at risk the opportunity to take more responsibility and control over their lives, their health, and their future."

discrimination.[198] These are but a few of the many disturbing examples of the various uses that personal data may be put to.

5. Beyond Zarsky's paradigm: a lack of transparency and accountability in the data flow

This chapter began with a disclaimer when describing concerns related to the processing of personal data; the analysis operates under a presumption that the classification of the concerns, which is based on Zarsky's paradigm, is not perfect, but is good enough to bring some order to a complex and multifaceted debate. The reader may have noticed one imperfection of the classification - some of the concerns mentioned relate to the all stages of the data flow: collecting, analyzing, and implementing data. Without repeating a more substantial description provided earlier, the concerns that are common to all three phases of information flow are the increasing availability of personal data for collection, storage, analysis, and implementation.

Another group of concerns, which goes beyond Zarsky's paradigm, is related to the new structure of the modern data flow. These concerns include data vulnerability, the lack of accountability on the part of the actors involved in the data flow, and the opacity – or lack of transparency – of the personal data related processes. These issues will be the focus of this section.

The new complexity of the relationships within the data flow described in Chapter 2[199] reinforces old and raises new data protection concerns, in particular those of transparency and accountability. Even more than previously, the lack of transparency in the data flow makes accountability for data protection violations a virtually unattainable goal. Firstly, the paths that personal data may take within the web of the data processing relationships are extremely entangled and difficult to trace or predict. This means that they are, therefore, also hard to regulate. Secondly, within the multiplicity of the intertwined information chains, it is unclear how the burden of accountability for data protection is distributed among all of the involved actors, since their identity, as well as their exact contribution to the entire process, are not clear.

For instance, when a mistake or a data security breach occurs in the context of chain informatisation, it is difficult to name a single responsible government agency

---

[198] ["A]re employees at stores that are trying to prevent theft of their goods justified in watching minority customers more carefully than they watch others? Macy's was recently fined for allegedly watching blacks and Hispanics more carefully, although the company denies that such profiling of customers is their policy." (Gary Becker, "Is Ethnic and Other Profiling Discrimination?," in *The Becker-Posner-Blog* (2005).)

[199] Chapter 2, section 2.6.4.

that is supplying, retaining or analyzing data, since it is not always clear how the piece of information at hand made it from point A to point B. Failures are blamed on the system and its complexity. Moreover, it also takes a long time to correct a mistake: first, the error has to be reported to the agency which used data in question, then those in charge of the original database from where the authentic data was retrieved have to be notified, look into the mistake, verify the data, and then let the next link in the chain know if the information was indeed false and share the corrected data. The organization receiving the new data also has to make sure that the mistake is corrected in its database. In the meantime, however, there is a big chance that a citizen will have suffered the consequences of 'bad' informatisation. What is more, because the different actors have access to the better or poorer data management resources, when the databases of different scales and quality merge together, they are inherently difficult to control and protect. It is also difficult to ensure that all of the actors who copied the false piece of data into their systems have corrected it.[200]

Cloud computing and, in the future, ambient intelligence, open access to personal data up to third parties – the contractors providing data storage, management, and analysis services. Therefore, the phenomenon of cloud computing represent similar 'transition of quantity-into-quality' dangers. 'Quantity-into-quality' in brief, means that the greater the number of data transfers between actors, the poorer the 'quality' of the data transfers, i.e. the higher the likelihood of errors, data loss, and security breaches, and the lower the opportunity to identify those responsible. Finally, especially on the Internet, the facts of collection, analysis and implementation of one's personal information are not apparent to a lay individual: although the knowledge that some information is being collected can be expected, which information that is will not be obvious, just as who collected it, what algorithms have been used to analyse it, and who, how and when if at all will be using it. In other words, the changes that occurred in the structure of the data flow gave ground for new concerns going beyond the old fears of collection, analysis, and implementation of personal data.

6. The need for a next generation personal data regime

The purpose of this section is to look at the concerns regarding personal data practices from the broader perspective of the evolutionary approach to the development of data protection legislation. The thesis advanced here is that, although the concerns that were addressed by the first, second, third, and fourth generation approaches to this issue are still valid, the recent developments in the

[200] "De Burger in De Ketens: Verslag van Nationale Ombudsman over 2008."

structure of modern data flow have taken them to a new level of complexity which calls for a next generation personal data regime. Another disclaimer does, however, need to be made here. The particular weaknesses of the current European data protection instruments will be demonstrated in detail in Chapter 7 of this book. The analysis in this section is of a principal level.

Let us again take a look at the evolution of the relationships in the data flow and data protection legislation so far. Data protection law has always had to conform to both quantitative and qualitative changes in the relationships within the data flow: quantitative because the number of actors collecting, analyzing, and using personal data has been constantly growing, as have the number of relationships; and qualitative because the relationships were becoming more complex. For instance, at the beginning of the Information Revolution, because computers were expensive and available only to a small number of actors, it was expected that there would only be a few data banks. As a result, the first-generation data protection norms targeted these databases individually and did not include generally applicable data protection rights.[201] However, as computers became easily available, and the number of actors processing personal data grew and could be counted in the thousands, second-generation data protection laws shifted in favour of the generally applicable negative – non-disclosure – rights of citizens, so that they could protect their interests.[202] Later, as data protection relationships extended beyond the mere collection of data, third-generation data protection regimes moved towards trying to strike a balance between privacy and participation in the information society, which they did by pairing non-disclosure with more participatory positive rights to control subsequent data use.[203] Finally, to address another complexity of data flow, *i.e.* the inequality of the negotiating powers of weak data subjects and powerful information industries, the fourth-generation data protection laws – including the 1995 Data Protection Directive – have, by means of regulation, established some ground rules, namely the principles of data processing.[204]

Currently, however, the new complexity of modern data practices has outgrown fourth-generation data protection measures. As demonstrated earlier, the rationale of the fourth generation regime of personal data protection is based on a system of personal rights of the data subject coupled with corresponding obligations on the part of the data processing actor (in the 1995 Data Protection Directive – data controller) and some regulation. These rights are personal, but not only in the sense that they protect an individual's personality; they may also be described as personal in the language of private law, where personal rights are in dichotomy with real rights. The major difference between the two types of rights is that the former are

[201] Mayer-Sch□nberger, "Data Protection in Europe." 225
[202] Ibid. 227-228
[203] Ibid. 229-232
[204] Ibid. 232-235

enforceable only against a party to a particular – e.g. contractual - relationship, whereas the latter take effect against the world, which is otherwise known as *the erga omnes* effect.[205] Accordingly, based on the personal rights and enforcement against a narrow range of data processing actors, the fourth generation data protection regime relies on the assumption that personal data relationships, as well as the data processing actors and the distribution of accountability between them, are transparent and identifiable. As this chapter has revealed, this simplicity in the flow of data is long gone. The number of actors involved in chain informatisation, cloud computing, and (potentially) ambient intelligence is so high, and the relationships between them so intertwined and opaque, that the structure of accountability that is characteristic of the fourth generation regime is virtually impossible to enforce.[206] As a result, although the rules of the fourth generation generally may address the personal data concerns and reflect values related to data collection, analysis, and implementation, the concerns raised by the new structure of the data flow are not dealt with; as a result, their other goals as well remain unreached. That inadequacy calls for reconsideration of the current data protection regime in favour of a regime of the next generation.

7. Conclusion

This chapter completes the account of the personal data problem with an overview of the concerns raised by the old and new personal data practices described in Chapter 2. The concerns are many and various. To name a few dominant ones, one concern is that the increasing collection of personal data undermines the notion of privacy in terms of the secrecy of personal information. A breach of secrecy, as well as undermining a value of secrecy in its own, is also argued to lead to a misbalance of powers between governments and private institutions and an individual. Thereby the individual freedom and autonomy are put at risk. In addition, there is also a fear of harmful consequences arising from errors in personal records, data being taken out of context, and misrepresentation. The implementation of data opens the door to unjust treatment, discrimination, economic segregation and general inequality. The traditional list of concerns has been added to with others which derive from the new structure of the modern flow of data anno 2000s. The increase in the number of data processing actors, and the relationships between them in information chains, computer clouds, and ambient intelligence, have made the paths that personal data

[205] For more on the distinction between real and personal rights see, e.g. Steven Bartels, et al., *Content of Real Rights* (Wolf Legal Publishers, 2004)., and Michael J. Milo, "Property and Real Rights," in *Elgar Encyclopedia of Comparative Law*, ed. Jan M. Smith (Edward Elgar, 2006).

[206] For more detail on the difficulties in the enforcement of the fourth generation data protection instruments (namely, the 1995 Data Protection Directive) see Chapters 6 and 9.

take ever more complex and difficult to predict or channel. This raised concerns about the lack of transparency of data flow and the accountability of the actors involved in it. Opacity and a lack of accountability not only aggravate the more traditional personal data related concerns, but also impede the enforcement of the current legal rules of the fourth generation of data protection legislation. This raises the questions of whether the currently in place fourth generation data protection laws are capable of meeting the challenges of the modern data flow and, if not, whether a new approach to personal data protection is required. Given that the creation of property rights in personal data is one of the proposed new approaches, the next chapter introduces the notion of property rights in law.

Chapter 4: Introduction to property discourse

1. Introduction: agreeing on terms

The aim of this chapter is to make some basic statements concerning property in general, which are vital for the further analysis of the notion of property in personal data. This will be conducted with three objectives in mind: firstly, to specify the perspective that this study takes on property; secondly, to address some reservations and concerns that are already in the minds of continental European readers regarding the propertisation of a new object such as personal data, especially in terms of the seeming impossibility of extending property rights beyond what is traditional to include such an unconventional object; and last, but not least, to deal with the view that market alienability is an allegedly inevitable aspect of propertisation. Finally, clarification of the range of perspectives on, and the uses of, property will prepare the reader for the critical scrutiny of the American information privacy and propertisation debate that follows in Chapters 5 and 6.

2. Distinguishing the legal perspective on property

Special attention to the perspective on property is a reaction to a remarkable trait in the body of literature on the propertisation of personal data: when engaging in the debate, its participants have relied on their various – legal as well as economic, normative, and other - backgrounds to draw assumptions about property. Simultaneously, however, they have not demonstrated much awareness of the differences in their respective approaches. For instance, it is quite common in the private law literature on property to emphasize that the meaning of property in economic theory is substantially different from its denotation in law,[207] while, again unlike the law, normative theories only focus on the moral justification of property rights and not on their content.[208] However, in the literature on the property in personal data, a number of authors still use moral or economic arguments in a legal

[207] E.g., Yoram Barzel, *Economic Analysis of Property Rights*, 2nd ed. (Cambridge University Press, 1997). p. 3: "Property rights in economics are "the individual's ability, in expected terms, to consume the good (or the services of the asset) directly or to consume it indirectly through exchange. […] Legal rights are the rights recognized and enforced by the government. These rights, as a rule, enhance economic rights, but the former are neither necessary nor sufficient for the existence of the latter. A major function of legal rights is to accommodate third-party adjudication and enforcement. In the absence of these safeguards, rights may still be valued, but assets and their exchange must then be self-enforced."

[208] E.g. James Gordley, *Foundations of Private Law : Property, Tort, Contract, Unjust Enrichment* (Oxford [etc.]: Oxford University Press, 2006).

debate.[209] At the same time, what has been overlooked is the fact that the concept of property in law has a meaning of its own which is certainly informed by but also largely independent of the meanings assigned to property elsewhere. As a result, the debate has been polluted with the persistent presence of contradictory statements about what property is and is not and what it is or is not able to achieve, as well as comments on the morality of property rights themselves and the assigning of those rights to various actors. To mention only a few of these contradictions, for some, property rights make sense because an individual then controls his personal data and can negotiate with the information industry about the terms of its disclosure and use. Others, however, wonder if propertisation is able to restrain the commodification of personal data when property rights are meant to *enable* the market exchange and alienability of resources.[210] Accordingly, in circumstances where there is no clarity about the perspective one is taking on property, or even an acknowledgement of the differences in backgrounds and assumptions, this provides for a debate without a constructive outcome.

The perspective of the present study is that of the law. This means that the notion of property in personal data is considered neither on the basis of its moral righteousness, as normative theories would demand, nor in terms of its economic efficiency. In other words, whereas introducing property in an object is almost always a policy decision informed by the arguments of the economic or normative theories or the potential effects it would have on the lay people, the concept of property in personal data is examined here solely on the basis of its content and consequences of its use in law. That is, the legal perspective on property employed here understands property in terms of the content of property rights and what effects those rights have in a larger context of a legal system.

The legal approach in this study on property will be clarified by setting out what it is not, *i.e.* distinguishing it from the alternative perspectives of a layman and the already mentioned economic and normative outlooks (Section 2). Since the legal perspective is tied to the meaning of property in law, Section 3 will address the latter, with the focus being on Europe as the region of interest to this work.

2.1. The layman's perspective

The layman's perspective on property greatly involves itself with the debate on the propertisation of unconventional objects of property, such as body parts and personal data. The laymen's perspective is taken by people with no legal training or

[209] For examples of this terminological confusion in the US discourse see Nadezhda Purtova, "Property Rights in Personal Data: Learning from the American Discourse," *Computer Law & Security Report* 25, no. 6 (2009).

[210] Chapters 5 and 6 give a more detailed description of this debate.

otherwise obtained expert knowledge on the meaning of property in law and sometimes forms a part of the policy discourse as a part of 'property talk'.[211] A defining characteristic of the layman's perspective on property is that, to such an individual, the concept of property means that some 'thing' is 'mine.'[212] More specifically, this statement expresses the two convictions that a layman has about property. The first of these is that 'property' refers to a *thing* (rather than a right or rights), which is often physical. However, since intangible values like a bank account or objects of intellectual property have lately become more common in everyday life, some non-physical items are now also included. Secondly, by stating that some 'thing' is 'mine', a layperson implies that he can do what he pleases with it, including destroying or selling it.

Both convictions have little in common with how property is seen in law. Firstly, to the lawyer, "property" is neither a tangible nor even an intangible "thing".[213] Instead, it is a concept signifying a legal relationship among people with regard to a thing, which is either tangible or intangible. Therefore, unlike the layman, the legal debate recognizes the distinction between property rights and their objects.[214]

Secondly, probably because the layman's perception of property is focused on the thing, an object of a right, rather than the right itself, his discourse often perceives property as an absolute dominion over a thing, and disregards the fact that property, including the power to sell, may be limited. To a lawyer, it is clear that the absolute nature of property is a legal fiction, and a number of legal rules from, e.g. environmental law or the law of tort, limit the freedom of the 'owner' to go about 'his property' in a way that is harmful to a common overriding interest or the rights of third parties.[215]

---

[211] "Property talk is just how we talk about matters of great importance" (Julie Cohen, "Examined Lives: Informational Privacy and the Subject as Object," *Stan. L. R.* 52 (2000)., p. 1378); "Property talk would give privacy rhetoric added support within American culture. If you could get people (in America, at this point in history) to see certain resource as property, then you are 90 percent to your protective goal." (Lawrence Lessig, "Privacy as Property," *Social Research: An International Quarterly of Social Sciences* 69, no. 1 (2002)., p. 255)

[212] John E. Cribbet, Finfley, Roger W., Smith, Ernest E., Dzienkovski, John S., *Property. Cases and Materials*, 9th ed. (New York: Foundation Press, 2008). p. 2

[213] Ibid.

[214] Ibid. p. 2

[215] For examples of the non-absolute nature of property rights in civil law see, e.g. Laurent Aynes, "Property Law " in *Introduction to French Law*, ed. G.A. Bermann, Picard, E. (Austin, Boston, Chicago, New York, the Netherlands: Wolters Kluwer, 2008)., p. 155; in common law - F.H. Lawson, Rudden, B., *The Law of Property*, 3rd ed., Clarendon Law Series (Oxford University Press, 2002)., p. 55

2.2. *Normative perspective*

It is especially important to be aware of the difference between legal property discourse and a philosophical, or normative, debate. The latter, however, only tells us why property should or should not exist, mostly, based on various justice reasons, and how it should be, telling nothing about the actual content of the concept.[216]

For instance, occupation theory assigns property rights to the one who first seizes a thing from its 'natural state'. However, such a standard is difficult to apply to the later stages of social development when all things out there have been already seized for the first time and the cases of, for example, unoccupied land or unutilized wealth are rare.[217]

The natural rights theory regards the existence of private property as a part of the law of nature. However, our perception of what is natural becomes so "ephemeral and mutable"[218] with time that the explanations offered up to describe property matters by the followers of this approach are, just like in occupation theory, hardly satisfactory. Labour theory justifies the assignment of property rights to a creator of a thing, since it is only just to reward his labours. However, it does not provide a justification for the content of vested rights, and nor does it explain why property should exist in land which no human being created. A legal theory of property boils down to the thesis that "whatever is recognized as such by law is rightfully private property."[219] Finally, there is also the theory of social utility, which advocates in favour of the introduction of property rights in cases and of scope that serve a social purpose. In addition, the reader may recall the legal pragmatism approach that this book declared it would stand by in the introductory chapter. Social utility theory is, in fact, similar to legal pragmatism, but also includes the economic theory of law, which dictates the introduction of property rights on the basis of efficiency and will be discussed separately in the following section. Property law tends to follow the normative views accepted in a society and expressed in various philosophical theories of law. Therefore, it is difficult and even undesirable to separate the two. However, property in law only reflects normative views if they have passed through the lawmaking process and received political approval. Therefore, the legal meaning of property continues to be of a distinct nature.

---

[216] Edwin R.A. Seligman, *Principles of Economics* (1905).
[217] Ibid. pp. 131-134, cited in Cribbet, *Property. Cases and Materials*., p. 6
[218] Seligman, *Principles of Economics*.
[219] Ibid.

2.3. Economic perspective

Although the law of property in modern capitalistic states is generally said to follow economic developments and adjust itself to them,[220] it does not mean that the content of property rights in law is identical to the content of property rights as understood by economists. On the contrary, when engaging in a debate on a property-related matter, one should be aware of a significant difference in the perspectives on property taken by the two disciplines.

Firstly, as the previous section explained, the economic approach to property belongs to the class of normative theories. Therefore, when explaining legal phenomena such as property, it focuses on a normative justification for its existence.[221] In the case of economic theory, efficiency is an important criterion guiding social decision-making. The term 'efficiency' refers to a manner of allocation of resources whereby value is maximized.[222] The law also accounts for efficiency, but additionally considers other normative values charshed in a particular society.

Secondly, and quite distinctly from other normative theories, economics does define the content of property rights, albeit differently from how the law regards them. Barzel explains that property rights in economics are "the individual's ability, in expected terms, to consume the good (or the services of the asset) directly or to consume it indirectly through exchange."[223] In that sense, even human rights – in economic terms - are simply part of an individual's property rights. "Human rights may be difficult to protect or to exchange, but so are rights to many other things."[224] In other words, economic proprietary entitlement is the end, whereas "legal rights are the means to achieve the end."[225] The main function of the legal property right is then seen as providing "third-party adjudication and enforcement."[226] Simultaneously, if a holder of an entitlement can actually consume a 'good' in question, the absence of a legal property right in an object does not exclude a de facto existence of an economic property right. Economic property rights, even without the recognition of the law, may also be self-enforced. Unlike property rights in law, their

---

[220] Ibid.

[221] But see an alternative view on the function of economics expressed in Richard A. Posner, *Economic Analysis of Law*, 5th ed. (New York: Aspen Publishers, 1998).: "The task of economics, so defined, is to explore the implications of assuming that man is a rational maximizer of his ends in life, his satisfactions – what we shall call his 'self-interest'." (Posner, *Economic Analysis of Law*., p. 3)

[222] Posner, *Economic Analysis of Law*., p. 13 ("[Efficiency] has limitations as an ethical criterion of social decision making. … [T]he book [Economic analysis of law] does assume that it is an important criterion. In many areas of interest to the economic analysis of law, it is, as we shall see, the main thing that students of public policy do or should worry about.")

[223] Alchian and Allen, *Exchange and Production*, 2nd ed. (1977). p. 114, cited in Barzel, *Economic Analysis of Property Rights*., p. 3

[224] Allen, *Exchange and Production*. p. 114, cited in Barzel, *Economic Analysis of Property Rights*., p. 3

[225] Barzel, *Economic Analysis of Property Rights*., p. 3

[226] Ibid., p. 4

existence is a function "of [people's] own direct efforts at protection, of other people's capture attempts, occasionally of formal and informal non-governmental protection, and of governmental protection effected … through the police and the courts."[227] In other words, when legal property rights are created by the lawmaking process, economic property rights signify one's de facto ability to enjoy a resource that results from an interaction of multiple factors, including the effectiveness of law enforcement and other non-proprietary legal arrangements.

Finally, another way to define economic property rights is by distinguishing a 'property rule' from 'a liability rule.' This is of special significance for this study, since some of the most influential arguments supporting the propertisation of personal data have been based on the distinction between the property and liability rules.[228] The approach was described in the 1972 article by Guido Calabresi and A. Douglas Melamed,[229] and shapes a large part of the US debate on the propertisation of unconventional objects, such as personal data.[230] Property rules, in contrast to liability rules, refer to the circumstance when "an entitlement is protected […] to the extent that someone who wishes to remove the entitlement from its holder must buy it from him in a voluntary transaction in which the value of the entitlement is agreed upon by the seller."[231] On the other hand, "whenever someone may destroy the initial entitlement if he is willing to pay an objectively determined value for it, an entitlement is protected by a liability rule."[232] In other words, property rules ensure that the entitlement is protected, whereas the liability's function is to ensure that the transfer of the entitlement is possible, even without consent of a holder of the entitlement, against objectively determined (often by a court) compensation. Actions in tort are often seen as an embodiment in law of the liability rules.[233] As Lessig puts it, "property protects choice; liability protects transfer."[234] The reader will see later in this chapter that this approach to the meaning of property also has little in common with the meaning of property in law. For instance, in the case of the dispossession of personal property, a remedy in common law is, at the discretion of a wrongdoer, either an order to return the thing itself or a payment representing its market value. Compensation is objectively defined in court, and the remedy in effect validates that the object of the personal property rights has changed hands. In Calabresi and

---

[227] Ibid., p. 4

[228] For more details see Ch. 6

[229] Guido Calabresi, Melamed, A. D., "Property Rules, Liability Rules, and Inalienability: One View of the Cathedral," *Harv. L. Rev.* 85 (1972).

[230] See, for instance, Richard A. Epstein, "A Clear View of the Cathedral: The Dominance of Property Rules," *Yale L.J.* 106 (1997)., p. 2091.

[231] Calabresi & Melamed, p. 1092

[232] Calabresi & Melamed, p. 1092

[233] See e.g. Vera Bergelson, "It's Personal, but Is It Mine? Toward Property Rights in Personal Information," *U.C. Davis L. Rev.* 37 (2003).

[234] Lessig, *Code and Other Laws of Cyberspace*.

Melamed's framework, this means that personal property in law falls under the liability rather than the property rule heading. Like the general economic understanding of property rights, Calabresi and Melamed's model is largely criticized for being far from legal.[235]

This section explained the legal perspective on the debate on the propertisation of personal data by distinguishing it from non-legal outlooks. Each of these perspectives performs its own function: knowledge of the layman's approach is indispensable for understanding what message the introduction of property rights will potentially convey to a wider public; normative perspectives on property focus on the fairness reasons for the introduction of property rights and assigning them in a particular way; and economic theory aims to structure rules in a manner that leads to the most efficient allocation of resources. Each of these outlooks, even though they have undeniable value, is different from the perspective in law. However, the legal perspective is particularly important when the introduction of legal property rights is concerned, having its own independent meaning and implications that should not be disregarded. The next stage of the analysis will, therefore, set out the meaning of property in law.

3. Defining the legal perspective: the meaning of property in law

The preceding section distinguished the legal from the non-legal concepts of property, thus making clear what property in law *is not*. Accordingly, the next step in the analysis is to demonstrate what property in law *is*. This is not a simple task. As Section 3.1 explains, what is meant by property has been determined by various social, political, and economic factors, which vary across time and space. This fluidity is one of the defining characteristics of the concept of property in law, and enables there to be discussions about the propertisation of new and unconventional objects, such as the human body and body parts and virtual objects and personal data. Section 3.2 will narrow the focus of the analysis down to the meaning of property in Europe, since this is the region of interest in this study.

3.1. The fluid nature of property in law

The development of the legal concept of property is a good example of pragmatism in the law; while philosophers of law are occupied with normative justifications of the existence of property, actual property rights address certain practical needs that

[235] See e.g. J.E. Penner, *The Idea of Property in Law* (Clarendon Press, 1997).

have emerged in a particular society.[236] Consequently, a noticeable characteristic of the concept of property is its fluidity; commentators speak of the evolution of property, as well as its flexibility and dynamism in terms of different objects, and the scope of its rights, which vary across time and space and are determined by socio-economic reality.[237]

The range of objects open to property rights is not static. Indeed, as Gray points out, "I may have 'property' in a resource today, but not tomorrow."[238] Equally, the fact that no property rights in an object are recognized at the current time does not necessarily mean that this will not change in the future. Indeed, a few examples of the exclusion and inclusion of objects of property rights, namely the property in human beings, have relatively recently been recognized as immoral[239], while early in the 20th century, Canadian and US laws decreed that "no property rights were to exist in alcoholic beverages."[240] Regular air traffic, as a consequence of technological developments, has also led to the 'shrinking' of the rights in land in English law; if before the advance of aeronautics the holder of the rights in a piece of land was the prima facie owner "of everything reaching up to the very heavens and down to the depth of the earth",[241] to enable air traffic to fly over England, landowners' property rights over airspace had to be limited to control of the "lower stratum", which was essential to the enjoyment of the piece of land itself.[242]

Often, debates on the propertisation of new objects involve a struggle to find a new regulatory solution rather than concentrating on whether certain objects may or may not be subject to property rights. Whether the participants in these debates realize it or not, they talk of property as a legal means to achieving regulatory goals; for instance, when anatomy became a standard medical practice, dead bodies suddenly gained economic value. However, in the absence of legitimate institutional arrangements, the initial source of supply was a group of people known as 'body-snatchers.' These men stole newly buried corpses from their graves, but the absence of a common-law property therein did not enable them to be charged with theft.

---

[236] Gordley, *Foundations of Private Law : Property, Tort, Contract, Unjust Enrichment*.; Kevin Gray, "Property in Thin Air," *Cambridge Law Journal* 50, no. 2 (1991).

[237] J.W. Bruce, Ely, James W. Jr., *Cases and Materials on Modern Property Law*, 6th ed. (Thomson West)., p. 19; Remigius N. Nwabueze, *Biotechnology and the Challenge of Property*, ed. Sheila McLean, Medical Law and Ethics (Aldershot - Burlington: Ashgate, 2007).; Gray, "Property in Thin Air."; Roy Vogt, *Whose Property? The Deepening Conflict between Private Property and Democracy in Canada* (Toronto: University of Toronto Press, 1999)., etc.

[238] Gray, "Property in Thin Air.", p. 296

[239] In the US, the XIII Amendment to the Constitution abolished slavery in 1865; in Eastern Europe slavery gradually began to disappear in the 15th century, but formally ceased to exist in Russia in 1861 (see "Slavery." Wikipedia, at http://en.wikipedia.org/wiki/Slavery).

[240] Arnold S. Weinrib, "Information and Property," *University of Toronto Law Journal* 38 (1988)., p. 121

[241] Gray, "Property in Thin Air.", p. 253

[242] Ibid. p. 254

Accordingly, the government introduced anatomy legislation. Indeed, as Nwabueze suggests, "part of the solution […] is to consider corpses as limited property."[243]

The objects of property rights vary not just across time, but also across jurisdictions; the same things may be treated as property in one country, but not in another. A good illustration is the legal treatment of so-called 'virtual property.' The term broadly refers to commodities in cyberspace, including online equivalents of real world things, as well as e-mail addresses, domain names, and social networking website accounts.[244] At present, online resources are explicitly given property protection in the Republic of Korea and Hong Kong.[245] In the US and Europe, however, the recognition by law of virtual property is only a matter of debate.[246] Similarly, ECJ and English case-law have established that some rights and interests, such as entitlement to milk reference quantities, social security rights, or the rights a tenant has over a leased item, can enjoy the protection of property rights.[247] These same rights and interests are, however, regarded as non-proprietary entitlements elsewhere.

As with the objects that are the subject of legal property rights, the structure and scope thereof also "differ from one society to another, and within the same society from one period to another, because they are historically determined."[248] The scope of property rights in a given country is constantly adapting to the current needs of the jurisdiction in question.[249] A typical example of such adaptation is the increasing state regulation of property.[250] Whether it is country A or country B also makes a difference in terms of the scope of granted property rights. Moral limits on property may also differ across space; two societies may operate under different normative convictions, thereby shaping the two sets of ownership interests

---

[243] Nwabueze, *Biotechnology and the Challenge of Property*., p. 17

[244] See, e.g. Juliet Moringiello, "Towards a System of Estates in Virtual Property " *Int. J. Private Law* 1, no. 1-2 (2008).

[245] All of these jurisdictions passed relevant laws and set precedents in giving criminal sentences to those infringing upon others' virtual property. (e.g., see Joshua Fairfield, "Virtual Property," *Boston University Law Review* 85 (2005).)

[246] Ibid.

[247] Examples of the ECJ case-law: Case 5/88, *Wachauf*, [1989] ECR 2609; Case C-84.95, *Bosphorus*, [1996] ECR I-3953, etc.; on tenants' rights in English law see, e.g. Lawson, *The Law of Property*. p. 81, etc.

[248] Vogt, *Whose Property? The Deepening Conflict between Private Property and Democracy in Canada*., p. 17

[249] Although the rules of the civil law property model are characterized as "hard" and "inflexible," the commentators on continental European property law observe that it also "undergoes an evolutionary and thus gradual change, caused by changing social, economic, cultural and political conditions." (in Sjef Van Erp, "Security Interests: A Secure Start for the Development of European Property Law," *Maastricht University Faculty of Law Working Papers* (2008)., p. 16, also in print: ———, "Security Interests: A Secure Start for the Development of European Property Law," in *Sicherungsrechte an Immobilien in Europa*, ed. Hinteregger M. and Boric T. (Vienna/Berlin: Lit Verlag, 2009).

[250] Think of, e.g. gun laws, changing registration requirements in land law, etc.

differently.[251] It was public policy considerations that prevented the court from vesting in Mr Moor a property right over his spleen,[252] while a court in another country could have operated a different policy, leading to another outcome and a property right over a human body parts. As long as property rights are enforced by the state, their scope and what they cover are political, and thus depend on the political environment in a particular nation.[253]

What property is varies a great deal depending on whether a particular country utilizes the Anglo-Saxon legal tradition or has adopted a Continental legal system. To say that X has a property right in his house in a country with the latter approach would probably mean that X has full ownership of his home, i.e. with some limitations, he can possess it, enjoy it by living there himself or renting it out, or, ultimately, sell or otherwise alienate it. To those more familiar with the Anglo-Saxon legal lexicon, the same statement would not convey the same message. Firstly, in English law the term 'land law' rather than property law is used with regard to realty.[254] Secondly, a characteristic trait of the Anglo-Saxon approach to property is the so-called 'fragmentation of ownership.' This means that, as well as ownership in the fullest sense – 'fee simple' in English land law vocabulary - other property rights can exist in the same object, such as the rights of a tenant or the lessees of land.[255] Ownership in the Anglo-Saxon legal tradition "can involve very different combinations of [the] constituent parts."[256] Such a system of property rights is often described with the metaphor of a 'bundle of rights.' The complete bundle represents full ownership, with each element or 'stick' within it representing one of the many 'fragments' comprising full ownership, for example, the right to use a resource and the right to use it for a fixed period of time, which is conditional upon the fulfilment of an obligation or is unconditional. Each 'stick' can be retained in the bundle or held independently. As a result, there may be more than one person holding different property rights over the same object.[257]

---

[251] Human rights considerations may serve as moral limitations on property rights: "'Property' in a resource stops where the infringement of more basic human rights and freedoms begins." (Gray, "Property in Thin Air.", p. 294)

[252] *Moore v. Regents of the University of California* (51 Cal. 3d 120; 271 Cal. Rptr. 146; 793 P.2d 479)

[253]The idea of property as a political institution appears in Jeremy Bentham, "Security and Equality of Property," in *Property: Mainstream and Critical Positions*, ed. C.B. Macpherson (Toronto: University of Toronto Press, 1978), Gray, "Property in Thin Air."; Nwabueze talks about property rights reflecting the expectations of the members of a given society as expressed by its political system. Nwabueze, *Biotechnology and the Challenge of Property*. E.g. p. 25

[254] Lawson, *The Law of Property*.

[255] Ibid., starting on p. 90

[256] Weinrib, "Information and Property.", p. 121

[257] Section 3.2 of this chapter will focus on the distinction between the common and Continental law systems of property.

Nwabueze suggests that the 'bundle of rights' approach to the common law institution of property is the key to its inclusive nature,[258] meaning that the boundaries of property in the Anglo-Saxon legal tradition (possible objects and the content of property rights) "are still to be explored."[259] This does not, however, mean that boundaries, in terms of what can be a property right, both in the Continental and the common law systems, do not exist. Under a so-called principle of *numerus clausus*, parties are not free to create previously non-existing property rights at will.[260] The application of this principle in the Continental approach is quite strict, although the degree of rigour with which it is applied varies from country to country.[261] In English law, however, as, for example, Akkermans concludes, although property law is not completely inclusive and the *numerus clausus* principle does apply, the courts are more willing to recognize new property rights than their counterparts in the continent of Europe.[262]

The more inclusive than exclusive nature of the common law approach to property makes it more susceptible to the inclusion of new objects and rights than is the case elsewhere in Europe. However, as the subsequent sections of this chapter will reveal, the fragmentation of ownership has also touched property institutions in continental Europe, while legal thinking there is not so different from talk (using property vocabulary) about unconventional property objects like welfare entitlement or personal data.

To summarize, the concept of property in law is flexible. Accordingly, and provided that it serves the current needs of a jurisdiction and there is political will to transform it, there is nothing in the nature of the legal phenomenon of property to prevent it from changing to include personal data as one of its objects.

3.2 The idea of common European property law, new property rights and their objects

As the preceding section demonstrated, the substance of property in law is not easy to capture in a rigid definition that is valid across time and space. This section attempts to overcome this obstacle and define property in Europe by focusing on a common denominator rather than on differences between the various national property laws. It will be argued that, despite perceived differences between national

---

[258] Nwabueze, *Biotechnology and the Challenge of Property*. P. 9

[259] See Charles A. Reich, "The New Property," *Yale L.J.* 73 (1964).; the common law property framework is used for the analysis of many relationships, as well as unconventional objects of property such as race, social security entitlements, etc. Nwabueze, *Biotechnology and the Challenge of Property*.

[260] Bram Akkermans, *The Principle of Numerus Clausus in European Property Law* (Antwerp - Oxford - Portland: Intersentia, 2008)., p. 19

[261] Ibid.

[262] Ibid., p. 389 et seq.

property regimes, common principles, as well as recent developments in modern property law in some member states and at the EU level, suggest that the formation of a common European property law is not far away. These principles and developments, if not pointing to the possibility of the unification of property law, at the very least enable a common discussion on property matters in Europe, including about new property rights and objects such as personal data. Let us start with the differences.

Narrowing the focus of the study down to the meaning of property in Europe reduces the number of national jurisdictions one needs to consider, and makes the task of defining property in a limited number of judicatures easier than searching for a universal definition. It does not, however, completely solve the problem of the lack of a common European definition of property. Each European member state traditionally determines the scope and regime of property rights independently.[263] Moreover, purely national differences in defining and dealing with property, which is the main division between national property laws, lies in the separation between common and civil law systems, the latter of which splits into four groups originating from French, German, Scandinavian and socialist law. The characteristic elements of each national approach to property law are undoubtedly of great interest for a comparative study, but go far beyond the scope of this book. So, for the purposes of the present study, it will be enough to focus on the more general differences between the common and the civil law, and these will be illustrated by examples from national legal systems.

3.2.1 Civil law property

a. Revolutionary origins and codes as sources

Both the civil and common law systems of property have their roots in medieval European feudalism, but developed differently after the revolutionary changes at the end of the 18th and the beginning of the 19th centuries.[264] Under the feudal system, everyone was bound by their status in the society's hierarchy of "reciprocal obligations of service and defense",[265] which were tied to land; the landlord guaranteed the possession of the land by the vassal and the fair resolution of disputes. In return, and on the basis of an agreement, the vassal owed the lord a service known as a 'tenure', with different types of tenures representing the ways the

[263] Property law traditionally lies within the national rather than the international domain.
[264] Sjef Van Erp, "From "Classical" To Modern European Property Law?," *Maastricht University Faculty of Law Working Papers* (2009). p. 7, also in print: ———, "From 'Classical' to Modern European Property Law?," in *Essays in Honours of Konstantinos D. Kerameus/Festschrift Für Konstantinos D. Kerameus* (Athens/Brussels: Ant. N. Sakkoulas/Bruylant, 2009).
[265] Bryan A. Garner, ed. *Black's Law Dictionary*, 9th ed. (West,2009)., p. 698 ("Feudalism")

vassals held property in land.[266] The king provided land to aristocrats, and they in turn provided it to smaller vassals. The more powerful vassals were able to secure the inheritance of their tenure and, consequently, wealth and political weight. The vassal's service included implied military aid, the payment of a tax. In case of serfs (peasants who were in the lowest position in the social hierarchy), the service implied a condition of bondage to the land, which was a restriction on personal freedom that resembled slavery.

The civil, or Continental, property law system as we know it today in the overwhelming majority of EU member states, originates from the ruins of feudalism. More precisely, it rests on the notions of freedom and equality of the 1789–1799 French Revolution and its rejection of any special treatment based on status in society. As van Erp suggests, a force behind the formation of the Continental system of property law was a desire to do away with feudal duties and a personal lack of freedom by eliminating the bondage types of relationships based on the possession of land.[267] The rejection of the old feudal rules led to the 'rediscovery' of Roman law as a basis for a new approach to property. This was further developed in European universities and written down in codes.[268] As a result, and regardless of national differences, modern civil law jurisdictions share two common pillars: the strong influence of Roman law and "a resulting 'classical system' of property."[269]

b. Structure and scope: unitary ownership

Developed to counteract the pillars of the feudal system, the classical model of property law was built to prevent the formation of property rights and feudal duties at will. Consequently, there is a distinctive feature of the classical model - a strong separation between the laws of property and contract, namely real and personal rights respectively. The division follows a blueprint laid down in Roman law - the terms 'real' (*in rem*) and 'personal' (*in personam*) originate from the Institutes of Justinian.[270] Rights *in rem* are rights in the thing itself, protected against everyone, whereas personal rights only exist between particular individuals and are enforceable only between them. The parties are generally free to create new forms of personal rights at will. On the other hand, the number and scope of real rights are established by law, and the parties involved are not free to modify their character.[271] The latter is known as a principle of *numerus clausus* and, in other words, provides

---

[266] Ibid.
[267] Van Erp, "From "Classical" To Modern European Property Law?.", p. 7
[268] Ibid., p. 6
[269] Akkermans, *The Principle of Numerus Clausus in European Property Law*., p. 10
[270] E.J.H. Schrage, "Property from Bartolus to the New Dutch Civil Code of 1992," in *Property Law on the Threshold of the 21st Century*, ed. G.E. van Maanen, van der Walt, A.J. (Antwerpen-Apeldoorn: MAKLU Uitgevers, 1996)., p. 41
[271] Ibid., p. 39

that parties are not free to create previously, non-existent property rights at will.[272] As a result, it is no surprise that the Continental property law approach is traditionally perceived as a system of "hard and fast inflexible rules."[273]

Another defining characteristic of the civil law property system is its reliance on a unitary right of ownership. Ownership is often spoken of as "the most comprehensive right possible,"[274] which is, in principle, exclusive, unlimited and perpetual.[275] Under the French Civil Code, ownership implies "the right to enjoy complete mastery over a thing,"[276] and "a legal prerogative, indeed the most extensive prerogative there is."[277] The scope of this most extensive right is captured in the Latin formula *usus, fructus* and *abusus* (see e.g. Article 544 French CC).[278] In French law, an influential instance of civil law, *usus* (the right of usage) includes the right to exploit, inhabit or otherwise "enslave" a thing as a commodity, or, in contrast, not to use it. *Fructus* means the prerogative to collect 'the fruits' of a thing, which are either produced by it naturally or legally (e.g. the fruit of an apple tree or interest on money), and which become the property of the owner. The owner can decide whether and how to produce the fruits, e.g. whether to inhabit an apartment personally or rent it out. Finally, *abusus* stands for a prerogative to dispose of a thing, i.e. to modify its structure or even destroy it physically or legally (e.g. by alienation). Aynes explains that, although significantly limited, *inter alia* by environmental law and the law of land usage, etc., "the right to dispose still remains the most significant aspect of the owner's prerogatives."[279]

Ownership is also said to be exclusive, unlimited and perpetual.[280] Exclusivity means that the owner, as the holder of a real right, has an absolute right to prevent other, indefinite numbers of people from enjoying the thing owned unless they are authorized to do so. This is also known as the *erga omnes* effect (or effect against everyone else). Ownership is unlimited because the owner is, in principle, a holder of a full dominion over his thing and entitled to do what he pleases with it without having to show a legitimate interest. However, the dominium is not absolute, since, firstly, the owner can be held liable (sometimes strictly liable) for damage caused to a third party by the use of his thing, e.g. in the case of 'abnormal neighbourhood disturbances' (*'troubles anormaux de voisinage'*). Secondly, the freedom to do what one pleases with property is limited by the theory of the abuse of rights (*'abus de droits'*),

---

[272] Akkermans, *The Principle of Numerus Clausus in European Property Law*. P. 19
[273] Van Erp, "From "Classical" To Modern European Property Law?.", p. 16
[274] Ibid.
[275] Aynes, "Property Law "., p. 154
[276] Ibid., p. 152
[277] Ibid.
[278] Ibid.
[279] Ibid. p. 153
[280] Ibid. p. 154

which deals with circumstances in which the owner seeks to harm others. Ownership is perpetual because it lasts for an indefinite period of time.[281]

The attribute of civil law ownership that is most interesting for the purposes of this study is its unitary nature. Created in reaction to the feudal system of the possession of land, where a king was the formal owner of the land in the entire country and divided his dominium rights among his vassals to ensure their allegiance, ownership is now said to be a unitary right because, theoretically, it cannot be divided, except in the case of co-ownership. It is for this reason that it is often – albeit erroneously – perceived as the only property right in Continental law. In principle, creating property in an object by implying a right as extensive as Continental law ownership means the widest, and sometimes undesirable and fully transferable, degree of control over a resource. This may explain why the Continental approach to extending property rights to cover new objects like personal data is conservative and hesitant.

Given the relative rigidity of the classical property model, in Continental law it may seem to be more appropriate to use the singular term 'property right' instead of the plural, 'property rights', since the anti-feudal roots of the system are, in principle, hostile towards any division of the unitary rights of ownership. However, the reality of use of wealth already on the stage of formation of the classical model of property and even more now often involves multiple economic interests in one object. To accommodate these interests the model, as well as the main ownership right, the classical model also includes some 'lesser' or accessory property rights, which are the result of the disentanglement of the three ownership prerogatives, but which are still enforceable against an indefinite number of people. Yet, to be recognized as interests of a proprietary nature, and to consequently enjoy proprietary status, the lesser rights in the classical property model must comply with two "leading principles of property law" or 'filters', as Van Erp describes them:[282] the *numerus clausus* principle, i.e. the rights have to be on the list of property rights recognized as such by law, and their content cannot be modified at all, or can only be modified a little; and the principle of transparency, i.e. the rights have to be made public, either by registration (in the case of immovable property) or possession (in the case of immovable objects).[283]

The examples of such 'lesser' or 'accessory' property rights in French law include, but are not limited to, usufruct (or *usufruit*), which is a restricted and temporary property right to use (*usus*) and enjoy the fruits (*fructus*) of a thing 'owned' by another (who may be known by the name of *nu-propriétaire* or 'base owner'). This works "as if the right of ownership has been split between two

[281] Ibid. p. 155
[282] Van Erp, "From "Classical" To Modern European Property Law?.", p. 10
[283] Ibid.

different persons." [284] The right of usage gives its beneficiary a 'real' right to use the thing owned by another, for example to inhabit a rented apartment, but does not include the right to collect its fruits (e.g. sublet) or alienate it. [285] A servitude or easement (Article 637 of the French Civil Code) is "a real right that is accessory to a piece of real property and which burdens another piece of real property." [286] In essence, it represents a burden imposed on real property, like a piece of land, for the benefit of another piece of property, like a building, e.g. a right of way on the property of another, or a right to prevent the construction of buildings on a neighbouring property in order to safeguard a view[287] (known in common law as a restrictive covenant[288]).

The inter-relationship between ownership and 'lesser' rights is governed by certain ground rules. Briefly: one cannot transfer more rights than one has and deny the title to the owner (*nemo dat*); the previously established property right has priority over subsequent rights, except for the right of ownership itself (*prior tempore*); and the 'lesser' rights have priority over the fuller rights, i.e. they limit the right of ownership and are enforceable against the owner, as well as against the rest of the world.[289]

c. The rigid application of the *numerus clausus* principle resulting in an exclusive system of property rights

Despite the exceptions to the non-fragmentation approach to ownership in civil law countries, the transitions from contractual to property rights can only be made after an amendment to a civil code, which, due to both the underlying ideology and rigid doctrine of civil law, and partly due to the resistance of the legal elites, does not happen often. One of the more recent examples is the 19th February 2007 statutory introduction in France of a general institution of fiduciary ownership (*propriété fiduciare*), thereby amending Arts 2011 and 2031 of the Civil Code. Fiduciary ownership is temporary, and purposive ownership is created to secure a credit or enable a trustee to manage a patrimony. [290] The German Civil Code, on the other hand, holds on much more strongly to the separation between contract and property, and yet, also accepts few 'lesser' rights.[291]

In addition, the top-down reasoning of Continental law, which first relies on a general rule of statute, does not allow the backdoor use of the law of tort to extend the list of property rights through civil litigation. An example of such an attempt can

[284] Aynes, "Property Law "., p. 165
[285] Ibid.
[286] Ibid., p. 167
[287] Ibid., p. 167
[288] Lawson, *The Law of Property*., p. 122
[289] Van Erp, "From "Classical" To Modern European Property Law?.", p. 11
[290] Aynes, "Property Law "., pp. 161-162
[291] Akkermans, *The Principle of Numerus Clausus in European Property Law*., p. 19

be found in Dutch law, which has been influenced by both French and German traditions. Van Erp cites two cases. The first is the 1905 decision of the Netherlands Supreme Court in *Blaauboer v. Berlips*,[292] which held that "the law of property and contract are of such different nature that they should be distinguished with great care" and that "the separation between the law of property and the law of contract cannot be circumvented by the use of tort law."[293] The second case is the 1985 *Boyé* decision of the Supreme Court, which dealt with the law of the Dutch Antilles.[294] The Boyé family were an original beneficiary of a contractual clause entitling them to receive part of the proceeds from a plantation. Under the original contract of sale of the land, the clause had to be included in each subsequent contract of sale, with the purpose being to establish a ground rent. The last contract did not, however, contain this provision, and the Island of Curaçao, the new owner of the plot, refused to comply with it. The Boyé family, therefore, sued the Island and based their claim on the tort of negligence. The court ruled that "although a tort claim was possible, courts had to be very careful in their analysis. In particular courts had to avoid giving proprietary effect to a clause that was of a contractual nature." [295] In van Erp's interpretation, "the Court refused to bypass the *numerus clausus* principle by only allowing the enforcement of contractual clauses vis-à-vis third parties under tort law within strict limits."[296] In other words, it is contrary to the nature of civil law to recognize a proprietary interest on the ground that it receives protection. In contrast, an interest benefits from an *erga omnes* effect, and is protected against the entire world, only after it has been recognized as proprietary by law.

Unitary ownership, the strict application of the *numerus clausus* principle, and the related impotence of the courts to create new property rights make the Continental law of property a relatively exclusive system, although the degree of rigour applied in guarding the frontiers of traditional property rights differs across jurisdictions.[297]

3.2.2. Property in the Common law

a. Feudal origins and sources in case law

Unlike in countries of the continental Europe, in England – the mother jurisdiction of common law - the feudal system of land ownership was not immediately ended by a revolution, but instead underwent several gradual changes which continued throughout the 20th century. As a result, the feudal system still forms, in Elizabeth

[292] Hoge Raad 3 March 1905, Weekblad van het Recht 1905, no. 8191
[293] Van Erp, "From "Classical" To Modern European Property Law?.", p. 9
[294] Hoge Raad 17 May 1985, Nederlandse Jurisprudentie 1986, 760 (*Eilandgebied Curaçao v. Erven Boyé*).
[295] Van Erp, "From "Classical" To Modern European Property Law?.", p. 9
[296] Ibid.
[297] Akkermans, *The Principle of Numerus Clausus in European Property Law*.

Cooke's words, the "mental furniture"[298] of the law of property in England, Wales and Northern Ireland and has practical effects.[299] Although this chapter focuses on European property discourse, for the sake of the analysis of the American propertisation argument in the subsequent chapters, it worth mentioning that the US, as a former British colony, inherited the colonial property law approach and now operates with roughly the same logic and terminology, but in a more archaic manner. The modernization of English property law, also the reforms of land law, no longer had any effect on US soil after independence.

Unlike the civil law system of property, which was laid down in codes, English property law mainly consists of case-law decided in the common law courts, which is amended by the case-law of the courts of equity,[300] as well as by statutes, e.g. the Land Registration Act of 2002, all of which reformed the system of land law.[301] The role the statutes play is not, however, comparable to the French or German Civil Codes, since "the legislature has never attempted to set [property rules] out in a coherent structure."[302] For instance, although the 1922 Law of Property Act and subsequent real property statutes of 1925 were meant to harmonize "the law of real and personal estate" (i.e. property in immovables and movables), it still sounds odd to a Continental legal ear that the systems of land law ('real property') and property in chattels, i.e. other objects ('personal property'), are independent and quite different.[303] The system of land law is more reminiscent of the old feudal structure of land possession and is subject to the fragmentation of ownership. It is, as a result, quite distinct from the classical model of property law in Continental Europe; personal property law is an independent branch of the law, although it also knows fragmented ownership and is, therefore, comparable to land law.

b. Structure and scope: fragmented ownership

To avoid further confusion, the dichotomy of 'real' vs. 'personal' appears twice in English law. As just mentioned above, the first reference is to real and personal property, while the second occasion relates to the separation between real and personal rights. The first distinction came from the kinds of remedies available to someone whose property was wrongfully taken from them. In the case of land, the action was aimed at the thing itself, i.e. the lawful holder was entitled to get the thing back (in Latin, *res*), hence the term 'real property'. In the case of chattels, any legal action was personal, i.e. against a wrongdoer who had a choice either to return the

[298] Elizabeth Cooke, *Land Law* (Oxford: Oxford University Press, 2006)., p. 13
[299] Van Erp, "From "Classical" To Modern European Property Law?.", p. 6; Cooke, *Land Law*., p. 13
[300] The division between common law and equity relates to the division of jurisdictions; common law and equity effectively represent two independent legal systems, but the same court may act on different matters both in a common law court and a court of equity capacity.
[301] Lawson, *The Law of Property*., p. 12
[302] Ibid.
[303] Ibid., p. 12

thing in question or pay its value, hence the term 'personal property'.[304] In contrast, the real vs. personal rights' dichotomy builds on the same principles as in Continental law, i.e. real rights have an *erga omnes* effect, whereas personal rights are only enforceable against the parties to a contract. The *numerus clausus* principle secures the separation. Accordingly, the term 'real rights' applies to any type of property, whether real or personal.

The quality that remains from the feudal origins of land law, and which distinguishes the common law approach to property from its Continental counterpart, is the lack of the concept of unitary ownership. This conveys two messages. Firstly, the use of the term 'ownership' is questionable in itself. Some authors reject the use of the word altogether,[305] since "no subject can in the technical sense own land, even though he has the exclusive benefit of it, since only the sovereign can own land and all others hold it of him."[306] Others regard the rejection as "meaningless and indeed inaccurate,"[307] since the word indicates the fullest property right that there is, and rejecting the existence of such a right is not convincing. Meanwhile, yet a third group of authors uses the term 'ownership' to refer to all types of estates in land.[308] Like in the civil law, the common law 'ownership' is the widest in scope among property rights and consists of many disparate claims against an indefinite number of persons.

The second and most important message is that 'ownership' in the common law is not unitary but fragmented. Fragmentation is important as it defines the system of property rights in common law. It means that, firstly, the law sanctions more than one person having property claims at the same time. That is why the allegory often used to describe common law 'ownership' is a "bundle of sticks."[309] In effect, the complete bundle represents full ownership and each 'stick' in the bundle represents one of its many 'fragments', for example, the right to use a resource and the right to use it for a fixed period of time, whether conditionally or unconditionally. The 'lesser' property rights, which are limited in time, are in turn known as 'estates' or 'titles'.[310] The second consequence of fragmentation is that holding an estate does not necessarily include enjoyment of the complete set of prerogatives that are characteristic of Continental ownership (*usus, fructus* and *abusus*).

The American approach to land law still retains an archaic system of estates, consisting of freehold (originating from feudal estates held by a free man) and non-

---

[304] Ibid., p. 13; see also Schrage, "Property from Bartolus to the New Dutch Civil Code of 1992.", p. 41
[305] W.J. Swadling, "Property: General Principles," in *English Private Law*, ed. P. Birks (Oxford: Oxford University Press, 2007).
[306] Schrage, "Property from Bartolus to the New Dutch Civil Code of 1992.", p. 43
[307] Ibid.
[308] E.g. Cooke, *Land Law*., p. 13
[309] Cribbet, *Property. Cases and Materials*., p. 2
[310] Lawson, *The Law of Property*., p. 15

freehold estates which, in US land law, have been transformed into leases.[311] Freehold land can be held either perpetually and unconditionally, with the opportunity to alienate and inherit it (fee simple absolute), or conditionally, with a view to accommodating a wish to transfer property, while retaining a measure of control over its use (defeasible fees), or guaranteeing that with the holder's death the land passes intact to the next generation (fee tail), or is, alternatively, held until the death of the holder of the estate (life estate).[312] These estates co-exist, and can each be treated as the object of property, as "each can be sold, mortgaged, given away, reached by creditors, and so on." [313]

In modern English law, all of these estates, except for fee simple absolute (now simply known as freehold) have lost their significance and were abolished in the course of reforms. As well as freehold, a lease, although it was outside of the feudal system, is now also regarded as an estate, despite its combined property and contractual nature.

Fee simple absolute would be an equivalent to civil law ownership of land, since it is the largest estate and lasts forever, in principle denoting the privileges of *usus, fructus,* and *abusus*, and may also be conveyed to any transferee.[314] Interestingly, even someone who is holding another's property wrongfully or 'adversely' (e.g. squatting) in relation to the rest of the world may be said to have a fee simple absolute. This is because this right is protected against interference from an unidentifiable number of people, and may last forever, be alienated, inherited and reached by creditors, unless the holder of the estate is evicted by the rightful holder of the stronger title.[315]

A remarkable manifestation of the fragmentation of ownership is that fee simple absolute, just like any other estate, does not always include the rights to benefit from the fruits of the object of property, or destroy or alienate it. Under the law of trusts, a trustee may be a holder of a fee simple absolute, but is only able to exercise the ownership privileges necessary to carry out his functions as trustee, i.e. manage the property for the benefit of another person or a charity, but not sell it. Moreover, the trustee's creditors cannot reach such an estate.[316]

The leasehold status enables an individual to hold land "for a period which is certain or capable, by notice to quit, of being made certain, and is a form of landholding".[317] This firstly implies the existence of a freehold, as every lessee has a landlord. Secondly, the lessee's privileges of usus, fructus and abusus are limited in

---

[311] Ibid., pp. 79-80
[312] Bruce, *Cases and Materials on Modern Property Law*., pp. 215-227
[313] Lawson, *The Law of Property*., pp. 79-80
[314] Ibid., p. 101
[315] Ibid., p. 80
[316] Ibid.
[317] Ibid., p. 101

time; since a lease is only valid for a certain period, it will eventually expire and possession will return to the landlord. Thirdly, the existence of a lease denotes the simultaneous presence of more than one rightful holder of an entitlement in a piece of property, namely a freehold, a lease and possibly a sub-lease, which is an excellent illustration of fragmented ownership in land. Finally, although a lease can be transferred, a lessee can only transfer to another the rights that he has, and no more. In other words, the lessee cannot create a sub-lease with wider rights than those contained in his own lease or for a longer term than the unexpired period of the lease. [318]

Along with the freehold and the lease, there are also the 'accessory' property rights of easements and covenants, which are, in substance, equivalent to servitudes. These are linked to an object of real property, like a plot of land or a building, and denote rights to use a neighbouring property (e.g. a right of way) or to restrict the use of another's property (e.g. prescribing that it is not possible to build on a plot of land to preserve a pleasure garden – a restrictive covenant).[319]

The fragmentation of ownership is also known to the system of personal property. Although terms of ownership and possession are used, the expression 'bailment' describes the relationship where a thing is owned by one person but legally possessed by another.[320] The logic, which is similar to that of estates, structures the interests of a bailee and bailor. Similar to the law relating to leases, bailment is a mixture of property and contractual relationships.[321] The bailment originates in an agreement between parties and confers on the bailee a 'special property' in the chattel for a limited period of time, while the bailor has 'the general property'. The interest of the bailee has the *erga omnes* effect, since it is protected from trespass and, in the case of wrongful dispossession, the bailee is entitled to recover the object or its value.[322] As Lawson and Rudden conclude, "there is little to differentiate in principle a bailment of a chattel for a period from a lease of land."[323]

---

[318] Ibid., p. 101

[319] Cooke, *Land Law*., p. 27

[320] Lawson, *The Law of Property*., p. 115

[321] Swadling, "Property: General Principles."; Akkermans, *The Principle of Numerus Clausus in European Property Law*., p. 391 citing: "In personal property law the courts have also been reluctant to recognize new property rights at law. This is best illustrated when returning to bailment. […] Bailment does not create a property right as such. A personal right granting possession does not make it into a property right just because of that. […] in general, the relationship between bailor and bailee remains personal."

[322] Lawson, *The Law of Property*., p. 81

[323] Ibid. p. 81; an important difference between the lease and bailment is that "the lessee of land is protected, for the whole period of the lease, against the lessor's successor – someone, for instance, who bought out the lessor. Such a person cannot evict the tenant. […] But in the case of a chattel, a buyer from the bailor could oust the bailee during the period of the bailment, leaving him to a contract claim against the bailor. There is, however, little judicial and no statutory authority for this; in the case of ships, there is case-law against it." But see Swadling who disagrees with the qualification of bailment as a property right. (W.J. Swadling, "Property: General Principles," in *English Private Law*, ed. P. Birks (Oxford: Oxford University Press, 2000).)

c. The flexible application of the *numerus clausus* principle and the resulting inclusive system of property rights

Despite the fragmentation of ownership, the list of interests regarded as real or property rights is not endless. Similar to the Continental law system, in common law the transition from the status of a contractual right to a property right is not without limits. The principle of *numerus clausus* secures the separation between the two types of rights, and provides that parties are not free to create previously non-existing property rights at will.[324]

However, the manner of the application of the *numerus clausus* principle in English law is quite different from the Continental system, although some Continental law jurisdictions are more open than others to the accommodation of new economic realities by recognizing new property rights. Nevertheless, Continental property law traditionally still relies on the presumption of the exclusivity of property rights. In contrast, in English land law, and originating from fragmented feudal land ownership, the list of property rights is more inclusive, and the creation of new property rights is, in comparison to the Continental system, less difficult.

Legal literature often takes the position that before a right is admitted into a category of property rights, it has to satisfy a number of criteria, just as in the Continental law approach. According to Lawson and Rudden, the right must: be alienable; die when the object perishes, or until that time take effect against an indefinite number of persons (*erga omnes* effect); and be reachable by its holder's creditors or, when the holder of the thing itself is bankrupt, enable the holder of the real right to remove the protected interest from the bankruptcy.[325] There is no statute that establishes these criteria or governs their application. Moreover, there is no agreement in the legal doctrine as to the exact list of criteria.[326] The recognition of new property rights and the requirements that the interests in question have to meet are, in essence, left to the English courts,[327] which have acted accordingly on numerous occasions, albeit more often acting as the courts of equity than the courts of common law.[328] For instance, a restrictive covenant was recognized as a property right by a court in equity. In *National Provincial Bank v Ainsworth*, the House of Lords

---

[324] Akkermans, *The Principle of Numerus Clausus in European Property Law*., p. 19

[325] Lawson, *The Law of Property*., p. 14

[326] See, e.g. Gray, "Property in Thin Air." Gray argues that the presence of the *erga omnes* effect is sufficient for a new property right to emerge.

[327] See, e.g. Akkermans, *The Principle of Numerus Clausus in European Property Law*., p 393, citing Swadling, *Property: General Principles*, p. 225

[328] The distinction has to do with the different sources of the English land law - common law and equity. Equity is a set of principles which application in the interest of natural law justice is considered to mitigate the outcome achieved or which would be achieved according to the rules of common law. When a court considers a claim in equity it acts as a court of equity; when the claim is considered under the common law, the same court is acting as a court of common law.

considered whether the right of an abandoned wife to live in the matrimonial home was of proprietary nature. The question arose when the bank tried to evict the woman from the house, which the husband had used as security for his debts, which he was unable to pay. The issue was whether the wife's interest was binding on the creditor and, therefore, constituted a real right. Lord Hodson looked at existing property rights in land and, as the interest in question was not amongst these, answered the question negatively. The presumption behind this ruling is that the line between real and personal rights is unambiguous, and a right is not of a proprietary nature unless it has previously been established as such. Lord Wilberforce, however, proffered a different explanation:

> *On any division, then, which is to be made between property rights on the one hand, and personal rights on the other hand, however broad or penumbral the separating band between these two kinds of rights may be, there can be little doubt where the wife's rights fall. Before a right or an interest can be admitted into the category of property, or of a right affecting property, it must be definable, identifiable by third parties, capable in its nature of assumption by third parties, and have some degree of permanence or stability. The wife's right has none of these qualities, it is characterised by the reverse of them.*[329]

In his judgment, in essence, Lord Wilberforce made two important points: first, the border between real and personal rights is not as clear-cut as, e.g. the opinion of Lord Hodson suggests, and the transition is possible; second, similar to the position often taken in legal writing, e.g. by Lawson and Rudden in the previous paragraph, for this transition to take place the right in question should satisfy a number of requirements. However, the approach of the courts to the admission of new property rights is even more vague as, according to Swadling, "Lord Wilberforce's criteria have not since been followed, not even in cases where the court considered the possible existence of a new property right."[330]

In addition, unlike in the Continental law system, where protection in tort law cannot be used as a backdoor way of creating a new real right, it is not always clear in English law whether the elements required of the right in question are, in fact, the preconditions of it being considered a real right, or the effect. This is partly the result of a legal technique that is characteristic to common law, where, as Gray puts it, "property resonates in dialogue of trespass and nuisance (torts)."[331] Hamilton and Till share the view that "it is incorrect to say that the judiciary protected property;

---

[329] *National Provincial Bank Ltd v Ainsworth* [1965] AC 1175, HL at 1247-1248 per Lord Wilberforce.
[330] Swadling, "Property: General Principles.", p. 225, 242-243
[331] Gray, "Property in Thin Air." p. 266

rather they called that property to which they accorded protection."[332] In particular, when it comes to the application of the *erga omnes* effect to new property rights, Gray expresses the opinion that a right is often recognized as being of a proprietary nature "not because property is the basis upon which that protection is given, but because 'of the effect of that protection.'"[333] In other words, when considering claims of the existence of new property rights, the English courts are known in some cases to employ reverse reasoning, basing a conclusion on the proprietary nature of the interest in question on its (desirable) protection against the world, rather than granting *erga omnes* protection based on property status. This reverse approach makes the application of the *numerus clausus* principle even more ambiguous and, thus, less strict.

The fragmentation of ownership, in terms of disentangling the ownership prerogatives of *usus, fructus* and *abusus* and the less rigid application of *numerus clausus*, make, at least in theory, property in the common law approach a relatively inclusive system, which is open to talk of new property rights in unconventional objects such as personal data.

3.2.3. In search of common ground: fragmented ownership and the erga omnes effect

When it comes to flexibility and openness to new property rights, the reader may have noticed that the examples are primarily from common law jurisdictions, whereas Continental law is, in theory, resistant to new developments. Given the systematic differences between common and Continental property law, the terminological disagreements, and a possible degree of refusal by local legal elites to accept the 'contamination' of their national legal systems, one may wonder if a common European discussion on matters of property, such as the propertisation of personal data, is possible, or even makes sense. It will, however, be demonstrated here that some common principles of property, along with the recent developments in modern property law in some EU member states and at the EU level, if not pointing to the possibility of the unification of property law, do, at the very least, enable a common discussion on property matters in Europe, including about property rights in new objects such as personal data.

It became clear from the earlier analysis that fragmented ownership and the less rigid approach to the application of the *numerus clausus* principle are the key to flexibility when it comes to property in common law countries, enabling the adoption of new property rights and the propertisation of new objects. Briefly, the phenomenon of fragmentation makes property flexible. This is firstly because it

---

[332] Hamilton & Till, "Property," *Ency. Soc. Sci.* , no. 12 (1933). cited in John E. Cribbet, "Concepts in Transition: The Search for a New Definition of Property," *U. Ill. Law Rev.*, no. 1 (1986). P. 4

[333] Gray, "Property in Thin Air.", p. 301

enables the transfer of resources without the necessity for the original proprietor to completely surrender all control over them, which may not be a desirable option regarding some resources. Secondly, fragmentation implies that property does not always mean that an individual has complete control over a resource, which may also be undesirable in terms of some objects. In the common law, property rights that are narrower in scope than complete ownership receive the same protection against third parties. Simultaneously, and in the meaning of the classical model, the existence of property rights in an object always implies the fullest possible control over the resource. Accordingly, the propertisation of any object, especially one as unconventional as personal data, has greater implications and is harder to accept in Continental than in common law.

Each 'stick' can be maintained in the bundle or, potentially, after passing the *numerus clausus* filter, be held independently. As a result, there may be more than one person holding different property rights over the same object. By assigning property rights of various scopes (and the corresponding obligations to respect those rights), it is often possible to create a regulatory regime – a system of desired control rights and responsibilities - with regard to a certain resource, including personal data. For instance, tenant-landlord relationships were given a (partial) property status when it became clear that the purely contractual nature of a tenant's rights did not provide an individual with the desired protection.[334]

The classical property model that is at the core of Continental property law does not, as a rule, enable fragmentation, and is therefore less open to the introduction of property rights than its common law counterpart However, the globalization of the modern economy has led to the need for the laws in different countries to accommodate international trade practices, including taking the first steps towards the convergence of property laws.

The fragmentation of property rights has touched property institutions in Europe and is the first step towards the formation of a common European concept of property. French law in particular is showing signs of openness to the fragmentation of property law.[335] The process may become European-wide under the influence of EU legislation and ECJ case-law. The latter already recognizes claims such as milk and fishing quotas and social security rights as property.[336] Finally, the ECJ's decisions in line of the *Cassis de Dijon* case promote the further harmonisation of

---

[334] Lawson, *The Law of Property*.

[335] Van Erp, "Security Interests: A Secure Start for the Development of European Property Law." For examples of the 'lesser' property rights in German civil law see Akkermans, *The Principle of Numerus Clausus in European Property Law*.

[336] K. Lenaerts, Vanvoorden, K., "The Right to Property in the Case Law of the Court of Justice of the European Communities," in *Property and Human Rights*, ed. H. Vandenberghe (Bruylant, 2006).

European property law by establishing that when an object is tradable in one country, it has to be tradable to the same extent throughout the common market.[337]

The fact that the traditional civil law approach gradually albeit to a limited extent accepts the possibility of fragmented ownership is the result of a more flexible interpretation of the *numerus clausus* principle in these jurisdictions. Indeed, from the most rigid extreme that no new property rights were possible, the approach became more flexible, i.e. parties are still not free to attribute property status to privately created rights, but the creation and unitary ownership of new property rights is possible through the lawmaking process.

The fact that the notion of fragmented ownership has entered continental Europe on a national and supranational level enables a common European discussion on property in personal data in two ways. Firstly, it confirms that the common and civil law systems of property have (even) more common ground than is conventionally thought. Consequently, it is possible for the two systems to 'agree on terms' and hold a meaningful debate on property in personal data. Secondly, because fragmented ownership is less rigid in its consequences and less ideologically loaded, it allows for a more pragmatic approach to the creation of new property rights, including in unconventional property objects such as personal data.

a. (Re)discovered common ground

The idea to look beyond the differences of the property law systems in countries with the Continental and common law and to focus instead on similar ground rules, is not new. Among others, the results of research conducted by the group working with van Erp in Maastricht reveal that the logic behind the common and Continental property models is not as different as traditionally perceived, with the differences being more of form than substance:[338] both systems are based on a separation of real and personal rights and the principle of *numerus clausus* applies. Moreover, after the right in question has been qualified as a property right, the same basic rules govern its relationship to other entitlements.[339] Finally, the separate treatment of real and personal property in common law is not alien to Continental law systems; indeed, the latter, like their common law counterparts, also have a separate regime for property rights in land, which require obligatory registration.[340]

---

[337] Van Erp develops this point in Van Erp, "Security Interests: A Secure Start for the Development of European Property Law."

[338] ———, "From "Classical" To Modern European Property Law?.", Sjef Van Erp, "European and National Property Law: Osmosis or Growing Antagonism?," in *Walter van Gerven Lectures* (Europe Law Publishing, 2006)., Van Erp, "Security Interests: A Secure Start for the Development of European Property Law."

[339] Van Erp, "From "Classical" To Modern European Property Law?.", pp. 11-13

[340] E.g. Article III:89 of the Dutch Civil Code requires notarisation and registration for the contracts with land and other immovables.

In effect, the fragmentation of ownership takes the European property discussion 'back to [its feudal] basics.' This does not mean that society is returned to the feudal system of socio-economic relationships. Instead, what is meant is that even the civil law approach to property was, in fact, based on the feudal model of divided ownership interests in the sense that civil law developed in opposition to it. Yet, this also means that the civil law system of unitary ownership was built on a background of such a division and implies the – at least theoretical - possibility of its existence. A metaphor illustrates the point nicely; the entire body of theoretically possible property rights in their widest scope may be compared to a completed puzzle - a picture or a pattern consisting of small basic parts. The civil law system chose not to break the picture into pieces and only regards the assembled puzzle in its entirety, with occasional broken off pieces, as property, or, more accurately, a unitary ownership right. The common law system of property, on the other hand, chose to allow the puzzle to be broken into smaller, separate pieces of various real rights, and considers them as well as their entirety as proprietary rights. However, in both common and civil law, it is the same puzzle built from the same basic parts. So, if someone with a broken puzzle in the context of the common law communicates with someone else in the context of Continental law, where the puzzle is assembled into a complete picture, they can meaningfully talk about the same puzzle provided the former is aware that his basic parts are the pieces of the common pattern and the latter accepts that his complete picture is a mosaic comprised of the same basic parts.

b. The pragmatic application of *numerus clausus*: the *erga omnes* effect as the cause of propertisation

One may reasonably wonder if the 'puzzle' approach to the legal concept of property undermines the foundational principles of property in law, namely the division between property (real) and contractual (personal) rights guarded by the principle of *numerus clausus*. This study takes the position that it does not. Indeed, as Rudden explains, *numerus clausus* must exist, otherwise the fact that parties are free to create new property rights at will "would create a pyramid of rights, in which each successive right-holder would want to create property rights himself."[341] Allowing this unrestricted fragmentation would undermine legal certainty as to the obligations of third parties and result in the deflation of the value of land.[342] The fact that the mosaic is breakable into pieces does not enable one to break it up at will. What the puzzle model of common European property law does, however, imply is that the *numerus clausus* principle should be respected, although it should, at the same time, be applied in a more flexible way, which is not restricted by past fears of the restoration of the feudal system and is open enough to accommodate, e.g. new social

[341] Quoted in Akkermans, *The Principle of Numerus Clausus in European Property Law.*, p. 396
[342] Ibid.

goals. In other words, the fact that private parties should not be allowed to privately create rights that impose obligations on third parties does not mean that authorized bodies – legislatures or courts – cannot be more pragmatic and flexible in creating such rights for a good reason. Van Erp maintains a similar view and calls for a more flexible application of the ground rules of property, leading to the formation of a common European property law.[343]

The next question that one may legitimately ask is: if the application of the *numerus clausus* principle becomes more flexible, what would be the defining factor or characteristic on the basis of which rights are admitted to the category of real rights? The position taken herein is that this question should be answered from the standpoint of legal pragmatism. That is, new property rights should be able to be introduced with a view to achieving a regulatory goal that can be accomplished by a legal tool such as property. The defining characteristic of property (real) rights in law is their *erga omnes* effect. Accordingly, the admission criteria should be the desirability for the interest in question to have this effect and be protected against an indefinite number of people. In this way, and from a pragmatic standpoint, the *erga omnes* effect stops being a mere result of creating real rights, but instead becomes the rationale for doing so, also enabling control and the protection of material and normative values. Consequently, the reasoning behind a decision as to whether or not to introduce property rights in an object should come from the answer to the question of "whether a certain interest deserves *erga omnes* protection" and, if the response is yes, property rights in it should be considered as a possibility. Another basic principle of property law - transparency - can also still be achieved (by registration or possession).

3.2.4. Map of new property rights in a common European property discussion

A map of the mosaic of property rights, showing the big picture and its basic pieces, can be drawn on the basis of the conclusions reached on the defining elements and structure of property in law. However, an important disclaimer should be made at this point. Although, in the author's opinion, there is enough evidence to support the possibility of a harmonized European approach to the meaning of property rights in law, the ambition of this study does not go further than demonstrating the possibility of a common European discussion on property in personal data. The map below is meant to guide the legal debate on the propertisation of personal data, but, with additional reasoning, can also be used as a blueprint for a general European property

[343] For a more detailed explanation of his position see, e.g. Van Erp, "Security Interests: A Secure Start for the Development of European Property Law."

discussion. The foundation of the map is a spectrum of property interests developed by Harris, and described in his book "Property and Justice".[344]

To accommodate different types of property (which also vary from one national legal system to another) in his model, and with reference to wealth-allocation models in a number of imaginary societies, Harris developed a spectrum of ownership interests ranging from 'mere property' to 'full-blooded ownership', as set out in the diagram below.

Ownership interests and mere property are two ends of the spectrum.[345] Full ownership, much like the ownership formula *usus, fructus* and *abusus* in civil law, is defined as "an open-ended set of use-privileges and control-powers."[346] The presumption of existence of such an open-ended set of rights is the departure point and key element of the system of property rights, and is "separate and indispensable of a property institution,"[347] since all other property interests derive from ownership and are narrower in scope. The mere property in Harris' framework implies that "something that pertains to a person is, maybe within drastic limits, his to use as he pleases and therefore his to permit others to use gratuitously or for exchanged favours. … It embraces some open-ended set of use-privileges and some open-ended set of powers of control over uses made by others."[348] What distinguishes mere property from full-blooded ownership is a prima facie, absolute alienability rule in the latter case. However, the uniting idea beneath every point on Harris' spectrum is the opportunity to exercise some control over a thing.[349] This study interprets the latter thesis in such a way that the power of control is present due to the *erga omnes* effect, which is the common denominator of all property interests. This pragmatic approach, in which property rights are defined by their *erga omnes* effect, does, however, require some adjustments to the map proposed by Harris. So, as well as full ownership being the broadest property right possible, the narrowest property right

344 J.W. Harris, *Property and Justice* (Oxford [etc.]: Clarendon Press, 1996).
345 Ibid., p.27
346 Ibid., p.26; "[T]he rules of the property institution are premised on the assumption that, prima facie, the person is entirely free to do what he will with his own, whether by way of use, abuse, or transfer." (Harris, *Property and Justice*., p. 29)
347 Harris, *Property and Justice*., p.26
348 Ibid., p.28
349 Ibid.

on the spectrum is defined only by its *erga omnes* effect. Other property rights of a wider scope, in between full ownership and mere property, are possible. However, how to draw the borders of these rights and set their scope with regard to personal data is a matter of regulatory strategy, i.e. it is to be decided based on the desired degree of control that the parties involved should have.

3.3. The market function of property: the rebuttal of one objection to the flexible application of property rights

A traditional objection to the propertisation of unconventional objects, such as body parts or personal data, is that it would encourage a free market in these sensitive objects rather than control it. Since the present analysis rests on a core concept of property in law – *inter alia* its *erga omnes* effect – it is essential to explain here that some features – like free market alienability – which are often attributed to property in the layman debate, are not defining. This section will demonstrate that it is a misperception to link property rights and the free market, and that modern property law is increasingly being relied on to exercise its protective rather than its market function.

A number of commentators generally see the commodification (and propertisation as legitimized commodification) of certain goods, including personal data, as a problem. This is a "public good" argument, which generally implies that information privacy has value not only for an individual, but also for society at large. The market is, however, unable to account for the latter. For instance, Katrin Schatz Byford submits that regarding "privacy as an item of trade … values privacy only to the extent it is considered to be of personal worth by the individual who claims it",[350] while Pamela Samuelson argues that the propertisation of information privacy as a civil liberty might be considered "morally obnoxious."[351] "If information privacy is a civil liberty, it may make no more sense to propertize personal data than to commodify voting rights."[352] One of the main points made in this contribution in defence of the propertisation of personal data is that if property rights are structured in a certain way, even after the transfer of some control by 'selling' a fraction of the rights, an individual would always retain a degree of control over his personal data, e.g. allowing and defining the goals of data processing. It is more appropriate to define this function of property as being regulatory or protective of data protection rights rather than serving the free market. This partially addresses the 'public good' objection to propertisation. However, some additional points rejecting the idea of a

[350]Katrin Schatz Byford, *Privacy in Cyberspace: Constructing a Model of Privacy for the Electronic Communications Environment*, 24 Rutgers Computer & Tech. L.J. 1 (1998)

[351] Pamela Samuelson, "Privacy as Intellectual Property?," *Stan. L. R.* 52 (2000)., p. 1143

[352] Ibid., see also Rouvroy, "The Right to Information Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy."

purely market nature of property and supporting its use as a protective or regulatory tool now follow.

Firstly, unlimited market alienability is a myth. The alienability of any object of some public significance, e.g. food, medication, children's products, homes with minors as residents etc., is heavily regulated by the state. The free alienability inherent in and necessary for the market function of property may, therefore, be limited, since property is never absolute.

Secondly, although the main property function is rightly said to be to protect 'value' from third parties, that value may be both material and immaterial.[353] The latter is in no way linked to the free market. For instance, in English law, as Lawson and Rudden point out, in the 20th century the concept of property changed from a means of securing and investing wealth to "a direct denial of the general commercial thesis that every physical thing can be adequately replaced by its price in money."[354] This new vision has particularly influenced tenant-landlord relationships, where the value of a home for a family began to be substituted for the value of the wealth invested in a house.[355]

Thirdly, the concept of property used in criminal, constitutional and human rights law also serves a protective (against theft, damage, or state taking) rather than a market function. For instance, albeit only in two lower court decisions, in the Netherlands virtual property received criminal law protection before it received a property status in private law.[356]

Fourthly, it seems that the notion of property is only closely related to the free market in Western legal thought. Nwambueze quotes examples of some aboriginal societies that are familiar with the concept of property but not with the idea of its sale.[357] Gray explains that a large proportion of Western scholarly writing focuses on the market side of property, since the formation of the common law approach to property coincided with "the age of bargain and exchange."[358] One of the points of dispute in the modern common law property debate is whether alienability is a necessary element of property rights, with a strong position being argued against it.[359]

Finally, property and its meaning are inherently political. As long as property rights are enforced by the state, their scope and objects are governed by the political goals of a given society. Consequently, if there is a need for property to be a

---

[353] Nwabueze, *Biotechnology and the Challenge of Property*.

[354] Lawson, *The Law of Property.*, p. 198

[355] Ibid.

[356] A.C. Lagemaat, Boonk, M.L., Briet, M., "Vermogensrechtelijke Aspecten," in *Recht in Een Virtuele Wereld: Juridische Aspecten van Massive Multiplayer Online Role Playing Games.* (Elsevier, 2007).

[357] Nwabueze, *Biotechnology and the Challenge of Property*.

[358] Gray, "Property in Thin Air.", p. 294

[359] According to Gray, "the criterion of "excludability" gets us much closer to the core of 'property' than does the conventional legal emphasis on alienability or enforceability of benefits." Ibid.

protective or regulatory tool, and there is a respective political will to achieve this, the meaning of property can be shaped accordingly.

4. Conclusion

The goal of this chapter was to make some basic, general statements about property to prepare the reader for the further examination of the idea of property in personal data. To conclude this exercise, let us bring together and summarize the most important messages that this chapter aimed to convey.

Firstly, when engaging in discussions on property matters one should always be aware not only of the multiplicity of possible perspectives and forums using the concept of property, but also which of these is appropriate in the debate at hand.

Secondly, although the layman's, normative, and economic perspectives on property each have their own value, these should not be substitutes for the legal perspective when the debate concerns the introduction of *legal* property rights. Indeed, the non-legal discourses focus on mainly normative reasons to have or not to have property and often disregard the content and effect of property rights. Adoption of property rights by a legal system is guided by normative considerations but is also a matter of fact. It implies that the rights in question are of a particular content and scope and that their enjoyment will have certain legal effects. This distinction between the normative and matter-of-fact arguments should be kept in mind at all times when discussing an issue such as a possibility of property rights in personal data.

Thirdly, since the content of laws in general, and property laws in particular, is influenced by a number of extra-legal factors, *inter alia*, political considerations, the meaning of property rights in law, as well as their objects and scope, are fluid and adjust to the conditions of a given society, varying across both time and space.

Fourthly, despite these differences, in particular between common and civil law jurisdictions, due to the flexible application of the principle of *numerus clausus* and the resulting fragmentation of ownership, it is possible to have a European discussion on property matters, such as the property in personal data, which is united by the common denominator – the *erga omnes* effect that property rights have.

Fifthly and finally, a closer look at the legal notion of property addresses some important reservations invoked in the debate on the propertisation of unconventional objects like personal data. In particular, it became clear that market alienation is not indispensable in the property debate, and property rights cannot, therefore, be presumed to serve only a market function.

Part II: Origins of the idea of propertisation

Chapter 5: Limitations of US information privacy law in dealing with the personal data problem

1. Introduction

In order to devise a viable European perspective on the propertisation of personal data, it is essential to fully grasp the idea as it emerged in its 'mother-jurisdiction', the United States. The logic of the functional comparison demands that to incorporate a legal innovation advanced somewhere other than in his native legal system, a true comparatist should first understand the background of the argument in question and to appreciate the legal style[360] of the system from where an innovation arose. The legal style here is broadly understood as encompassing historical developments, modes of legal thought, institutions, legal sources, and ideology.[361] Accordingly, the goal of this chapter is to do more than just provide an introduction to the debate on property rights in personal data as it has unfolded in the United States. Instead, the aim of the subsequent pages is to prepare the groundwork for the reader to view the idea of the propertisation of personal data as a logical development in the interplay of various factors: history, institutions, legal sources, and ideology as employed in the United States in the field of personal data. The analysis of those factors includding legislative history will be strictly limited to what is necessary to build the argument of this chapter.

This chapter starts with an overview of the legislative history in the US in the field of personal data protection. It will consider how the problem of data protection or, in the native language - 'information privacy', first appeared and how it has been defined on the political agenda (Section 2). This perspective is of particular importance for a meaningful comparative study since it makes the European reader familiar with the American legal concepts that are relevant for the debate, e.g. privacy and information privacy and their relation to European data protection. Section 3 sketches the US system of data protection along with its shortcomings as indicated by authoritative commentators on the country's data protection laws. The chapter concludes that the personal data protection system in the US was perceived by many as failing in multiple aspects to adequately respond to the challenges posed by recent technological developments when it comes to the protection of personal information. The chapter also presents a range of proposed solutions (other than propertisation) to the perceived inadequacies of the US system of personal data protection, along with criticisms of those solutions (Section 4).

---

[360] Zweigert & Kötz, pp. 68-69

[361] Zweigert & Kötz, pp. 68-69

An important disclaimer must be made at this stage. This chapter is not intended to provide an all-inclusive description or analysis of the specifics of American history, political developments, or legal system. The analysis only goes as far as is demanded by the purpose of the chapter, namely explaining which factors, in the author's opinion, have contributed to the emergence of the idea of propertisation of personal data in the United States.

2. "Mantra of privacy": *conceptualis*ation of the personal data problem in the United States

Chapters 2 and 3 have already described both the changes undergone by western post-industrial societies such as the United States and the concerns they have had since the middle of the 20th century. This study refers to those developments and concerns as "the personal data problem." This section will, therefore, not repeat what has already been established. Instead, and being true to the legal pragmatism approach, the analysis will focus on how the personal data problem was *conceptualis*ed in the US at the time of the formation of the country's information privacy laws as, according to legal pragmatism, the way of a problem is perceived, discected into elements and filed into categories determines the legislator's approach to solve it.[362] The way in which the problem of databases was conceptualised in the US has channelled and, therefore, now, at least partially, explains the choice of tools used to tackle it,[363] whether it be the personal data protection instruments currently employed, or the proposed alternative tools of which the propertisation of personal data is just one potential solution. This section will reveal that the definition of the personal data problem as a privacy and secrecy of information issue dominated the policy debate at the time that the country's information privacy law were drafted. The consequence of such an approach is that it is extremely difficult for the legislation to cope with modern information practices and adequately respond to new challenges, which go far beyond issues of secrecy.

As shown elsewhere in this book, despite the vast amount of attention devoted to new information practices since the 1960s, when it comes to the substance of the concerns, a uniform position on the participants of the debate, whether they are scholars or policymakers, seems to be difficult to achieve. Indeed, this chaos in establishing the personal data related concerns seems to be inherent to the nature of the personal data problem itself.[364]

---

[362] see Dewey's quote in Chapter 1 outlining principles of legal pragmatism (from John Dewey, Logic: The Theory of Inquiry 108 (1938))

[363] Another part of the explanation concerns the properties of the US legal and political systems and will be considered in the subsequent section of this chapter.

[364] Bennett, *Regulating Privacy - Data Protection and Public Policy in Europe and the United States.*, p. 12

The vague fears of databases that were raised in the United States in the 1960s have ever since been the reason behind attempts to articulate the precise nature of the personal data problem on a variety of levels, for example in legislative hearings and scientific debate. What has, however, united these quite distinct forums is the fact that in defining the personal data problem those involved have all been focussed on, as Solove puts it, the "mantra of "privacy".[365] The issues of personal data protection addressed during congressional hearings, for example, were *conceptualis*ed as steps towards "the protection of our individual right to be let alone."[366] The scientific debate concerning the personal data problem has likewise been phrased in terms of either "privacy" or "information privacy."[367] Of course, the use of the term is not problematic in itself, since privacy is a flexible enough concept to protect a number of related interests.[368] However, US scholars and policymakers often utilized the concept of privacy in its narrowest sense to denote the secrecy of personal information. As a result, the dangers of new information practices were associated with problems of the disclosure of confidential information and surveillance.[369] Priscilla Regan, for instance, writes that "a new technology might allow for [the] observation of actions regarded as 'private', listening in on conversations thought to be 'private', [the] collection and exchange of information thought to be "private", or [the] interpretation of psychological responses viewed as 'private.'"[370]

Of course, the issue of secrecy was not only perceived as being valuable in itself. Along with the protection of mere personal space, a gradual loss of secrecy was seen as being a gateway to other, greater, evils. Indeed, a metaphor of 'Big Brother' was often used to illustrate the problems of an imbalance of powers and manipulation. The metaphor was borrowed from George Orwell's *Nineteen Eighty-Four,* a novel in which a totalitarian state was described. The power of this state over an individual was rooted in the illusion that every aspect of a person's life was being watched, and every wrong move was noted and would, inevitably, be punished by Big Brother. As a result, the freedom of the citizens of Orwell's state was sacrificed

---

[365] Solove, "Privacy and Power: Computer Databases and Metaphors for Information Privacy."; Regan, *Legislating Privacy: Technology, Social Values, and Public Policy*., pp. 3, 15; Blok, *Recht Op Privacy*., p. 245; United States. Congress. Senate. Committee on the Judiciary. Subcommittee on Constitutional Rights, *Federal Data Banks and Constitutional Rights* (U.S. Govt. Print. Off., 1974)., p. ix, etc.

[366] Senate Floor debates, reprinted in US Senate and House Committees on Government Operations, Legislative History of the Privacy Act of 1974, s. 3418 (PL 93-579), 94th Cong., 2d sess. (Washington, D.C.: Government Printing Office, 1976), p. 775

[367] Fred H. Cate, Litan, Robert "Constitutional Issues in Information Privacy," *Mich. Telecomm. Tech. L. Rev.* 35, no. 9 (2002).; Cohen, "Examined Lives: Informational Privacy and the Subject as Object.", Richard A. Epstein, "Privacy, Publication, and the First Amendment: The Dangers of First Amendment Exceptionalizm," *Stan. L. R.* 52 (2000)., etc.

[368] For more on a definition of "privacy" see, e.g. Solove, "A Taxonomy of Privacy."; see also the discussion elsewhere this book on the difference between legal and philosophical definitions of privacy (Chapter 9, section 2).

[369] ———, "Privacy and Power: Computer Databases and Metaphors for Information Privacy.", p. 1431

[370] Regan, *Legislating Privacy: Technology, Social Values, and Public Policy*., p. 2

and their behaviour manipulated as they began to correct themselves and act according to the standards imposed on them. The metaphor of the 'little brothers' was used in the US to describe a similar phenomenon of power and manipulation by private organizations.[371] Regan, for instance, explains how new technology supplies organizations with a novel source of power over individuals, which is derived "from the organizations' access to information about individuals' histories and activities, the content and patterns of their communications, and their thoughts and proclivities"[372], all of which enables them to manipulate consumer behaviour. Daniel Solove, who has conducted in-depth research into the terminology of privacy employed in the US debate, concludes that even commentators who do not use the 'Big Brother' metaphor, nevertheless, describe the problem "in similar conceptual terms."[373] He goes on to quote Paul Schwartz and Joel Reidenberg who write: "The more that is known about an individual, the easier it is to force his obedience. Through the use of databanks, the state and private organizations can transform themselves into omnipotent parents and the rest of society into helpless children."[374]

To be fair to the US information privacy debate, more inclusive language of control over personal information was invoked early on to describe the essence of the personal data problem. In 1970, Alan Westin defined privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[375] Jerry Kang refers to control as "the heart of information privacy."[376] The language of control over personal information is still used to refer to desired landmarks in the data protection landscape, such as the transparency of data processing, the accountability of data processing actors, control over the fact and manner of the collection of personal information, and the analysis and use of data.[377] US commentators, especially in the work published in the 2000s, were among the scholars who contributed to the discourse on the meaning of control. In brief, Solove, Bennett[378] and others added new dimensions of freedom, dignity, and dehumanization to the problem of a lack of control of personal data, which in Solove's words was caused "by the often thoughtless and irresponsible ways that bureaucracies use personal information and

---

[371] Solove, "Privacy and Power: Computer Databases and Metaphors for Information Privacy."
[372] Regan, *Legislating Privacy: Technology, Social Values, and Public Policy*., p. 2
[373] Solove, "Privacy and Power", p. 1395-96
[374] Paul M. Schwartz & Joel R. Reidenberg, *Data Privacy Law* 39 (1996); see also Paul M. Schwartz, Privacy and Participation: Personal Information and Public Sector Regulation in the United States, 80 Iowa L. Rev. 553, 560 (1995)
[375] Westin, Privacy and Freedom, p. 7
[376] Jerry Kang, "Information Privacy in Cyberspace Transactions," *Stan. L. R.* 50 (1998)., p. 1266
[377] See discussion in Chapter 3
[378] Bennett, *Regulating Privacy - Data Protection and Public Policy in Europe and the United States*. Note that Bennett, although originally comes from the UK and works in Canada, actively participated in the US information privacy discourse and therefore this Chapter's analysis of the US argument considers his work equally with the US scholars.

their lack of accountability in using and protecting the data. In other words, the problem is not simply a lack of control over information, but "control out of control" – a situation where nobody [*not just an individual himself – N.P.*] is exercising meaningful control over the information."[379] However, as indicated above, this broad definition of control only appeared in the information privacy literature relatively recently, and had no influence in the 1970s when the foundations of modern US information privacy law were laid. At that time, the terminology of control was utilized in its narrowest sense, and implied little more than secrecy: limits on transfers of personal information from an individual to a data collector and then to third parties, with there being little knowledge of the actual processes involved in relation to one's data.[380]

As the personal data problem became an issue gaining greater international importance and requiring international solutions, and taking into account the fact that the intellectual community is free of many of the restrictions implied by national borders, American scholars have participated in and enriched the debate on the substance of the data protection problem. Indeed, it would be inaccurate to state that American authors still adhere to the narrow definition of the personal data problem as an issue of secrecy. However, some of the limitations of the US legal and political systems, which will be described later on in this chapter, make it difficult to incorporate these more modern viewpoints into existing legal norms. The origins of current information privacy laws, with their narrow definition of the personal data problem, are not only visible 30 years on, but the 'mantra of privacy' imposes significant limitations on the capacity of the country's legal rules to deal with the challenges of the modern data flow. The following section will explain how.

3. US information privacy law

The author of this work believes that the origins of the idea of the propertisation of personal information in the US largely come from the fact that the country's data protection laws were perceived in many aspects as being unable to adequately respond to the (already not so new) challenges of the information revolution. The purpose of introducing property rights in personal data would be to compensate for this perceived handicap of the US legal and political system. This section will explain why.

The US law on personal data protection requires considerable effort on the part of an unfamiliar reader if he is to understand it. Its complexity has several sources. The first has to do with terminology. In Europe it is uncommon for

[379] Solove, "Privacy and Power", p. 1428; Solove uses the Kafka metaphor to capture this condition.
[380] For example, see Bergelson, "It's Personal, but Is It Mine? Toward Property Rights in Personal Information.", Cohen, "Examined Lives: Informational Privacy and the Subject as Object.", etc.

textbooks and scholarly writing to refer to this body of law as the law of information privacy or, simply, privacy law.[381] Secondly, although this choice of wording is unsurprising given the fact that the data protection problem in the US has been *conceptualis*ed as an issue of privacy, it still reflects (or arguably leads to) some confusion when traditional mechanisms of privacy protection are applied to new personal data related problems.[382] Paul Schwartz and Joel Reidenberg brand this as an attempt to put "new wine in old bottles."[383] Another source of complexity, especially in the eyes of a European reader, is that US information privacy law does not have a single, hierarchical order of rules, but is instead comprised of the norms of tortious, constitutional, and statutory law, being a patchwork of rules from different sources, subjects of regulation, and applicability. Finally, the body of law at hand operates in the country's federalized legal system, meaning that the capacity to act is divided between the federation and the states.[384] With no uniform, hierarchical personal data protection laws in place, Solove describes the US system as one which "uses whatever is at hand [...] to deal with the emerging problems created by the information revolution."[385]

The folowing sections introduce the US information privacy law system,[386] explain how it operates, identify which areas of the data protection problem it addresses, and address what gaps the commentators have identified which could, arguably, be dealt with by propertisation.

3.1 Law of tort

It has been widely acknowledged that the law of tort has played a groundbreaking role in the protection of privacy in the US.[387] In 1890 in their renowned article,[388] Warren and Brandeis derived a right to privacy from common law torts. However, the role that torts now play in resolving the data protection problem is limited, both due to the narrow scope of individual torts and the more systematic shortcomings thereof as a common law institution.

---

[381] Daniel J. Solove, Rotenberg, Marc; Schwartz, Paul M. , *Information Privacy Law* (New York: Aspen Publishers, 2006)., p. 9; Jerry Kang, Buchner, Benedikt, "Privacy in Atlantis," *Harvard Journal of Law and Technology* 18, no. 1 (2004)., p. 231, etc.

[382] Solove, "Privacy and Power"

[383] Paul M. Schwartz, Reidenberg, Joel R., *Data Privacy Law: A Study of United States Data Protection* (Charlottesville, Virginia: MICHIE Law Publishers, 1996)., p. 102

[384] Ibid., pp. 7-8

[385] Solove, "Privacy and Power", p. 1430

[386] This overview of the law is incomplete and only goes as far as is required to prove the point of this Section of the paper: to introduce the propertisation argument as it is made in the US in light of the legal background against which the argument emerged.

[387] Solove, Rotenberg, Schwartz, *Information Privacy Law*, p. 9

[388] Warren, "The Right to Privacy."

White defines US torts as a field reflected in individual actions and concerned with civil wrongs not arising from contracts.[389] The law of tort is mainly a common law approach, *i.e.* it has been developed by courts through the system of precedent.[390] In other words, when ruling on a case, the courts rely on previously decided similar cases. Yet, the binding force of precedent is limited in the US, where the courts are "more willing [...] to develop the law in accordance with social reality."[391] Indeed, due to the constitutional division of federal and state powers, the US law of tort is mainly state law.

The branching out of the law of tort between US states has resulted in "numerous variations within different jurisdictions"[392] and "the lack of agreement on fundamental principles of the common-law system"[393] leading to difficulties in administering justice. To overcome these problems, the American Law Institute[394] produced the Restatement of the Law of Torts, which is regarded as "a very significant attempt at a searching and exhaustive analysis of the entire field."[395] The Restatement is not, however, binding. Instead, its role is comparable to that of scholarly writing in international law.[396] However, it is "the most complete and thorough consideration which tort law ever has received,"[397] and this study will, therefore, rely on it when considering privacy torts in the US.

The Restatement distinguishes between four types of privacy torts: (1) intrusion upon a plaintiff's seclusion or solitude, or into his private affairs; (2) public disclosure of embarrassing private facts; (3) publicity which places one in a false light in the public eye; and (4) appropriation, for the defendant's advantage, of the plaintiff's name or likeness.[398] This section will demonstrate, *inter alia,* that all four of these torts are so tainted by the notion of secrecy that they have very little to offer when it comes to addressing the challenges of the modern data flow beyond keeping data 'private'.

---

[389] G. Edward White, *Tort Law in America : An Intellectual History*, Expanded ed ed. (New York Oxford University Press, 2003)., p. xxiii

[390] Ralf Michaels, "American Law (United States)," in *Elgar Encyclopedia of Comparative Law*, ed. Jan M. Smith (Cheltenham and Northampton: Edward Elgar, 2006)., p. 68-69.

[391] Karl Llewellyn, *The Common Law Tradition* (Boston: Little, Brown, 1960).

[392] web-site of the American Law Institute available online at <http://www.ali.org/index.cfm?fuseaction=about.creationinstitute> (accessed on November, 18th, 2008)

[393] Ibid.

[394] Ibid.

[395] W. Page Keeton, Prosser, William Lloyd, *Prosser and Keeton on the Law of Torts*, 5th student ed. ed., Hornbook Series (West Publishing co, 1984)., p. 17

[396] Peter Blok, *Recht op Privacy*, (2002)

[397] Prosser and Keeton on Torts, p. 17

[398] William Prosser, "Privacy," *Cal. L. Rev.* 48 (1960)., p.389

3.1.1. Intrusion

This tort protects against the intentional intrusion, whether physical or otherwise, "into the solitude or seclusion, or private affairs or concerns," of another "in a manner that is highly offensive to a reasonable person."[399] The tort thus has the potential to provide a remedy for a data protection problem that is, in part, related to "an unauthorized acquisition or transfer of personal information."[400] Indeed, this tort is relevant to the intangible world of personal information since it does not require an intrusion into one's home or other physically defined space, but can constitute an invasion of one's "personality" or "physical integrity."[401] However, in reality it is difficult to extend this tort to cover new information practices, with problems stemming either from some of the conceptual characteristics of the tort, or from the mere unwillingness of the courts to expand its boundaries.

There are several obstacles if new information practices are to constitute an intrusion as defined by this tort. Firstly, the intrusion must involve an invasion of "seclusion." Although this does not relate to any physically defined private space, the courts have rejected claims when plaintiffs have been in public places.[402] As a result, a major aspect of the data protection problem is not covered by the tort of intrusion, since the collection and use of information often occur in cyberspace, much of which "may well be considered public places."[403]

Secondly, the intrusion must be unauthorized, and the courts have interpreted this requirement as protecting only secret information. In *Dwyer v. Am. Express Co,*[404] a group of American Express cardholders challenged the company's profiling practices and its 'renting' of information relating to its cardholders' spending habits. American Express's analysts created cardholders' profiles based on how they shopped, how much they spent, and their behavioural characteristics and spending histories.[405] The plaintiffs argued that such practices involved the disclosure of private financial information and resembled cases involving intrusion into private financial dealings, such as bank account transactions.[406] The court refused to classify the information practices cited as intrusion, because the plaintiffs did not establish that it was unauthorized: "[b]y using the American Express card, a cardholder is

---

[399] American Law Institute, §652B (1977)

[400] Bergelson, "It's Personal, but Is It Mine? Toward Property Rights in Personal Information.", p. 405; see also Solove, "Privacy and Power", p. 1432

[401] *Phillips v. Smalley Maint. Servs*., 435 So. 2d 705, 711 (Ala. 1983) cited in *Bergelson, "It's Personal, but Is It Mine?", "It's Personal, but Is It Mine?",* p. 406. The case-law analysis in the section on torts is mainly drawn from the works of Daniel Solove and Vera Bergelson.

[402] *Muratore v. M/S Scotia Prince*, 656 F. Supp. 471, 482-83 (D.Me. 1987) cited in Solove, "Privacy and Power", p. 1432

[403] Solove, "Privacy and Power", p. 1432

[404] *Dwyer v. Am. Express Co.,* 652 N.E. 2d 1351, 1352-53 (Ill. App. Ct. 1995)

[405] *Dwyer,* at 1353

[406] Ibid, at 1354

voluntarily, and necessarily, giving information to defendants that, if analysed, will reveal a cardholder's spending habits and shopping preferences."[407] In other words, merely compiling and renting information voluntarily disclosed by the plaintiff to the respondent, or the creation of new information on the basis of voluntarily revealed data (profiling), does not constitute intrusion.[408]

The third obstacle to new information practices being defined as a tortious intrusion is the division between different kinds of information based on the level of secrecy thereof. The courts in *Remsburg,*[409] for example, distinguished between information that may be reasonably expected to be kept private, even after disclosure to a third party, and data that is less "secret".[410] The court had to decide whether obtaining the plaintiff's social security number from a credit reporting agency and obtaining her work address[411], all of which occurred without her knowledge or consent, constituted an intrusion. The *Remsburg* court classified a social security number as information that may be reasonably expected to remain private, even after its disclosure to a third party, whereas a work address was not regarded as "secret, secluded or private" information. Only in the first case did the plaintiff have a cause of action in intrusion.[412] According to Daniel Solove's analysis of the case law, the courts have rejected intrusion claims involving the types of information that are the most likely to be the subject of collection and inclusion in databases.[413] This covers, *inter alia*, unlisted phone numbers,[414] selling subscription lists to direct mail companies,[415] and collecting and disclosing an individual's past insurance history[416].

Fourthly, the use of the tort of intrusion in the context of the data protection problem is limited by the requirement that an information practice must be highly offensive to a reasonable person if an action is to succeed.[417] In so determining, one has to take into account "the degree of intrusion, the context, conduct and circumstances surrounding the intrusion as well as the intruder's motives and objectives, the setting into which he intrudes, and the expectations of those whose privacy is invaded."[418] Daniel Solove points out that the "highly offensive to a reasonable person" requirement is difficult to satisfy in an individual case,[419] especially because "each particular instance of collection is often small and

---

[407] Ibid.
[408] Ibid.
[409] *Remsburg v. Docusearch, Inc.*, 816 A. 2d 1001 (N.H. 2003)
[410] *Remsburg* at 1004-05
[411] Ibid.
[412] Ibid.
[413] Solove, "Privacy and Power", p. 1432
[414] *Seaphus v. Lilly*, 691 F. Supp. 127, 132 (N.D. Ill. 1988)
[415] *Shibley v. Time, Inc.*, 341 N.E.2d 337, 339 (Ohio Ct. App. 1975)
[416] *Tureen v. Equifax, Inc.*, 571 F.2d 411, 416 (8th Cir. 1978)
[417] See, e.g., *Remsburg*
[418] *Remsburg*, at 1008-09
[419] Solove, "Privacy and Power", p. 1432

innocuous,"[420] and the required level of danger is created only "by the aggregation of information, a state of affairs typically created by hundreds of actors over a long period of time."[421]

Finally, even if the shortcomings referred to above are corrected, the applicability of this tort to the data protection problem would be limited only to data collection, due to the very nature of an intrusion.[422]

3.1.2. Disclosure

The tort of the disclosure of private facts is committed when publicity is given "to a matter concerning [the] private life of another [...] if the matter publicized [...] would be highly offensive to a reasonable person, and is not of legitimate concern to the public."[423] Similar to the tort of intrusion, this tort "could conceivably be applied to certain uses of databases, such as the sale of personal information by the database industry."[424] However, it is highly unlikely that these practices would meet the requirements established by the relevant case law.

Publicity is the first such requirement. For a transfer of data to constitute a disclosure, the information must be communicated "to a sufficient number of people, so that it is "substantially certain to become [...] public knowledge."[425] However, the sale of personal information is normally limited to a transfer from a primary to a secondary collector.

Furthermore, the standards of "highly offensive" or "highly personal" information, which are often interrelated in actual practice, are difficult to satisfy. This tort only protects "highly personal information", i.e. it "is not intended for the protection of any shrinking soul who is abnormally sensitive about such publicity."[426] Disclosure becomes highly offensive when it concerns personal facts that are not available for public scrutiny and are kept by a plaintiff "entirely to himself or [are] at most revealed only to his family or to close friends."[427] When considering information that is available to public scrutiny, it is possible to apply Solove's concern with regard to the tort of intrusion; even if a plaintiff can prove the highly personal and embarrassing character of the information disclosed, there will

---

[420] Ibid.

[421] Ibid.

[422] Bergelson, "It's Personal, but Is It Mine? Toward Property Rights in Personal Information.", p. 406; William J. Fenrich, "Common Law Protection of Individuals' Rights in Personal Information," *Fordham L. Rev.* 65 (1996)., p. 972 n.150; Joel R. Reidenberg, "Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?," *Fed. Comm. L. J.* 44 (1992)., pp. 222-223

[423] Restatement §652D

[424] Solove, "Privacy and Power", p. 1433

[425] Restatement §652D, comment a.

[426] Prosser, "Privacy.", p. 397; *Forsher v. Bugliosi*, 608 P.2d 716, 723 (Cal. 1980)

[427] Restatement §652D, comment b.

be no cause of action if he happened to reveal this data in cyberspace, which is often regarded as being a public arena.

Similarly, the tort of disclosure does not protect an individual against the publication of facts in a public record "such as the date of birth, the fact of his marriage, his military record, the fact that he is admitted to the practice of medicine or is licensed to drive a taxi cab."[428] However, this information is routinely used for profiling. As Vera Bergelson concludes, the disclosure of merely neutral facts would not be actionable.[429] In most cases, lifestyle information, along with names[430] and places of work and residence,[431] is not regarded as being "highly personal and embarrassing."[432]

The third obstacle to this tort's applicability to new information practices is that the level of protection afforded thereby is linked to social conventions: "the customs of the time and place, to the occupation of the plaintiff and to the habits of his neighbours and fellow citizens."[433] However, the reality is that these 'normal' habits and adopted social standards in data processing have been altered by the very technological and marketing developments which these social norms are intended to restrain.[434]

Finally, it is difficult for a plaintiff to make use of such protection, even if it is afforded to him. According to Solove, it is difficult "to discover that such sales or disclosures have been made."[435] By design, Solove continues, the tort of private facts serves to redress excesses of the press and, consequently, deals with the widespread dissemination of personal information in ways that naturally become known to the plaintiff, whereas "the use and sale of databases is often small and done in secret."[436]

3.1.3. False light

The tort of false light protects against "publicity to a matter [...] that places the other before the public in a false light" that is "highly offensive to a reasonable person."[437] Commentators agree that this tort has limited or no applicability to the data protection problem. Indeed, apart from the publicity and "highly offensive" requirements addressed earlier, there are several other obstacles that are specific to the false light tort.

---

[428] Ibid.
[429] Bergelson, *"It's Personal, but Is It Mine?"*, p. 409
[430] *King County v. Sheehan*, 57 P.3d 307, 316 (Wash. Ct. App. 2002)
[431] *Webb v. City of Shreveport*, 371 So. 2d 316, 319 (La. Ct. App. 1979)
[432] Bergelson, *"It's Personal, but Is It Mine?"*, p. 410
[433] Restatement §652D, comment c.
[434] Leenes, "'Code': Privacy's Death or Saviour?."
[435] Solove, "Privacy and Power", p. 1433
[436] Ibid.
[437] Restatement §652E

Firstly, the tort of false light protects an individual's reputation,[438] whereas data processing is rarely harmful to this interest.[439] Secondly, as Bergelson comments, this tort is not applicable to the kind of data processing whereby individuals provided the relevant information themselves. The defining element of this tort is that the information revealed is false or erroneous, whereas personal data transferred by primary to secondary collectors has usually been provided by the data subjects themselves and is correct. Bergelson speculates that a set of information, or a profile that is the subject of a transfer, may be limited or one-sided and thereby puts an individual in a false light.[440] Nevertheless, she concludes that this argument leads to the absurd possibility of all information transfers being banned because "no information is 'complete'."[441] It is only when data was not provided by a plaintiff that the courts can apply this tort to protect against the dissemination of erroneous information "when the defendant has not taken proper steps to ensure its correctness."[442]

3.1.4. Appropriation

A particular type of information practice is actionable under the tort of appropriation if it involves the exploitation of "the name or likeness of another" to a defendant's "own use or benefit."[443] The literature distinguishes between appropriation and the right of publicity. According to Prosser, the difference between the two results not from the actions that gave rise to a complaint, but from "the nature of the plaintiff's rights and the nature of the resulting injury. [...] [W]hile the appropriation branch of the right of privacy is invaded by an injury to the psyche, the right of publicity is infringed by an injury to the pocketbook." [444] Virtually every state recognizes one or the other (or both) of the two wrongs, often making no distinction between the two.[445] This study will, therefore, also consider them together.

Commentators agree that this tort has the potential to provide a remedy to the use of personal information for targeted marketing if it is regarded as the utilization of an individual's name to make a profit.[446] Three cases - *Shibley v. Time Inc.*,[447] *Dwyer*, and US *News and World Report v. Avrahami*[448] - are usually regarded as attempts to

[438] Prosser, "Privacy.", p. 400
[439] Solove, "Privacy and Power", p. 1433
[440] Bergelson, *"It's Personal, but Is It Mine?"*, p. 405, fn 143
[441] Ibid.
[442] Ibid.
[443] Restatement §652C
[444] Prosser, Law of Torts §117, p. 401, fn 154:
[445] Bergelson, *"It's Personal, but Is It Mine?"*, p. 410;
[446] Solove, "Privacy and Power", p. 1433-34; Bergelson, *"It's Personal, but Is It Mine?"*, p. 411
[447] *Shibley v. Time Inc.*, 341 N.E.2d 337, 340 (Ohio Ct. App. 1975)
[448] US *News and World Report v. Avrahami,* No.95-1318, 1996 Va. Cir. LEXIS 518 at *1 (va. Cir. Ct. June 13. 1996)

bring an appropriation suit against the practices of the unauthorized dissemination of personal information through the sale of mailing lists. However, the courts have seemed to be unwilling to extend the applicability of the tort of appropriation to new information practices and attempts to do so have failed. *Shibley* was a class action brought in Ohio against a number of journals and the issuer of the American Express credit card who sold to direct mail companies the details of lists of subscribers without their prior consent. The court found that there was no appropriation because the plaintiffs were not used to endorse any product.[449] In *Dwyer* (Illinois), the court found that in the case of subscription lists "an individual name has value only when it is associated with one of [the] defendants' lists"[450] and "defendants create value by categorizing and aggregating these names."[451] In *Avrahami,* the court in Virginia maintained that "the tort of appropriation is intended only to give redress to a person whose name, portrait, or picture was used for either advertising or trade."[452] Similarly, in *Remsburg,* the New Hampshire Supreme Court refined the appropriation requirement by stating that it requires there to be a benefit from the "reputation, prestige or other value" associated with an individual,[453] and "does not protect one's name per se."[454] In this case, an appropriation claim was rejected against a private investigator who provided his client with personal information about a woman who was subsequently stalked and killed by that client. The action failed because the benefit did not accrue from the victim's reputation, but from the client's willingness to pay for the data.[455] Since the key element of a cause of action in appropriation is the reputation, prestige or other value associated with a name, the tort of appropriation is most effective at protecting celebrities who have created value in their personalities.[456] It is not, however, likely to be of assistance to an average person who believes that his data has been misused.

3.1.5. Tort as a common law institution

Leaving aside the possibility of fixing the shortcomings of privacy torts by creating a new cause of action against improper information practices, it is important to note that the inherent limitations in the law of tort would still not permit the creation of a general system of data protection. Included in these limitations is the inhomogeneous and unsystematic nature of torts,[457] such as the protection of only

---

[449] *Shibley*, at 339
[450] *Dwyer,* at 1356
[451] Ibid.
[452] *Avrahami* cited in *Bergelson, "It's Personal, but Is It Mine?",* p. 412
[453] *Remsburg*, at 1009
[454] *Remsburg*, at 1009 (see also Restatement §652C, comment d.)
[455] *Remsburg*, at 1010
[456] Solove, "Privacy and Power", p. 1434
[457] Michaels, "American Law (United States).", p. 71

negative rights[458]. The task of creating positive rights, or imposing affirmative obligations, which is, as some claim, the essence of data protection,[459] is alien to the nature of the law of tort, which is concerned with providing a remedy for civil wrongs that have already been committed. This means that this branch of law cannot create positive rights and does not have a preventative function.[460]

3.2 Constitutional law

Some authors assign to the United States Constitution[461] a very special role in the development of the law of privacy and, consequently, to information privacy as its manifestation. According to Whitman, "to Americans, the starting point to [achieving an] understanding of the right to privacy"[462] is the Constitution and the Bill of Rights in particular, "with its vigorous circumscription of state power. Whitman continues, "At its origin, the right to privacy is the right against unlawful searches and seizures,"[463] as enshrined by the Fourth Amendment.[464] However, the role of the Constitution in the modern system of information privacy is rather limited. The purpose of the following sub-sections is to explain this role in terms of how constitutional norms and principles are relevant for the protection of personal data. Sub-section 3.2.1 outlines the scope of the constitutional protection of information

---

[458] Bergelson, *"It's Personal, but Is It Mine?"*, p. 415

[459] Paul de Hert, Gutwirth, Serge "Making Sense of Privacy and Data Protection: A Prospective Overview in the Light of the Future of Identity, Location-Based Services and Virtual Residence in the Institute for Prospective Technological Studies: Report Eur 20823 En," *Security and Privacy for the citizen in the post-September 11 digital age: a Prospective overview* (2003).

[460] Bergelson, *"It's Personal, but Is It Mine?"*, p. 415

[461] Although the focus of this section is primarily on the Federal Constitution the major points of the discussion are applicable to the Constitutions of the individual states. Thus, although a number of state constitutions expressly protect privacy rights (e.g. Arizona Constitution, ArticleII, para.8; California Constitution, ArticleI, para.1; Illinois Constitution, ArticleI, para.6), these state constitutional mechanisms are subject to same criticisms since they impose restrictions only on governmental activities; (Reidenberg, "Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?.", p. 208, fn 61). See also Schwartz, *Data Privacy Law: A Study of United States Data Protection*., p. 9: "For the corresponding rights at the state level, each state also has its own constitution that strives to protect civil liberties in a manner similar to the federal constitution."

[462] James Q. Whitman, "The Two Western Cultures of Privacy: Dignity Versus Liberty," *Yale L.J.* 113, no. (2004)., p. 1211-12

[463] Ibid.

[464] According to Gormley, "if privacy was explicitly acknowledged anywhere in the early contours of American law, it was within the folds of criminal procedure, where even in the early days of colonial life there existed a strong principle, inherited from English law, that a "man's house is his castle; and while he is quiet, he is well guarded as a prince in his castle." … Such a fierce protection of the inner sanctum of the home therefore made its way into the US Constitution in the fashion most relevant to citizens of the early American period. A prohibition against the quartering of soldiers was placed in the Third Amendment; … A requirement of particularized warrants to guard against unreasonable searches and seizures was embodied in the Fourth Amendment." (Ken Gormley, "One Hundred Years of Privacy," *Wis. L. Rev.* (1992)., pp. 1358-59)

privacy in the US in general, while the subsequent sections both explain how individual constitutional norms are invoked in the context of information privacy and describe what aspects of the personal data problem they do and do not address.

3.2.1. The scope of the constitutional protection of information privacy

To fully appreciate the special role of the Constitution of the United States in the information privacy system one has to first understand the nature and function of this document in the US legal order. The ideas driving the adoption of the Constitution were the establishment of the federal government and the protection of the American people from possible tyranny by placing a limitation on government powers.[465]

The second goal referred to above has had a major impact on the scope of all constitutional rights in the United States. Moreover, when it comes to the issue of the constitutional protection of information privacy, the relevant literature clearly points out the main implications of the Constitution. Firstly, constitutionally protected privacy interests only impose restrictions on a state's actions, whereas the data processing practices of private entities are not subject to these constitutional constraints.[466] Secondly, although the Constitution prevents the government from acting in certain ways, it does not impose upon it positive duties, including the duty "to create data protection that allocates the burdens and benefits of the state's information use."[467] Furthermore, the Constitution does not demand a baseline of information privacy protection. Finally, and provided the limits on a state's use of personal information are respected, the emphasis "on the restraint of government rather than the limitation of behaviour between citizens … creates a basic regulatory philosophy that favours the free flow of information."[468]

Another important aspect of the constitutional protection of personal data in the US is the absence in the Constitution of an express right to privacy, let alone

---

[465] Akkermans, *The Principle of Numerus Clausus in European Property Law*., Schwartz & Reidenberg, *Data Privacy Law*, p. 29; see also Schwartz, *Data Privacy Law: A Study of United States Data Protection*., p. 6: "The US Constitution … focuses on the allocation of power among the branches of the federal government and the division of legal authority between the federal government and the states."This doctrine is generally referred to as "state action" and is explained in a series of US Supreme Court decisions, e.g. *DeShaney v. Winnebago County Department of Social Services*, 487 US 189 (1989) with regard to the Substantive Due Process Clause: "[Nothing] in the language of the Due Process Clause itself requires the State to protect the life, liberty, and property of its citizens against invasion by private actors. The Clause is phrased as a limitation on the State's power to act, not as a guarantee of certain minimal levels of safety and security. … Its purpose was to protect the people from the State, not to ensure that the State protected them from each other. The Framers were content to leave the extent of governmental obligation in the latter area to the democratic political processes…"

[466] Solove, "Privacy and Power", p. 1435; Schwartz, *Data Privacy Law: A Study of United States Data Protection*., p. 6;

[467] Solove, "Privacy and Power", p. 1435

[468] Schwartz, *Data Privacy Law: A Study of United States Data Protection*., p. 6

information privacy. The sources of constitutional protection in the field are, however, contained in several amendments to the text, which have been interpreted by the US Supreme Court as protecting various aspects of an individual's privacy against government intervention. When applied to the information privacy context, these amendments have been invoked to prevent the government "from carrying out certain kinds of collection, utilization and disclosure of personal information."[469] The provisions mentioned most often as the legal basis of such protection are the Substantive Due Process Clause of the Fourteenth Amendment, the Fourth Amendment prohibition of unreasonable searches and seizures, and the Fifth Amendment bar on self-incrimination.[470] The following sub-sections will, therefore, address each of these provisions individually, with a special emphasis on the scope of the protection granted and the remaining lacunas in the legislation.

3.2.2. Substantive Due Process Clause of the Fourteenth Amendment

The first section of the Fourteenth Amendment, also referred to as the Substantive Due Process Clause, prohibits deprivation by any state of any person's "life, liberty, or property, without due process of law."[471] As Chemerinsky explains, "substantive due process asks the question of whether the government's deprivation of a person's life, liberty, or property is justified by a sufficient purpose … [or] whether there is a sufficient substantive justification, a good enough reason for such a deprivation."[472] Accordingly, the courts have been using Substantive Due Process to safeguard rights that are not otherwise enumerated in the Constitution.[473]

The clause became potentially important for personal data protection after the US Supreme Court expressly found that the notion of privacy, albeit initially in cases involving issues of contraception and abortion, was covered by the concept of personal liberty as secured by the Fourteenth Amendment. In the landmark case of

---

[469] Ibid., p. 29

[470] Ibid., p. 29

[471] US Constitution, I Am., s.1

[472] A related concept to procedural due process, in contrast, "asks whether the government has followed the proper procedures when it takes away life, liberty or property." (Erwin Chemerinsky, "Substantive Due Process," *Toronto Law Review* 15 (1999)., p. 1508)

[473] Ibid., pp. 1505, 1509-10: "There are two main areas where courts use substantive due process. The first is in the protection of unenumerated constitutional rights. The origin of this is the Lochner [*Lochner v. New York*, 198 US 45 (1905)] era substantive due process decisions. *Lochner* proclaimed freedom of contract to be a fundamental right under the due process clause. [id, at 53] Meyer [*Meyer v. Nebraska*, 262 US 390 (1923) at 399] and Pierce [Pierce v. Society of Sisters, 268 US 510 (1925) at 535] proclaimed the right to control the upbringing of children to be a fundamental right." … "Since 1937, the Court has repudiated economic due process. [West Coast Hotel Co. v. Parrish, 300 US 379 (1937) at 391]. … [However] In the first third of the century, the Court did not use substantive due process only in the economic area, it also used it to protect civil liberties and these cases continue to this day."

Griswold v. Connecticut,[474] where the court declared that an individual has a constitutional right to privacy, the majority in part, and Justice Harlan in his concurring opinion, both based the protection of decisional privacy with regard to contraception on the Substantive Due Process Clause.[475] In *Roe v. Wade*, Justice Blackmun explained that the "right of privacy, whether it be found in the Fourteenth Amendment's concept of personal liberty and restrictions upon state action or … in the Ninth Amendment's reservation of rights to the people, is broad enough to encompass a woman's decision whether or not to terminate her pregnancy."[476] In the 1977 *Whalen v. Roe* decision,[477] the Supreme Court extended its substantive due process privacy protection to personal data, and shaped what is often referred to as the "constitutional right to information privacy,"[478] also worded as "the individual interest in avoiding [the] disclosure of personal matters."[479] After *Whalen*, the Supreme Court reaffirmed the existence of the constitutionally protected interest in information privacy in *Nixon v. Administrator of General Services*,[480] ruling that ex-president Nixon had a legitimate interest in the records of private communications with his family, doctor, and minister.[481]

However, for several reasons, the applicability of the Substantive Due Process Clause to the modern personal data problem is somewhat limited. The first limitation, according to Solove, is inherent in the way the *Whalen* court formulated the information privacy interest, namely, in terms of the non-disclosure of information, i.e. privacy as secrecy, instead of privacy as control. *Whalen* concerned a New York statute which required that computerized records be created and kept about patients who obtained prescriptions for certain, potentially addictive, medications. The appellees contended that the statute infringed upon their privacy. Firstly, the mere existence of a computerized database containing the details of the patients using classified drugs created the possibility that this information could be abused, and thereby violated an individual's interest in "avoiding [the] disclosure of personal matters."[482] Secondly, concerns about the possibility of the public disclosure

---

[474] 381 US 479 (1965)

[475] The majority found this right to be within the "penumbras" or "zones" of freedom created by the first eight amendments and therefore protected against state intervention by due process. Justice Harlan argued for the protection of the right to privacy on its own merits, as "implicit in the concept of ordered liberty" protected by the Fourteenth Amendment.

[476] *Roe v. Wade* 410 US 113 (1973), at 153

[477] 429 US 589 (1977); Justice Brennan, concurring, explained: "[Broad] dissemination by state officials of such information … would clearly implicate constitutionally protected privacy rights, and would presumably justified only by compelling state interests." Ibid, at 606

[478] Solove, *Information Privacy Law*., p. 400

[479] *Whalen*

[480] *Nixon v. Administrator of General Services* 433 US 425 (1977)

[481] Not a government minister but a Christian minister. Such exsemptions were not maid regarding the records pertaining to his official duties (Ibid.).

[482] *Whalen*, at 600

of such sensitive facts made some patients and their doctors unwilling to take or prescribe the required medications, thereby undermining the former's independence to make important decisions.[483] The court recognized a constitutionally protected interest in the non-disclosure of private information, although it also found that there was no violation of the said interest since the state had taken adequate precautionary measures against disclosure.[484] The problem with the decision, in Solove's view, lies in its mis*conceptualis*ation of the problem. Solove contends that the plaintiffs' argument "was not that disclosure was the real privacy problem [but rather]… that the collection of and greater access to their information made them lose control over their information. A part of themselves – a very important part of their lives – was placed in the distant hands of the state and completely outside their control."[485] Furthermore, "the anxiety caused by living under such a regime"[486] was not taken into account.

The second limitation of the Substantive Due Process Clause's potential when it comes to information privacy protection concerns the great uncertainty relating to the scope and content of the protected right. The fact is that ever since recognizing the existence of the constitutional right to information privacy, the Supreme Court has done little to establish its boundaries and content.[487] As a result, protection under the Substantive Due Process Clause continues to be uncertain, with the lacunas filled in by the lower federal courts in ways that are not always beneficial for information privacy. For instance, although most federal circuit courts have recognized such a right,[488] the Sixth Circuit Court has adopted a much more limited version thereof based on a narrow interpretation of the XIV Amendment. In *J.P. v. DeSanti*, the circuit court rejected the idea that there is a general constitutional right to the non-disclosure of personal information: "Absent a clear indication from the Supreme Court…we will not construe isolated statements in *Whalen* and *Nixon* more broadly than their context allows."[489] Instead, "any constitutional right to privacy must be restricted to those personal rights that can be deemed fundamental or implicit in the

---

[483] Ibid.

[484] Ibid, at 601-02

[485] Solove, "Privacy and Power", p. 1436

[486] Ibid.

[487] For examples of such an evaluation of the information privacy jurisprudence of the Supreme Court, see Solove, "Privacy and Power", p. 1437 ("From then on, however, the Court did little to develop the right of information privacy."); citing *Davis v. Bucher,* 853 F.2d 718, 719 (9th Cir. 1988) (the right "has been infrequently examined; as a result, its contours remain less than clear.")

[488] Solove, Rotenberg and Schwartz, *Information Privacy Law*., p. 401, referring to *Barry v. City of New York*, 712 F.2d 1554, 1559 (2d Cir. 1983); *United States v. Westinghouse Electric Corp*., 638 F.2d 570, 577-80 (3d Cir. 1980); *Walls v. City of Petersburg,* 895 F.2d 188, 192 (4th Cir. 1990); *Plante v. Gonzalez*, 575 F.2d 1119, 1132, 1134 (5th Cir. 1978); *Kimberlin v. United States Dep't of Justice*, 788 F.2d 434 (7th Cir. 1986); *In re Crawford,* 194 F.3d 954, 959 (9th Cir. 1999)

[489] DeSanti, 653 F.2d (6th Cir. 1981) at 1089

concept of ordered liberty"[490] and as protected by the language of the Amendment. In the absence of more precise guidelines, whether a particular instance of disclosure threatens a fundamental right or liberty is decided on a case-by-case basis, leading to even more uncertainty about the scope of the protection that is available. In *Kallstrom*, the Sixth Circuit Court found that undercover police officers have a constitutionally protected privacy interest in some personal information contained in their personnel files under the Substantive Due Process Clause,[491] since the files "implicate a fundamental liberty interest, namely, their lives, their families' lives, and their personal security,"[492] which if released could be threatened by "a violent gang likely to seek revenge"[493]. The information pertaining to "private sexual matters" was also found to "warrant constitutional protection against public dissemination."[494] However, the correctional officers' social security numbers were not found to be sufficiently sensitive information to require constitutional protection, despite the threat of retaliation faced.[495] Moreover, the release of personal financial affairs[496]or records on HIV infection[497] have likewise not been regarded as sufficiently sensitive to prevent their publication.

Overall, the significance of Substantive Due Process when it comes to resolving the personal data problem as defined by US commentators is considerably diminished. Firstly, as interpreted in *Whalen* and *Nixon*, it only protects information privacy that is understood as the non-disclosure of personal information. Secondly, the ambiguous definition of the scope and content of the right at hand permits an even narrower reading of the clause, limiting protection to a few kinds of personal information pertaining to an abstract notion of liberty.

3.2.3. V Amendment

The Fifth Amendment provides that "[n]o person … shall be compelled in any criminal case to be a witness against himself…."[498] In this way, the Amendment establishes a privilege against self-incrimination and also prohibits the government from compelling individuals to disclose incriminating information about themselves. In so doing, the Fifth Amendment limits the government's power to collect data about its citizens.[499]

---

[490] Ibid., at 1090
[491] *Kallstrom* 136 F.3d at 1059
[492] Ibid., at 1062
[493] *Kallstrom* 136 F.3d at 1063
[494] *Bloch v. Ribar*, 156 F.3d 673, 686 (6th Cir.1998)
[495] *Barber v. Overton*, 496 F.3d 449, 456 (6th Cir.2007)
[496] *Overstreet v. Lexington-Fayette Urban County Gov't*, 305 F.3d 566, 575 (6th Cir.2002)
[497] *Doe v. Wigginton*, 21 F.3d 733 (6th Cir.1994)
[498] US Constitution, V Amendment
[499] Solove, Rotenberg and Schwartz, *Information Privacy Law*., p. 208

The most obvious limitation of the Fifth Amendment as an information privacy protection tool is that it is only applicable within the scope of criminal proceedings. Moreover, as it is applied by the courts, it does not create a right to the general protection of information privacy or guarantee the non-disclosure of personal matters in criminal proceedings, instead only providing protection against "compelled self-incrimination."[500] Specifically, this means that, as currently interpreted by the Supreme Court, the Fifth Amendment does not prevent the government from requiring an individual to produce his personal papers and records in general.[501] Moreover, nor does the Amendment protect against the issuing of subpoenas for personal records held by third parties (e.g. private sector data collectors). The Supreme Court explained that "the Fifth Amendment privilege is a personal privilege: it adheres basically to the person, not to information that may incriminate him."[502] In other words, what the Fifth Amendment is only meant to prevent is "[i]nquisitorial pressure or coercion against a potentially accused person, compelling her, against her will, to utter self-condemning words or produce incriminating documents."[503] Furthermore, to be within the scope of its protection, the information must be "testimonial" in nature, which, as follows from the case law, does not include fingerprinting, photographing, taking measurements, writing or speaking for identification purposes, and having blood or bodily fluids drawn and tested.[504]

3.2.4. IV Amendment

The Fourth Amendment protects "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." It provides that "no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." [505] Some commentators claim that the right to prevent unlawful searches and seizures forms the basis of and gave rise to the American approach to privacy.[506] Moreover, when it comes to information privacy in

---

[500] *Fisher v. United States*, 425 US 391 (1976)
[501] *Shapiro v. United States*, 335 US 1 (1948)
[502] *Couch v. United States*, 409 US 322 (1973)
[503] Ibid.
[504] *Schmerber v. California,* 384 US 757 (1966) cited in Solove, Rotenberg and Schwartz, *Information Privacy Law*., p. 201
[505] US Constitution
[506] "To Americans, the starting point to [an] understanding of the right to privacy is … to be sought in the late eighteenth century, and especially in the Bill of Rights, with its vigorous circumscription of state power. In particular, "privacy" begins with the Fourth Amendment: At its origin, the right to privacy is the right against unlawful searches and seizures. It is thus a right that inheres in us as free and sovereign political actors, masters in our own houses, which the state is ordinarily forbidden to invade. Over time, to the American mind, the early republican commitment to "privacy" has matured

particular, the Amendment has been recognized as significantly limiting the power of the government to collect data as a form of search or seizure.[507]

In the 1886 decision of *Boyd v. United States*,[508] the US Supreme Court forbade the government from seizing the documents of a merchant, which it regarded as a violation of the Fourth Amendment. The Court explained that:

> *It is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offence; but it is the invasion of his indefeasible right to personal security, personal liberty and private property, where the right has never been forfeited by his conviction of some public offence.*

Some commentators regard the *Boyd* decision as the first in a line of constitutional privacy jurisprudence.[509] The pattern was further developed in a series of wiretapping cases. In 1928, in *Olmstead v. United States*[510], the Supreme Court majority found that there was no violation of the Fourth Amendment by intercepting phone messages since there was no entry into the plaintiffs' houses or offices. The court explained that "the well-known historical purpose of the Fourth Amendment … was to prevent the use of government force to search a man's house" whereas "the wires beyond his house, and messages while passing over them, are not within the protection of the Fourth Amendment."[511] The case is, however, renowned for Justice Brandeis' dissent wherein he states that the Amendment's protection extends beyond the physical walls of the house to secure the privacy of an individual against government intervention "whatever the means employed."[512] The court developed this line of reasoning in *Katz v. United States*[513] when it ruled that although there was no physical entry into the home of the petitioner, the recording of conversations from public phones constituted a violation of the Fourth Amendment[514], which protected "people, not places."[515] The court explained that "what a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in the area accessible to the public, may be constitutionally protected."[516] In his concurring opinion, Justice Harlan established a widely used test for the reasonable expectation of privacy.

---

into a much more far-reaching right against state intrusion into our lives." (Whitman, "The Two Western Cultures of Privacy: Dignity Versus Liberty.", pp. 1211-12)

[507] Solove, Rotenberg and Schwartz, *Information Privacy Law*., p. 208

[508] *Boyd v. United States*, 116 US 616 (1886) hereinafter referred to as *Boyd*

[509] See e.g. Whitman, "The Two Western Cultures of Privacy: Dignity Versus Liberty.", pp. 1211-12

[510] 277 US 438 (1928)

[511] 277 US 438 (1928)

[512] 277 US 438 (1928)

[513] 389 US 347 (1967)

[514] 389 US 347 (1967)

[515] Ibid.

[516] Ibid.

Under this test, the Amendment affords protection if (a) a person exhibits an "actual (subjective) expectation of privacy" and (b) "the expectation [must] be one that society is prepared to recognize as 'reasonable.'"[517]

Despite its acknowledged role in setting limits for the collection of information by the government, the Fourth Amendment's potential as a data protection tool is, however, limited. The basic criticism arises from the fact that the Amendment's protection is based on an understanding of privacy as secrecy,[518] which is "a discrete commodity, possessed absolutely or not at all."[519] Indeed, in *Katz* the Supreme Court had already explained that "what a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[520] In other words, the Fourth Amendment does not establish any rules for the processing of information that is not secret, or is left open to public scrutiny, e.g. on the web, or has even been revealed to only a small number of other parties. The court has already adopted this approach in, e.g. *Smith v. Maryland*,[521] when it held that there was no reasonable expectation of privacy in the phone numbers one dials, since they are communicated to a phone company. Similarly, financial records possessed by third parties have also been found to not be private and they are, therefore, not protected by the Fourth Amendment.[522]

The second point of criticism pertains to the "reasonable expectation of privacy" standard. Solove et al. clearly highlight that such a standard, as applied by a court, is not objectively verifiable since the court does not rely on any empirical evidence of what society is prepared to recognize as reasonable.[523]Moreover, even if it did, as Cate and Litan note, the threshold of what society is prepared to consider to be reasonable or normal is "under renewed scrutiny"[524] following the September 11th terrorist attacks and other security concerns, all of which have resulted in increased government surveillance. As Solove, Rotenberg, and Schwartz point out, there is a fundamental flaw or paradox at the core of the reasonable expectation of privacy test: "legal protection is triggered by people's expectations of privacy, but those expectations are, to a notable extent, shaped by the extent of the legal protection of privacy."[525]

To summarize, the attempts to address the personal data problem by constitutional means fail both for reasons of the specific nature of the US

---

[517] Ibid.
[518] Daniel Solove explains this point further in Solove, "Privacy and Power", p. 1435
[519] Laurence Tribe, *American Constitutional Law* 2nd ed. (1988)., quoting Justice Marshall's dissent in *Smith v. Maryland,* 442 US 735 (1979)
[520] 389 US 347 (1967)
[521] 442 US 735 (1979)
[522] *The United States v. Miller,* 425 US 435, 442-43 (1976)
[523] Solove, Rotenberg and Schwartz, *Information Privacy Law*., p. 251
[524] Cate, "Constitutional Issues in Information Privacy.", p. 9
[525] Solove, Rotenberg and Schwartz, *Information Privacy Law*., p. 251

Constitution and because of the conceptualisation of the problem as one of protecting the secrecy of information. However, commentators such as Schwartz and Reidenberg also point out that one cannot reasonably expect a document of the magnitude of the US Constitution to provide a detailed solution to the personal data problem. "The United States Constitution sets forth a structure for national dialogue by reserving only the most important principles to the higher law; it relegates most issues to the give-and-take of normal politics."[526] The following section focuses on the product of the political process – information privacy legislation.

3.3 Statutory protection

The purpose of this section is to describe both how US regulatory bodies have approached the problem of data processing as it emerged from the information revolution and whether that approach is regarded as adequate by American commentators. The following sections will, thus, focus on the Code of Fair Information Practices and its implementation in the public and private sectors.

3.3.1. Code of Fair Information Practices

The US federal government did respond to increased public concerns pertaining to the new information practices resulting from the information revolution. The Department of Housing, Education, and Welfare (HEW) was assigned the task of analyzing and making recommendations about the harmful consequences that could result from computerized information systems, including uses of an individual's social security number.[527] In 1973, the HEW Committee released a highly influential report, *Records, Computers, and the Rights of Citizens,* wherein it stressed the need for regulatory involvement since "the natural evolution of [the] existing law will not protect personal privacy from the risks of computerized personal data systems."[528] The HEW report contained a proposal to introduce a Code of Fair Information Practices to establish five basic principles: a ban on secret personal data record-keeping systems; the right of an individual to both find out what information pertaining to him has been collected and how it is used; the right of an individual to prevent information pertaining to him from being used for a purpose other than the one for which it has been collected; the right of an individual to be able to correct or

---

[526] Schwartz & Reidenberg, *Data Privacy Law*, p. 29

[527] US Department of Health, Education, and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, *Records, Computers, and the Rights of Citizens*, (Washington, D.C.: Government Printing Office, 1993)

[528] Regan, *Legislating Privacy*, p. 75-76

amend a record of identifiable information about him; and, finally, a data-processing organization must ensure the reliability of, and take reasonable precautions to prevent the misuse of, data.[529]

What made the Code stand out from the data protection efforts already in existence, for example, the privacy torts, was the fact that it effectively acknowledged the separate essence of and "gave…meaning to the idea of *information* privacy."[530] Regan points out that the assumption behind the Fair Information Practices' Code was not to prevent information from being collected, but "delineating fairness in information practices would protect individual privacy."[531] Solove et al characterize the Code as a general attempt "to correct [the] information asymmetries" between an individual and data-processing organizations resulting from massive data transfers.[532] Accordingly, the document is, in essence, a set of rights assigned to individuals and responsibilities imposed on organizations with regard to the transfer and use of personal information.[533] Regan agrees with the characterization of the document as empowering individuals, since "the Code was framed around the concept of giving individuals the means to protect privacy as they saw fit."[534]

US commentators agree on the significant role the Code played in formulating information privacy standards, not only in the United States, but also on an international level. Regan asserts that the Code provided "the framework for subsequent policy formulating."[535] Moreover, according to Rotenberg, the Code was highly influential in the adoption of the Organization for Economic Cooperation and Development's Recommendations Concerning and Guidelines Governing the Protection of Privacy and Transborder flows of Personal Data ("OECD Guidelines").[536] Furthermore, "the level of consensus … about the viability of Fair Information Practices as a general solution to the problem of privacy protection is remarkable."[537]

3.3.2. Implementation of the Code

Despite its positive evaluation and tremendous influence on defining the data protection problem and shaping privacy policies, the Code's significance when it

---

[529] US Dep't of Health, Educ. & Welfare, *Records, Computers, and the Rights of Citizens: Report of the Secretary's Advisory Comm. on Automated Personal Data Systems* 29-30, 41-42 (1973) ("HEW Report")
[530] Regan, *Legislating Privacy*, p. 75-76
[531] Ibid., p. 76-77
[532] Solove, Rotenberg and Schwartz, *Information Privacy Law*., p. 578
[533] Ibid.
[534] Regan, *Legislating Privacy*, p. 76-77
[535] Ibid.
[536] Marc Rotenberg, "Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)," *Stan. Tech. L. Rev.* 1 (2001).
[537] Ibid.

comes to finding a solution to the personal data problem is limited by the facts that it does not have a directly binding effect and its principles needed to be implemented. As Rotenberg points out, "the coverage of the US law [in this respect – N.P.] was uneven: Fair Information Practices were in force in some sectors and not in others."[538] The most significant difference in the implementation of the principles pertains to the different regulatory approaches to data processing taken by the government and businesses.

The US Congress responded to the HEW's recommendations by introducing the s.3418 bill - a draft of an omnibus law "comprehensive in its scope"[539], which concerned data protection in all aspects of life. The bill covered both the automated and manual processing of personal information in federal, state, and local governments as well as in the private sector. It adopted a regulatory approach, fully implementing the principles of the Fair Information Practices' Code, and empowered individuals by giving them the rights to access and amend their files and be informed about the dissemination of their personal data. Moreover, the bill also provided for a supervisory authority – a Federal Privacy Board - with a wide range of powers, including the authority to: enter premises where data were held; compel (by subpoena) the production of documents; hold hearings regarding violations; and order an organization to cease unauthorized information practices.[540]

However, under pressure from both public and private sector organizations, this legislative initiative ended with the passage of weakened legislation.[541] Public sector organizations (government agencies) argued that these powers would inhibit the effectiveness of their operations, while private sector entities, members of whom were witnesses during congressional hearings, testified that compliance with the regulations would be disproportionally burdensome given that there was not enough concrete evidence of information abuses in the private, as opposed to the public, sector.[542] The representatives of industries were joined by Alan Westin in promoting their alternative proposal to allow self-regulation, i.e. "to urge companies to enact voluntary protections for personal information."[543] The proposal to create a supervisory authority was opposed both by government agencies and the HEW Committee itself. The former argued that "implementation can best be accomplished by holding agencies accountable … and subjecting their performance to congressional and public scrutiny." [544] To establish a separate agency would only

[538] Rotenberg, "Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)."
[539] Regan, *Legislating Privacy*, p. 77
[540] Ibid.
[541] Ibid, p. 78
[542] Ibid; US Senate Committee, *Privacy*, pp. 515, 450-451
[543] US Senate Committee, *Privacy*, p. 75
[544] Ibid., p. 444

"increase costs, fragment responsibility, and delay implementation of the bill while the commission develops its guidelines and rules."[545] The HEW Committee, in turn, grounded its opposition on the absence of public support for "an agency of the scale and pervasiveness [proposed]. … Such regulation or licensing, moreover, would be extremely complicated, costly, and might uselessly impede desirable applications of computers to record keeping."[546] As a result, the idea of a supervisory agency and an omnibus regulation of the private sector were omitted from the piece of legislation that was adopted. According to Regan, such an outcome is not uncommon in American politics. "Most legislation" she says, "can be explained by examining the conflicts and compromises among the interests affected."[547]

In the case at hand, the interests opposed to more extensive data processing regulation were better organized, had more resources and, therefore, succeeded.[548] Some authors consider this outcome to be consistent with the American regulatory culture, which "has historically emphasized the restraint of government rather than the limitation of behaviour between citizens."[549] In any case, what the US approach to regulating data processing now represents is a system: with inherent gaps; no supervisory authority;[550] where public and private sector data processing have been treated separately; and with a 1974 Privacy Act, which regulates public sector processing, that is a reduced version of the s. 3418 bill and is generally in line with the Fair Information Practices' Code.[551] On the other hand, private sector data processing is an area almost entirely left to self-regulation, albeit with the exception

---

[545] Ibid.

[546] Ibid., p. 43

[547] Regan, *Legislating Privacy*, p. xii; for the same ideas on the influence of the lobby on the outcome of the US legislative process, see David Lowery, *Interest Groups*.

[548] Regan, *Legislating Privacy*, p. xii

[549] Schwartz & Reidenberg, *Data Privacy Law*, p. 6: "American law has historically emphasized the restraint of government rather than the limitation of behaviour between citizens. From the earliest days of the republic, federal and state constitutional protections sought to assure freedom from government interference for the press and communications. (U.S. Constitution, I Amendment). This emphasis creates a basic regulatory philosophy that favours the free flow of information."

[550] Although several civil liberties' offices have been created since September, 11, 2001, US privacy experts agree that "none of them are functionally equivalent to data protection authorities in Europe. … These new privacy officers are not structurally independent of the government bodies that they are responsible for overseeing; and they do not have the power to investigate and sanction privacy violations." (Francesca Bignami, "The U.S. Privacy Act in Comparative Perspective," in *Public Seminar on PNR/SWIFT/Safe Harbour: Are Transatlantic Data Protected?* (Brussels2007)., pp. 1, 7); see also Marc Rotenberg, "The Privacy Act and the Data Protection Granted to Non US Citizens," in *Public Seminar on PNR/SWIFT/Safe Harbour: Are Transatlantic Data Protected?* (Brussels2007).

[551] Although the Privacy Act does cover most records maintained by the state and local officials, it also has a wide range of other exceptions. For a more detailed analysis of the Act, see Rotenberg (Ibid.) who argues that, provided a few gaps are filled in, the Privacy Act is a satisfactory data protection tool in the public sector; Bignami discusses the weaknesses of the Act (Bignami, "The U.S. Privacy Act in Comparative Perspective.").

of a number of statutes, like the Video Privacy Protection Act of 1988 and the Right to Financial Privacy Act of 1978, both of which were adopted as a reaction to particularly shocking incidents of data mishandling.[552] Some areas of data processing are covered, whereas others, like a whole host of records held by libraries, charities, and merchants, are unaddressed.

In summary, commentators agree that the regulation of private sector data processing in the US is reactive rather than anticipatory, ad hoc or incremental rather than systematic and comprehensive, and fragmented rather than coherent.[553] As Bennett observes, there may be a lot of laws, but there is not much protection." [554]

To be fair, one should mention more recent, area-specific legislation in the field of data protection, for example, regarding children's data, financial data and health data (HIPPA), Genetic information non-discrimination act of 2008 etc. In the last 10 years the data processing in private sector became significantly more regulated in the information privacy laws. In addition, in December 2010 the Federal Trade Commission initiated a process of evaluation of the privacy law applicable to commercial data processing and proposing a framework of measures to protect consumer privacy, including privacy by design, privacy audits, etc.[555]

Nevertheless, although these developments have definitely been received as improvements, at the moment they still address only certain data processing sectors, meaning that the problem of the absence of an omnibus law establishing uniform data protection standards for the private sector continues to be unresolved.

4 Non-proprietary tools to fill in the gaps

As the previous analysis demonstrates, US information privacy law are routinely found to be inadequate in how they deal with the threats posed by new information practices created during the information revolution. The criticism of the current US data protection system has been followed by an extensive body of literature

---

[552] "The number of laws does not reflect [the] enormous policy success by privacy advocates. Some of these laws, notably the Video Privacy Protection Act of 1988 and the Right to Financial Privacy Act of 1978, were passed in response to specific circumstances that highlighted threats to privacy. But more importantly, the actual number of laws passed pales in comparison to the amount of congressional activity devoted to the subject and the number of laws not passed, involving, for example, medical privacy, personality tests, the sale of personal information, and the use of the social security number." Regan, *Legislating Privacy*, pp. 5-7

[553] See e.g. Regan, *Legislating Privacy*, pp. 5-7, Colin J. Bennett, "Convergence Revisited: Toward a Global Policy for the Protection of Personal Data? ," in *Technology and Privacy: The New Landscape* ed. Philip E. Agre & Marc Rottenberg (1997)., Solove, "Privacy and Power", p. 1440, etc.

[554] Bennett, "Convergence Revisited."

[555] Federal Trade Commission (Bureau of Consumer Protection) A Preliminary FTC Staff Report on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers (December 1, 2010) at <http://www.ftc.gov/reports/index.shtm#2010>

suggesting various solutions to its shortcomings. The most commonly proposed approaches to resolving the personal data problem are: the creation of new, or the expansion of already existing, torts; introduction of information privacy regulation; or, finally, the propertisation of personal information. To provide better insight into the position the propertisation argument takes in the US debate, and introduce the reader to the basic arguments for and against propertisation, each of the three alternative solutions to resolving the personal data problem need to be described and analyzed.

4.1. Retooling the system of torts

One of the more conventional options for correcting the failures of the current US data protection system is probably the proposal to retool the existing system of torts. A number of scholars have argued that information privacy should be protected through the expansion of either the tort of disclosure, the tort of appropriation, or the tort of breach of confidence.

Komuves has defended the position that courts should "take affirmative steps to prohibit [social security number] and name dissemination" by expanding the use of the torts of disclosure and appropriation.[556] The proposals to expand the former are subject to much criticism. Vera Bergelson, for example, points to the internal contradiction of the proposal. The disclosure tort, she claims, by its nature "protects only information that is kept secret."[557] To address a modern data protection problem, however, requires the abandonment of the secrecy model of privacy, for it is "not able to address many of the vital personal interests involved in the modern information economy … [where] … individuals are encompassed within a web of information about what they do, and when and why", which they disclose voluntarily.[558] Another problem with the tort of disclosure highlighted by Bergelson is the standard of the "reasonable expectation of privacy" that the tort relies on. For Bergelson, the application of that objective standard of privacy "raises both moral and practical concerns because what is *reasonably* private varies dramatically across different social, economic, and cultural groups."[559] What can reasonably be expected to remain private objectively depends on how much privacy protection one can financially afford. Bergelson concludes that "unless we, as a society, are prepared to treat individuals in different socio-economic groups differently, we cannot accept

---

[556] Flavio L. Komuves, "We've Got Your Number: An Overview of Legislation and Decisions to Control the Use of Social Security Numbers as Personal Identifiers," J. MARSHALL J. COMPUTER & INFO. L. , no. 16 (1998)., p. 574

[557] Bergelson, *"It's Personal, but Is It Mine?"*, p. 415

[558] Ibid.

[559] Ibid.

this approach."[560] In addition, increasing the internationalization of the information flow also raises the possibility of there being different standards for different jurisdictions. For instance, American companies trying to comply with "Safe Harbor" requirements may end up applying two different standards: "the higher one for European customers and the lower one for domestic customers."[561]

William Fenrich is an advocate of the expansion of the tort of appropriation (or publicity rights) to protect individuals from the unwanted commercial use of their personal information. He bases his choice of this tort on the fact that it is based in property, "which further enhances its flexibility as a common law doctrine, and opens up its ability to adapt to changing standards of technology and value."[562] To support his proposal, Fenrich refers to Nimmer, who claims that the right of publicity should not be limited solely to celebrities.[563] Nimmer claims that "it is impractical to draw a line as to which persons have achieved the status of celebrity and which have not."[564] Instead, it should be held that "every person has the property right of publicity, but the damages which a person may claim for infringement … will depend upon the value of the publicity appropriated which in turn will depend in great measure upon the degree of fame attained by the plaintiff."[565] In other words, the right should be accorded to everyone, but the value thereof will differ. As a number of commentators recognize, however, the problem with proposals to expand the tort of appropriation to cover personal information is that it would necessitate an implicit recognition of the proprietary nature of such data and the ignoring of the other, more personal, side of information privacy.[566] If, however, a proprietary interest is the one which should be protected with regard to information privacy within the framework of torts, why not introduce a property right in personal information in general, or, as Bergelson puts it, "why should a proprietary interest be regulated entirely through torts?"[567]

The alternative, which is quite different from the two proposals discussed above, is the suggestion made by Jessica Litman. She argues that it is possible to consider improper information practices as a breach of trust and, therefore, covered by the tort of breach of confidentiality.[568] She starts her argument by listing instances where the law of tort finds various data collectors (physicians, accountants, banks, etc.), who owe fiduciary duties to their patients or clients, accountable for the

---

[560] Ibid.
[561] Ibid.
[562] Fenrich, "Common Law Protection of Individuals' Rights in Personal Information.", pp. 997-8
[563] Ibid., p. 999
[564] Melville Nimmer, "The Right of Publicity," *Law & Contemp. Probs.* 19 (1954)., note 329 at p. 217
[565] Nimmer note 329 at p. 217
[566] Bergelson, *"It's Personal, but Is It Mine?"*, p. 416; Jessica Litman, "Information Privacy / Information Property," *Stan. L. R.* 52 (2000).
[567] Bergelson, *"It's Personal, but Is It Mine?"*, p. 416;
[568] Litman, "Information Privacy / Information Property.", p. 1308

unauthorized disclosure of the information involved.[569] The courts, however, insist that the obligation to keep information confidential derives from the exceptional nature of the relationships between these data collectors and data subjects.[570] Litman proceeds to argue that in fact the relationship between an individual and any other data collector to whom personal information has been revealed daily also has this special nature, i.e. it is based on trust. Indeed, "we expect the merchants, banks, and insurance companies we deal with to respect our privacy … [because] … merchants, banks, insurance companies, and brokers encourage it. … Without that trust, we'd be reluctant to volunteer our credit card numbers; we'd think twice before making embarrassing purchases or watching certain pay-per-view movies."[571] Moreover, "the fact that businesses respond to consumer privacy complaints with defensive apologies rather than toughing it out suggests that that perception is one businesses are aware of, intentionally cultivate, and may even to some extent share."[572] Accordingly, they should act subject to implicit constraints of confidentiality.[573] Litman continues that once a solution via a breach of the tort of confidentiality is found to be appropriate, it is relatively easy to implement. A relational approach to data privacy protection lying at the core of the confidentiality solution "carries significant intuitive appeal" and therefore "seems comparatively innocuous, since its scope can easily be limited by confining the definition of a qualifying relationship … [and] courts could be persuaded to take that route to that destination."[574] Moreover, because the adoption of a remedy via torts is incremental and gradual, it makes it easier to persuade cautious judges to endorse the theory safely, "a little bit at a time."[575] However, Litman is conscious of the weaknesses of the proposed solution. Its gradual approach and flexibility, which make it plausible, simultaneously weaken it by permitting the courts to limit the proposal based on free speech or informational policy issues, while opponents of restricted data practices seek to narrow the exclusive definition of the relationships that it applies to.[576] Furthermore, only minor changes to the current torts would have little effect on data protection, whereas more definite changes in the case law, when in the context of the US political system, would probably result in the businesses concerned undertaking strong lobbying at

---

[569] E.g. see *Horne v. Patton*, 287 So.2d 824 (Ala. 1973); *Doe v. Roe*, 400 N.Y.S.2d 668 (N.Y. App. Div. 1977); *McCormick v. England*, 494 S.E.2d 431 (S.C.Ct. App. 1997))] Accountants and banks have been held liable for divulging information about their customers. [Rubenstein v. South Denver Nat'l Bank, 762 P.2d 755 (Colo.Ct.App. 1988)]; Edward L. Raymond, Jr., Annotations, Bank's Liability Under State Law, for disclosing financial information concerning a depositor or customer, 81 A.L.R. 4th 377 (1990)

[570] Litman, "Information Privacy / Information Property.", p. 1308

[571] Ibid.

[572] Ibid., p. 1309

[573] Ibid.

[574] Ibid., p. 1311

[575] Ibid., p. 1312

[576] Ibid., p. 1313

the US Congress to "pre-empt the pesky state tort laws with a data privacy law they found more congenial."[577]

Most commentators come to the common viewpoint that the retooling of the existing system of torts may mitigate some of the current problems, but would leave the most significant issues of information privacy unresolved. This conclusion is based on the inherent weaknesses, or rather specificities, of American torts in general and on the nature of the personal data problem itself. Let us now first consider the inherent limitations of the system of torts.

The absence of homogeneity and its unsystematic character are probably the most obvious limitations of the law of torts, which make it impossible to develop a coherent approach to information privacy entirely through this method. As one may recall, the US law of tort is largely the common law. As a result, Michaels explains, "[law] students are taught the law as a line of cases, and as a forum for constant struggles between arguments and counterarguments, rather than as a substantive whole."[578] In case law, he continues, "legal reasoning is both more case-specific and more inductive than in Continental European systems. Americans doubt that there is 'one right answer' to every case that can somehow be distilled from the legal system as a whole: court decisions are the result of the better argument made by the winning party, not by logical deduction from a coherent system of law."[579]

The second limitation is that torts give individuals only negative rights by protecting recognized interests from infringement.[580] However, they do not create any positive obligations for data collectors to fulfil. Moreover, as Arthur Miller points out, "in some ways most significantly, the existing common-law structure [gives] the data subject a right to participate in decisions relating to personal information about him, a right that is essential if he is to learn whether he has been victimized by a privacy invasion."[581]

Furthermore, remedies in the law of tort have little preventative effect when it comes to information privacy infringements, at least while proving damages in the data protection cases is difficult. The common law approach involves the filing a legal suit *after* harm is inflicted and does nothing to stop harmful information practices from taking place.

Finally, when the federal government is a respondent in a tort case, the system of tortious liability is more protective of the state than the individual. It is also overcomplicated, implying that there are diverse systems and grounds of liability for federal and state officers on the basis of the violation of federal or state laws or the

---

[577] Ibid.; "Ironically, the widespread adoption of tort law liability for data misuse is perhaps the most realistic scenario for generating some sort of federal law protecting information privacy."
[578] Michaels, "American Law (United States).", p. 68
[579] Ibid., p. 71
[580] Bergelson, *"It's Personal, but Is It Mine?"*, p. 415
[581] Arthur R. Miller, The Assault on Privacy: Computers, Data Banks, and Dossiers (1971), p. 189

federal constitution. As Miller maintains, "a suit against a unit of the federal government for an invasion of privacy involves a trek through what is surely the world's most arduous obstacle."[582]

Another shortcoming of the tort solution to the personal data problem relates to the nature of the problem in itself. This point is argued by Solove, and is linked to his definition of what the personal data issue is. "The privacy problem with databases", he submits, "transcends the specific injuries and harms that the privacy torts are designed to redress."[583] In other words, by its very nature, the law of tort targets isolated acts and particular infringements and wrongs, whereas the problem with databases "does not stem from any specific act, but is a systematic issue of power caused by the aggregation of relatively small actions, each of which when viewed in isolation would appear quite innocuous."[584] Solove refers to this as the "aggregation problem" – "the fact that the whole is greater than the parts."[585] Accordingly, proposed solutions involving the reshaping of the law of tort will address only a small aspect of the personal data problem, whereas its core will remain the same.

In summary, most US commentators agree that although expanding the current system of privacy torts is plausible, it is inconsistent and unlikely to adequately address the essence of the personal data problem. The reasons for this lie in the specific features of the privacy torts, such as their reliance on the secrecy of protected information and the reasonable expectation of privacy standard. Proposals to improve torts by treating personal information as property raise the question as to why information privacy should not be recognized as a property interest in general rather than limiting it to torts. Moreover, there are some inherent limitations to the law of tort, which do not allow the creation of a general system of data protection in the US solely on their basis, with one of these shortcomings being their disregard of the aggregation problem.

4.2. Solution by regulation

Despite the claims that extensive regulation by statute is not in the American legal culture, some authors are inclined to see it as the means to address the personal data problem in the US. The content and scale of the proposed regulation of data processing differ considerably among authors, and this sub-section will touch upon only a few of the most typical proposals.

---

[582] Ibid.
[583] Solove, "Privacy and Power", p. 1434
[584] Ibid.
[585] Ibid.

It is possible to draw a spectrum of the regulatory solutions put forward, starting with those that interfere with existing data markets the least, and ending with the proposals to fully reconsider the current US system of dealing with personal data. At the start of the spectrum are default contractual rules and the introduction of property rights via legislation which, strictly speaking, is regulation, too. However, these aspects will be considered in more detail in the next sub-section, with the following pages focusing solely on the regulatory solutions that are proposed as an alternative to propertisation.

Another version of a regulatory solution further along the spectrum, and probably the most modest of the 'interfering' regulatory proposals, is the suggestion of fixing the shortcomings of the 1974 Privacy Act, namely eliminating major exceptions to the established rules of data processing and, most importantly, creating an independent privacy agency in charge of enforcing the statute.[586]

The regulatory proposals that would interfere the most in the current personal data processing regime in the US are set out by Daniel Solove. At the core of his solution is the necessity to introduce rules which cannot be contracted around and which would "govern our relationship with bureaucracies,"[587] both public and private, in order to eliminate the power inequalities created by the information revolution. Among the rules Solove proposes to limit is the currently unrestrained government officials' discretion on what records to make public,[588] along with a suggestion to make businesses introduce adequate security measures.[589] Solove agrees with Jeff Sovern and other commentators who argue in favour of an opt-in instead of an opt-out mode of giving consent to having one's data collected.[590] Solove refers to the 1995 EU Data Protection Directive as a model, and submits that it is more in line with his vision of the essence of the personal data problem as an issue of power inequalities and bureaucratic ways of handling information and making "important decisions that influence people's lives."[591] In particular, although Solove recognizes that the Directive is "far from perfect,"[592] he highlights two provisions which address the aspects of the personal data problems that are ignored in the US: the Article 15 prohibition on making decisions that have legal effects which significantly affect an individual, and which are based "solely on [the] automated

---

[586] E.g. Bignami, pp. 9-10

[587] Solove, "Privacy and Power", p. 1455-56

[588] Ibid., p. 1457

[589] Ibid., p. 1459

[590] Ibid., p. 1458; Jeff Sovern explains that opt-out systems create no incentive for businesses to make opting-out easy: "Companies will incur transaction costs in notifying consumers of the existence of the opt-out option and in responding to consumers who opt out." (Jeff Sovern, *Opting in, Opting Out, or No Options at all: The fight for control of personal information,* 74 Wash. L. Rev. 1033, 1082 (1999))

[591] For more details on how Solove *conceptualis*es the personal data problem, see Section 5.3 of this chapter

[592] Solove, "Privacy and Power", pp. 1460-61

processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc";[593] and the Article 8 prohibition on the processing of sensitive data without the express consent of an individual, subject to some necessary exceptions.[594] Solove also refers to a regulatory model that is 'closer to home' – the Code of Fair Information Practices – as the direction to follow. According to Solove, and in stating this he is joined by other commentators such as Mark Rotenberg,[595] the EU Directive was drafted under the strong influence of the Code, and the US regime of personal data protection would progress significantly if it incorporated the principles of fair information practices further.[596]

Whatever the content or scope of the proposed regulatory solutions might be, all of them are subject to one very powerful point of criticism: how likely is it that these proposals would be passed by the legislature? Indeed, as follows from the overview of the current statutory protection of personal data in the US, the country's lawmaking bodies have revealed themselves to not be very productive when regulating privacy. Firstly, as the reader may recall from how the Code of Fair Information Practices was implemented, the US Congress is highly susceptible to lobbying activities, while the interests opposed to more extensive data processing regulation are better organized and have more resources, meaning that they succeeded in 1974.[597] The reality is that these same interest groups almost certainly retain their strong positions today. Secondly, even if privacy advocates succeed and push their regulatory ideas through into legislation, as Solove points out, their efforts "may run into First Amendment problems,"[598] i.e. the regulation of data processing may be regarded as an infringement on free speech. Indeed, a tendency has already formed in US constitutional jurisprudence to hold that such regulations are unconstitutional.[599]

To summarize, despite the attractiveness of the idea of addressing the personal data problem in the US by legislative tools, the major shortcoming of this proposal is that it is not in tune with the country's political and constitutional reality. Accordingly, such issues may be the reason that other, less conventional, proposals, such as propertisation, appeal.

---

[593] 1995 EU Directive, Article 15
[594] Solove, "Privacy and Power", pp. 1461
[595] Rotenberg, "What Larry Doesn't Get."
[596] Solove, "Privacy and Power", pp. 1461
[597] Regan, *Legislating Privacy*, p. xii
[598] Solove, "Privacy and Power", p. 1458
[599] e.g. US *West v. Federal Communications Commission*

5. Conclusion

The purpose of this chapter was twofold: firstly, it intended to present US information privacy law and set out how these deal with the personal data problem, while also taking into account the criticism they are subjected to by US information privacy scholars. The second purpose was to present the US legal system and its integral part - the information privacy law - as the context where the idea to create property rights in personal data originated from. In brief, the main messages that the reader should draw from the analysis above is, first, that the formation of information privacy laws, especially privacy torts and US constitutional case law, in the eyes of some US commentators, was channelled by a one-sided *conceptualis*ation of the personal data problem as one of the secrecy of personal information. Arguably, as a result of such a narrow approach to privacy, the relevant legal norms mainly provide protection in the form of negative rights, comparable to the level of the second generation of data protection in European. The effect of the constitutional remedies is limited as the constitutional provisions are only applicable against the government. A number of statutes adopted since the 1970s introduced positive rights and administrative regulations with which to tackle the data protection problem, taking US information privacy law to the level comparable to the third and in some aspects even the fourth generation of the European data protection. However, this progress is also limited to the public sector and only the parts of the private sector data processing industry that attracted public outrage at well-publicized individual incidents of the abuse of data. Despite undeniable progress of the US information privacy legislation in recent years, a large part of private data processing, thus, continues to be unregulated. Due to the specificities of the US political system, the strength of the information industry lobby and the shortcomings of torts as a common law institution, critics of US information privacy law point out that improving the situation via legislation or the retooling of the system of privacy torts is unlikely to offer a solution to the personal data problem.

The perceived limitations of existing legal tools in preventing information privacy violations and, in a large part of the private sector, the absence of effective negative rights, makes the United States a jurisdiction wherein the emergence of an unconventional idea like the propertisation of personal data appears to be organic. The next chapter will, therefore, focus on the details and national specificities of the US propertisation argument.

Chapter 6: Correcting shortcomings of the US information privacy law by propertisation

1. Introduction

The US information privacy law, especially as applicable to the private sector, has been criticised by the US privacy scholars for offering limited or close to no tools to return to individuals control over personal data. The criticism of the US information privacy law has been followed by numerous proposals aiming to fix the alleged shortcomings of the system. The most established ones are retooling the system of torts, more regulation,[600] and, finally, propertisation of personal information. The latter has gained even more attractiveness in the eyes of its proponents given the already mentioned flaws of the first two: the peculiar nature of torts and lobbying power of the information industries in the US context. This chapter shows how property rights in personal data are, according to some commentators, able to perform where other solutions, arguably, fail, i.e. in giving the control over personal data back to the individual and create a better system of data protection in general. An important disclaimer has to be made at this point. This piece does not argue for or against introduction of property rights in personal data in the United States as a solution to the personal data problem. Instead, the reader should consider this chapter as a step preceding a full-blooded European discussion,[601] an attempt to look back at the past debate overseas and rehearse lessons learnt there to have initial points of reference when starting the European debate. In particular, it seems to be of great importance to make the reader aware of the several perspectives on property that appear in the US propertisation argument, each perspective defended from a different standpoint, bearing a different, often, non-legal meaning and performing a different function (outlined in sections 2, 3 and 4).

With this purpose in mind, this chapter will try to go beyond an obvious insight normally present in a comparative study, i.e. that when looking at the US-born idea of propertisation of personal information Europe cannot be blindly guided by the US debate but needs to develop its own view. Instead, after mapping the propertisation argument in section 2, this chapter will show that, in the US discourse, propertisation of personal information was expected to perform certain functions, namely, to give individuals some control over personal information (sections 3, 4.1 and 4.2), and generate incentives for companies in the private sector to respect privacy, create privacy enhancing technologies and, as a result, a better system of

[600] The proposals have been briefly considered in the previous chapter.
[601] Chapters 7 et seq.

data protection (sections 4.3); and thus to overcome shortcomings of the current US data protection system (outlined in section 5). Section 6 presents an outline of the ideas as to the scope of proposed property rights. It shows how different the propertisation initiatives are with regard to the approaches to regulation and content of the proposed rights, and therefore suggests that what will matter in a future European discourse is the actual content of granted rights, rather than the 'property' label. Section 7 continues the analysis of the US propertisation debate with main points of criticism towards the idea of propertisation, emphasizing again the importance in a discourse of the content of rights in personal data rather than a word used to call them, and raising a question of the necessity of an empirical study to (dis)prove some statements made in the US debate to support propertisation. Section 8 ends the analysis by making an inventory of lessons the Europeans could learn before considering the possibility of property rights in personal data. Before the analysis starts, another disclaimer should be made that since the chapter focuses on the US debate, it will draw primarily on US authors.

2. Mapping the US argument on propertisation of personal data

To get a more structured insight into the US argument for propertisation, it makes sense to divide the subject of property in personal data into three distinct issues. First, whether personal information should be regarded as an object of property rights. The second issue naturally follows from a positive answer to the first question and is with whom - individuals (data subjects), or data collectors - property rights should be vested. The third issue is, after property rights are introduced, what the default rules (if any) are that should govern their transfer.[602]

Ironically, with regard to the first issue, both information privacy opponents and privacy advocates argue for and against propertisation, albeit for different reasons. Representatives of the information industry argue for propertisation as a means to legitimize and facilitate the already existing market of data. On the other hand, Judge Richard Posner, an opponent to privacy and advocate of the uninterrupted flow of information, argues against. For Posner property rights in personal information provide a means of withholding true information from the marketplace and are therefore inefficient.[603] Some privacy advocates concur with Posner in his conclusion but for a different reason, i.e. that personal data is different

[602] However, consistent with the aim of this Chapter to consider the American idea of propertisation as a way of personal data protection, this contribution focuses on the argument for creating individual property rights in personal information and default contractual rules.

[603] The only instance when property rights in personal data are justified is when it will foster more efficient transactions (Richard A. Posner, *The Economics of Justice* (1981). at 235). It may be argued though that Posner is not against property rights in true personal information *per se*, but against vesting them with the individuals – data subjects.

from other objects and cannot be treated as property.[604] There are data protection proponents who regard a property regime as optimal for ensuring information privacy. Although, a remark should be made here that the privacy advocates do not tend to spend much time arguing in favour of propertisation per se, but, like Murphy, presume that personal information "like all information, is property"[605] and immediately move to the discussion on who should own it.[606]

When the need for property rights in personal data is agreed upon, the standpoints of the information privacy advocates and opponents are much clearer in defending who should be the owner of the data. Advocates of data protection stand for the allocation of this resource to the data subjects, whereas proponents of disclosure argue for vesting property with data collectors. According to Julie Cohen, "opponents of strengthened privacy protection think of collection of personally-identified data as 'their' property; as evidence, they point to their investment in compiling the databases and developing algorithms to 'mine' them for various purposes."[607] Those opponents of the unchained information market are consistent to argue against the need for any default rules governing the data transfers since the market already functions optimally.[608] To show how property, arguably, is able to give control of personal information back to data subjects, the following analysis will focus only on the arguments of privacy advocates.

Analysis along the lines of this roadmap promises a lot of interesting insights into the nature of property and personal data. However, the aim of this chapter is to consider the American idea of propertisation as a way of ensuring better protection of personal data, and it calls to tune the direction of analysis more finely. Therefore, the claims of privacy opponents stay outside the scope of the interest of this section, except in part helpful for better understanding of the argument on the privacy side. Besides, the anti-propertisation claims of information privacy proponents are considered only as a part of criticism of the arguments for propertisation. What is left

---

[604]More on that in section 7 on criticism of pro-property arguments; also see e.g. Samuelson, "Privacy as Intellectual Property?.", p. 1125, Schwartz, *Data Privacy Law: A Study of United States Data Protection*., Solove, "Conceptualizing Privacy.", p. 1087, Litman, "Information Privacy / Information Property.", p. 1283

[605] Richard S. Murphy, "Property Rights in Personal Information: An Economic Defence of Privacy," *Geo. L.J.* 83 (1996). pp. 2383-84

[606] Ibid.,

[607] Cohen, "Examined Lives: Informational Privacy and the Subject as Object.", p. 1378 referring to Harris S. Gordon, Steven J. Roth, Scott J. Lieberman, Ann Zeller & Anne McConnell, *Customer Relationship management: A Senior management Guide to technology for Creating a Customer-centric Business* <http://www.the-dma.org/library/publications/customerrelationship.shtml>)

[608] Privacy in Commercial World, 106th Cong. (2001) (statement of Paul H. Rubin, Professor of Law and Economics, Emory University School of Law), available at <http://www.house.gov/commerce/hearings/0301200143/Rubin66.htm.> (accessed on November 18th, 2008); Direct Marketing Ass'n, Inc., Consumer Privacy Comments Concerning the Direct Marketing Association Before the Federal Trade Commission (July 16, 1997); Fred H. Cate, Privacy in the Information Age 113 (1997)

is the focus of this section, namely, the argument for creating individual property rights in personal information and default contractual rules to enhance the US system of personal data protection. The subsequent parts consider the various grounds supporting this argument.

3. Natural rights and rhetorical justifications

Daniel Solove submits that a property claim for one's personal information may be made based on a natural rights theory implying some form of inherent connection between an individual and data pertaining to him.[609] Vera Bergelson points to the work of Margaret Jane Radin[610] who continued on Hegel's theory of "property for personhood" and argues that besides property facilitating market exchange, there is also property for personhood with regard to things "closely related to one's personhood if its loss causes pain that cannot be relieved by the object's replacement."[611] This sort of property is essential to the individual's "sense of continuity of self over time."[612]

Some commentators admit that there is a certain rhetorical value in property talk that would enhance privacy protection. 'Property talk' is called on to attribute a special value to a subject like privacy,[613] or educate general public about the value of privacy. For nstance, Rule and Hunter advocate for the introduction of property in personal data, inter alia, because it would transform the civic culture by making it immediately "plain to every citizen how much he or she shared an interest in the protection of personal information."[614] However, the vast majority of the commentators approach information privacy as property from an economics perspective and the perspective of the weaknesses of the current US information privacy law.

---

[609] Solove, "Privacy and Power: Computer Databases and Metaphors for Information Privacy.", p. 1446 (although he does not develop the natural law argument further)

[610] Bergelson, "It's Personal, but Is It Mine? Toward Property Rights in Personal Information.", p. 430

[611] Margaret Jane Radin, "Property and Personhood," *Stanford Law Review* 34, no. 5 (1982)., p. 959

[612] Ibid., p. 1004

[613] "Property talk is just how we talk about matters of great importance" (Cohen, "Examined Lives: Informational Privacy and the Subject as Object.", p. 1379); "Property talk would give privacy rhetoric added support within American culture. If you could get people (in America, at this point in history) to see certain resource as property, then you are 90 percent to your protective goal." (Lessig, "Privacy as Property.", 255)

[614] James Rule, Hunter, Lawrence, "Towards Property Rights in Personal Data," in *Visions of Privacy: Policy Choices for the Digital Age*, ed. Colin J. Bennett, Grant, Rebecca (Toronto: 1999)., p. 174. The rhetoric value of property talk is only one part of the propertisation argument Rule and Hunter develop. For the more detailed analysis of their ideas see Setion 5.

4. Economic argument for propertisation

Pro-propertisation argument from the economic perspective is of special interest for this study since it dominates the US propertisation debate. To remind a reader the content of the economic perspective on property, let us briefly name its basic points: first, depending on the vision one takes on the function of economic analysis, the economic perspective regards efficiency or maximization of utility the goal any regulatory measure or absence thereof should look to achieve; alternatively, the economic analysis focuses on prediction of behaviour. Both visions rest on the assumption that people are rational utility maximisers. Further, property in economic terms is considered to be an exclusive ability to consume a resource either physically or economically. Distribution of the so-called transaction costs, or individual and social benefits forgone in the course of or for the sake of a transaction, influences efficiency of distribution of resources.

Roughly, the US commentators engaging in the economic analysis of law see property as a tool facilitating market exchange which, provided transaction costs are minimal, will achieve optimal privacy by balancing the value of personal information to a company against the value of the information to the individual and the larger social value of data protection.[615] This perspective receives three interpretations by the US information privacy scholars. Each of them will be considered in more detail shortly. As a result, it will be shown that, despite the fact that the validity of the economics perspective is not limited to the United States, all three interpretations of the economic argument are difficult to divorce from the US context, namely, US-specific understanding of property, specific weaknesses of the US information privacy, and the specifics of the US legal system in general.

The three interpretations of the economic argument for propertisation are (1) argument for individual property rights in personal data as opposed to default disclosure rule, (2) property as opposed to torts, and, finally, (3) property as a means to create incentives to apply privacy enhancing technologies (PETs).

4.1 Individual property as opposed to disclosure

Some of US scholars argue in favour of the individual property in personal data based on the dichotomy between privacy rule (i.e. control) and a disclosure (absence of privacy) rule. Mostly, their argument stems from the assumption they make that personal information is the object of property, and assigning it to an individual,

---

[615] Solove brings as examples of such an approach John Hagel III & Marc Singer, *Net Worth: Sharing Markets When Consumers Make the Rules* 19-20 (1999) (advocating for an "infomediary" between consumers and vendors who would broker information to companies in exchange for money and goods to the consumer); Paul Farhi, *Me Inc: Getting the Goods on Consumers*, Wash. Post, Feb. 14 1999, at H1]

within their framework of analysis, is the only alternative to the absence of information privacy whatsoever. The argument by Richard S. Murphy illustrates this line of thought. Murphy approaches the problem from the perspective of maximal social utility. He merely presumes that personal information, as any information, is property. The question Murphy focuses on is then "who owns the property rights to such information--the individual [...], the person who obtains the information, or some combination?"[616] Depending on to whom the property right is assigned initially: an individual or a data collector, Murphy distinguishes two kinds of default rules: non-disclosure (or privacy rule) and disclosure. The substance of the privacy (non-disclosure rule) is that "the individual can control dissemination of (or has a partial property right in) information deemed "private," but not in other information.[617] Under a disclosure rule, control over personal data is initially assigned to a data collector.[618] Within Murphy's analytical framework, to have an individual property right in personal information is the only alternative to no information privacy at all.

Murphy does not hold a preference to any one of those two rules since for the achievement of maximum utility, initial assignment of the resource - personal data - does not matter. A party, who values the resource most will always negotiate in his or her favour, provided the transaction costs are minimal.[619] However, since the latter is not the case in a real world, the law in the form of default contract rules or tort should intervene and allocate the initial entitlement. Murphy engages in an economic analysis of privacy and concludes that "there are, also, substantial economic benefits to personal privacy."[620] Since in the utility calculus, not only financial but also some psychic values like shame, or a mere taste for privacy count, non-disclosure may be more efficient than a default disclosure.[621] "Limiting disclosure of information may be whenever the individual concerned values his privacy highly, for any reason other than to deceive."[622] That implies that Murphy's defence of non-disclosure holds only for some sorts of personal information and in particular circumstances, when disclosure will negatively influence the quality and quantity of information since they are both vital for the efficient transactions. The examples of such special circumstances are the relationships between a doctor and a patient, a client and an attorney, a state and a rape victim, etc.[623] A newspaper should

---

[616] Murphy, "Property Rights in Personal Information: An Economic Defence of Privacy.", pp. 2383-84
[617] Ibid.
[618] Ibid., pp. 2388
[619] Here Murphy relies on the Coase Theorem as explained in Ronald H. Coase, "The Problem of Social Cost," *J.Law & Econ.* 3 (1960)., in Murphy, "Property Rights in Personal Information: An Economic Defence of Privacy.", p. 2381, fn 85
[620] Murphy, "Property Rights in Personal Information: An Economic Defence of Privacy.", p. 2416
[621] Ibid., p. 2416
[622] Ibid., p. 2387
[623] Ibid., pp. 2409-10

be found liable for the violation of a property right of a rape victim when it reports her true name. The rationale is that the state has an interest in prosecuting rapists. If the state does not maintain confidentiality of the victims, they will not report crimes,[624] similar to the patients who will not disclose to physicians information vital for their treatment, or defendants who will be discouraged to fully cooperate with their attorneys.

Jerry Kang approaches the issue from the transaction cost perspective: he argues that vesting property right in personal information with individuals (i.e. giving the control back) as opposed to the firms would be a more efficient solution. First, if the initial entitlement is given to a data collector, the data subjects would incur substantial costs to find out what information has been collected and used. The collector, to the contrary, would not face extra costs since it already possesses the knowledge on what information was collected and how it was treated. Second, unlike the collector, the individuals would face a collective action problem. The companies would not respect individual privacy preferences because it would be prohibitively expensive to tailor new information practices for every data subject. Therefore, individuals would have to unite their effort. In the process "they would suffer the collective action costs of locating each other, coming to some mutual agreement and strategy, proposing an offer to the information collector and negotiating with it – all the while discouraging free riders."[625]

This is a basic economic argument in favour of privacy guided by the considerations of efficiency, and would as such be valid in the settings other than the US. What makes it hard to divorce from the American context is the understanding of property it rests upon. Neither of the two authors gives definition of property in favour of which he argues. Murphy only says that one way of securing control over personal information is when "[i]ndividual can control dissemination of (or, put another way, has a partial property right in) certain information."[626] This definition of the scope of property rights as applied to personal data corresponds to the popular definition of the data protection problem as the one of the lack of control. But besides that, it seems to be rooted in the notion of property as explained in the 1972 article by Guido Calabresi and A. Douglas Melamed[627] and now considered standard by the US commentators.[628] Calabresi and Melamed define property by contrasting it to the liability rules. "An entitlement is protected by a property rule to the extent that someone who wishes to remove the entitlement from its holder must buy it from him in a voluntary transaction in which the value of the entitlement is agreed upon by the

---

[624] Ibid., pp. 2410

[625] Kang, "Information Privacy in Cyberspace Transactions.", p. 1193

[626] Murphy, "Property Rights in Personal Information: An Economic Defence of Privacy."., p. 2384

[627] Calabresi, "Property Rules, Liability Rules, and Inalienability: One View of the Cathedral."

[628] See, for instance, Epstein, "A Clear View of the Cathedral: The Dominance of Property Rules.", p. 2091

seller,"[629] whereas "whenever someone may destroy the initial entitlement if he is willing to pay an objectively determined value for it, an entitlement is protected by a liability rule."[630] Some commentators read this definition of property as implying "an exclusivity axiom," i.e. that an owner has a legitimate claim to exclude the rest of the world from his property.[631] That is, property is ensuring that the entitlement (in the case at hand – information privacy) is protected, whereas the liability's function is seen as to make sure that transfer of the entitlement is possible even without a holder of the entitlement, against an objectively determined compensation. As Lessig puts it, "property protects choice; liability protects transfer."[632]

Understanding the US argument for propertisation from the angle of Calabresi and Melamed's definition of property makes it clear that within this analytical framework only property regime offers some degree of control and protection to personal data. Any alternative (liability) rule only secures transfer of personal data, albeit against some objectively defined compensation. The remaining versions of the economic argument for propertisation rest on the same understanding of property.

4.2. Property as opposed to torts

Another interpretation of the economic argument for propertisation is offered by e.g. Vera Bergelson.[633] This is a clear case of use of the term 'property' in a legal argument in the meaning attributed to it by economic theory. Bergelson argues in favour of propertisation on a number of grounds, among others, that property regime would cure the weaknesses of the current system of privacy torts. Bergelson argues that "the choice between the tort regime and the property regime for the protection of personal information means the choice between property rules and liability rules as defined [...] by Calabresi and Melamed."[634] Indeed, when a system of privacy torts is in place, they allow collection of personal information just like a liability rule allows transition of a resource. Tort remedy is available only post factum and has no preventive function. The value of transmitted personal data is determined not by the holder of the entitlement, i.e. an individual, but by the court. Bergelson brings a utilitarian argument similar to Murphy and Kang's that propertisation "affords the individual maximum control over personal information and allows all interested parties to enter into mutually acceptable transactions without tying up the valuable societal resources."[635] Her distinct contribution to the

---

[629] Calabresi, "Property Rules, Liability Rules, and Inalienability: One View of the Cathedral.", p. 1092
[630] Ibid.
[631] Paul M. Schwartz, "Property, Privacy, and Personal Data," *Harv. L. Rev.* 117, no. 7 (2004)., p. 2055,
[632] Lessig, *Code and Other Laws of Cyberspace*.
[633] *Bergelson,* "It's Personal, but Is It Mine? Toward Property Rights in Personal Information.", p. 379,
[634] Ibid., p. 417
[635] Ibid., p. 419

economic debate, however, is in two points. First, the preference for torts (i.e. the liability rule) as opposed to property implies that "individual entitlements to personal information [...] would have to be enforced by litigation, on a case-by-case basis, which would involve considerable expenditures of funds and time."[636] Second, since the compensation under the liability rule is defined by the state, "the plaintiff will have to prove actual damages, which most likely will be trivial. That by itself will discourage people from bringing lawsuits against those who violate their rights in personal information, thereby making the rule inefficient."[637]

4.3. Property as an instrument to create a general system of personal data protection

There is another group of US authors defending propertisation from an economic standpoint, though of a different nature. Their focus is not efficiency, but prediction and channelling of behaviour of the data processing actors as rational utility maximizers and, as a result, the creation of an overall system of data protection. The latter is meant to comprise law, technology and market tools, the interaction of which can ensure proper level of information privacy. Namely, Julie Cohen speaks of law as only a mechanism to create incentives to build a general privacy infrastructure: "Law can and should establish a new set of institutional parameters that supply incentives for the design of privacy-enhancing technologies to flourish. Legal protection alone cannot create or guarantee information privacy."[638]

Lessig is probably the most outspoken commentator within this group. He also brings an economic argument that property rules would permit each individual to decide what information to disclose and protect "both those who value their privacy more [...] and those who value it less."[639] Lessig uses economic analysis as a building block of his own theory of privacy protection in the information age, as explained in the book *Code and Other Laws of Cyberspace*[640] and its revised version *Code 2.0*. First, he argues quite traditionally, information privacy is in essence control over personal information. Second, unlike in the real world, the architecture (or "code") of a cyberspace makes collection of information and control over that information, difficult for lay people. Third, such an architecture is a result of human activity and, therefore, can be altered.[641] Fourth, the US information processing practices are based on self-regulation, i.e., there is no general legislation requiring businesses to alter this architecture and use privacy-friendly technologies. Nor is

---

[636] Ibid., p. 417

[637] Ibid., pp. 417-18

[638] Cohen, "Examined Lives: Informational Privacy and the Subject as Object.", pp. 1437-38

[639] Lessig, *Code and Other Laws of Cyberspace*.

[640] Ibid.

[641] The same point is also made by Cohen in Cohen, "Examined Lives: Informational Privacy and the Subject as Object.", p. 1437

there motivation to account for interests of the individuals. In the absence of property interests, the companies make use of personal data for free. However, if individuals had property rights in personal data, it would force businesses to negotiate with the individuals, account for their interests, and alter the architecture, i.e. invest into development of PETs. The individual privacy would be better secured, not only by law but by interaction of the latter, market mechanisms and technologies.[642]

Cohen shares Lessig's views that interaction of law, market, and technology can create conditions for individuals to exercise meaningful control over personal information.[643] She believes that information privacy protection may learn from copyright where technology already offers means to secure property rights that were difficult to protect in the past.[644] Cohen refers to Phil Agre who described 'technologies of identity' which made it possible to prevent collection of personal data.[645]

> *The same technologies that enable distributed rights-management, she continues, functionally might enable the creation of privacy protection that travels with data – obviating the need for continual negotiation of terms, but at the same time redistributing "costs" away from individuals who are data subjects.*[646]

One cannot deny the potential benefits technology offers to information privacy protection. However, Lessig's argument must be treated with care. Apart from general criticism of the propertisation argument explained further in the Chapter, the weakness of his theory is that one of Lessig's basic assumptions (the reliance of the current data protection system on self-regulation and absence of general regulation of personal data processing) is characteristic of the American regulatory tradition.[647]

---

[642] Lessig, *Code and Other Laws of Cyberspace*.
[643] Cohen, "Examined Lives: Informational Privacy and the Subject as Object.", 1391
[644] Ibid, p. 1391
[645] P. E. Agre, Rotenberg, Marc eds., *Technology and Privacy : The New Landscape* (Cambridge: MIT Press, 1997).
[646] Cohen, "Examined Lives: Informational Privacy and the Subject as Object.", p. 1391
[647] Albeit other jurisdictions not covered by this study may also rely primarily on self-regulation as a main data protection strategy. Some US scholars, in particular, Mark Rotenberg, disagree with the idea that the US data protection rests on self-regulation and criticize Lessig's theory on that basis (Rotenberg, "Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get).")

5. The Propertisation argument pertaining to the specificities of the US legal system

Along with various interpretations of the economic argument for propertisation, some commentators favour the introduction of property rights in personal data as it could overcome the limitations inherent in the US legal (and political) system.

Murphy argues that recognition of information privacy as a property right will revive the current system of the US privacy torts. For instance, according to Murphy, one of the reasons why the tort system fails to protect personal data is that when a court comes to balance First Amendment interests of the press against some vaguely defined privacy interest, free speech naturally outweighs. That would not happen to privacy defined as constitutionally protected property:[648]

> *The disclosure tort is not a complete dead letter… But overall, it has fared poorly. One reason it has failed is that it is not conceived as a dispute about property rights in information, but rather as a battle between First Amendment values and an inchoate, elastic privacy "right." It is easy to see why the First Amendment generally wins this battle.*[649]

Rule and Hunter make a similar argument. They advocate for the system of property rights in commercial exploitation of personal information consisting of the individual's default right of control over transfers and commercial use of the data pertaining to him and the use licences comparable to mineral rights, development rights, or air rights and defined by purpose and time.[650] Although the interest of privacy is commonly recognised as deserving protection, in the US this interest "[does not] necessarily prevail in situations where it is contested. There are […] too many contexts where, from almost anyone's viewpoint, interests in personal information other than those of the individual data subject deserve recognition," e.g. commercial interests of the information industry. In this context, propertisation would introduce a major change to the default rule of data processing. The individual would be guaranteed control over his data and be able to benefit from its commercial use by means of royalties. While when the article was written there were little limitations on the commercial collection and (secondary) use of personal information, under the right proposed, "no information could legally be sold or traded from any personal data file, for any commercial purpose, without express permission from the person concerned,"[651] obtained directly or via information intermediaries which in turn would take on functions of privacy advocates

---

[648] Murphy, "Property Rights in Personal Information: An Economic Defence of Privacy.", p. 2388
[649] Ibid., p. 2388
[650] Rule, "Towards Property Rights in Personal Data.", p. 169-70
[651] Ibid., p. 170

monitoring data processing and representing data subjects' interests. Propertisation would not only strengthen the position of the individual against large corporations, but also establish organisations' legal responsibility to determine that every data transfer is consistent with the authorisation given by the data subject.[652]

Propertisation of personal data will respond to the individual preferences for privacy as the individual will have a chance to decide for himself whether to disclose data and benefit from it or pay a higher price for, e.g. mortgage in a more sensitive way than the current tort system does. Current privacy torts operate with some objective standards of privacy whereas it is not an objective but a subjective standard of privacy that has to be protected. In privacy cases, Murphy argues, "strictly speaking, 'norms of civility' are irrelevant [for calculating utility – added by N.P.]" since "the depth and diversity of privacy preferences are highly variable across individuals" and "the objective approach will often get the balance of preferences wrong." It is the subjective privacy preference that needs to be weighed against the value of the availability of information. In particular, it is the individual's pure privacy preference that matters, as distinct from his reputational interest."[653]

Another factor playing in favour of propertisation is that the change in law would not have to go through the federal legislative system, which, either due to the constitutional limitations or influence of the lobby as Chapter 5 demonstrated earlier, showed itself unproductive when it comes to regulating privacy. Jessica Litman who otherwise is a critic of the idea of propertisation, admits that "the appeal of the property model derives from the fact that property rights can be recognized as a matter of state common law without invoking the federal regulatory machinery, which seems too helpless, pernicious, or corrupt (depending on your political persuasions) to offer a meaningful solution."[654]

6. Scope of property rights: default rules

Another key issue in the US propertisation discourse is the scope of property rights in personal data, limited or unlimited by regulation in the form of, e.g., default rules. When describing the range of views on this matter in the US discourse, this section will show that despite a label of property attached to possible sets of rights in personal data, what really matters is not the name, but the content of the rights. Indeed, the proponents of the market solutions insist on the widest scope of the rights possible, whereas privacy advocates supporting propertisation argue for certain default rules. The main discussion is focused on alienability, or a possibility to sell personal data, which is somebody's property, freely. Full alienability and

[652] Ibid., pp. 169-174
[653] Murphy, "Property Rights in Personal Information: An Economic Defence of Privacy.", p. 2393
[654] Litman, "Information Privacy / Information Property.", p. 1303

absolute inalienability are two opposites on a continuum, other options ranging from more intensive to ad hoc regulation.

As the information industry's representatives are against individual ownership of personal data, they reject any idea of regulating transactions, including default rules. According to the "market purists," as Solove names them,[655] the market already accounts for privacy concerns.[656] To the extent that consumers want their privacy protected, the market responds to this demand and accounts for it in its utility calculus. Indeed, the industries have been adopting privacy policies in response to the consumers' privacy concerns. If privacy is not sufficiently protected in other cases, it means that people value efficient and convenient transactions, custom-tuned service, etc. more.[657]

When it is agreed that property rights in personal information should be vested with the data subject, the information privacy proponents continue to develop default contractual rules that would govern market transactions enabled by propertisation. However, as Solove points out, propertisation proponents are "certainly not in agreement over the types of property entitlements and contractual default rules that should be required."[658] The literature is divided already on the issue whether the rules should be of a contractual nature, i.e. whether the parties may negotiate for a different set of rules. Pamela Samuelson, who is not a proponent of propertisation, claims that "information privacy goals may not be achievable unless the default rule of the new property rights regime limits transferability."[659] Most market proponents, however, favour default rules that can be "bargained around."[660]

Kang recognizes that merely deciding on the initial entitlement in personal data is insufficient and he develops, compared to Murphy's privacy versus disclosure dichotomy, a more elaborated system of default rules. Since it is not efficient for individuals to have to research what information about them is collected and how it is used a contractual default rule should be adopted that "personal information may be processed in only functionally necessary ways" and that parties are "free to contract around the default rule."[661] The ban on transfer of personal data from the individuals, or inalienability rules in Kang's view would be too

---

[655] Solove, "Privacy and Power: Computer Databases and Metaphors for Information Privacy.", p. 1393

[656] In describing the purists' argument Solove refers to Privacy in Commercial World, 106th Cong. (2001) (statement of Paul H. Rubin), available at <http://energycommerce.house.gov/reparchives/107/hearings/03012001Hearing43/print.htm> (accessed on November 18th 2008); Direct Marketing Ass'n, Inc., Consumer Privacy Comments Concerning the Direct Marketing Association Before the Federal Trade Commission (July 16, 1997); Fred H. Cate, Privacy in the Information Age 113 (1997)

[657] Solove, "Privacy and Power: Computer Databases and Metaphors for Information Privacy.", p. 1448

[658] Ibid.,

[659] Samuelson, "Privacy as Intellectual Property?."

[660] Solove, "Privacy and Power: Computer Databases and Metaphors for Information Privacy."

[661] Kang, "Information Privacy in Cyberspace Transactions."

paternalistic. "Control is at the heart of information privacy," he claims, and control means that individuals should be able to sell or disclose their information if they wish so.[662] Inalienability will risk "surrendering control over information privacy to the state."[663] According to Solove, Kang's solution "creates a property right in personal information through a contractual default rule that limits the way personal information is used after being transferred to another."[664]

Paul Schwartz offers probably the most elaborated, and more far-reaching, set of the default rules, or better, a model of a property regime for data protection. He accounts for three elements of critique of propertisation in his hybrid inalienability model, those elements being the "public good" nature of information privacy; the market failures, i.e. pointing to the impact of propertisation under current conditions; and resentment to free alienability of personal data which implies that the owner may sell it whenever he pleases on whatever conditions.[665] First, he asserts that a public good argument - i.e. that the market cannot possibly account for a social value of privacy - does not reject propertisation entirely but calls for restrictions on it. As examples of privatized public goods he names outsourcing in some sectors of national defence, marketization of environmental laws, and democratic discourse via private media.[666] The market failures, he argues, may be corrected via regulation which constitutes a part of his model.[667] As for the fear of unrestricted alienability, Schwartz submits that free alienability is not implied by his model since "[according to Blackstone,] property can also take the form of incomplete interests [i.e. be inalienable – N.P.] and [...] can serve to structure social relationships."[668] This is a premise on which the copyright law[669] and the US intellectual property jurisprudence rely when rejecting the full alienability axiom.[670] The hybrid inalienability model that arguably responds to all three challenges thus implies: "limitations on the individual's right to alienate personal information; default rules that force disclosure of the terms of trade; a right of exit for participants in the market; the establishment of damages to deter market abuses; and institutions to police the personal information market and punish privacy violations."[671] The default rules are: an allowed initial transfer of personal data from the individual, but only if the individual has an opportunity to stop further transfers or uses by third

[662] Ibid.
[663] Ibid.
[664] Solove, "Privacy and Power: Computer Databases and Metaphors for Information Privacy."
[665] Schwartz, "Property, Privacy, and Personal Data.", p. 2076
[666] Ibid., p. 2090
[667] Ibid., p. 2089
[668] Ibid., p. 2092
[669] Ibid., p. 2093
[670] Ibid., p. 2093
[671] Ibid.

parties. The ability to block is to be set as an opt-in, that is, any further use or transfer is not allowed without an affirmative consent.[672]

The model proposed by Schwartz is probably the most privacy-friendly among the ones outlined here. However, one may ask what is left of the idea of propertisation when property rights are so heavily regulated, and why then not to opt for mere regulation. A point of special interest is Schwartz's rejection of the free alienability axiom. By rejecting it, Schwartz creates a model of property the main function of which is not fostering market exchange but protecting a privacy interest. Namely, a value of calling the set of rights vis-à-vis personal data in Schwartz's model is that using the label of property will overcome structural limitations of the US legal system, e.g. by changing the balance between privacy and the free speech considerations in tort and constitutional cases, as well as, property law being mostly judge-made, avoid the necessity to push new legislation through the US Congress.

To sum up, the lesson Europeans can learn from the US debate on default rules is that property is not an entirely straightforward concept. It has many faces and bears more than one function, among others, facilitating market exchange (a function of property used by utilitarian views and better achieved with minimal regulation) or a mere protective function (performed by invoking other than market qualities of property). Therefore, the answer to the question whether or not propertisation of personal information might be a good idea for Europe cannot be simply yes or no, but requires further deliberations on what approach to data protection – market or non-market - we are prepared to take, what 'face' of property suits best for it, and, most intriguingly, if the approach is non-market, whether we have to go through the trouble of introducing a new model of data protection via property, like some of the US scholars propose.

7. Established and added criticism of the US propertisation argument

This part will consider points of criticism towards the idea of propertisation of personal data as it emerged in the US and will focus both on established criticism developed by the commentators in the area of the US information privacy, and on its weak points as become apparent from the perspective of this study. Let us start with the evaluation of the idea offered by the US commentators.

Despite a seeming popularity of the idea, a number of US commentators are strongly opposed to translating information privacy into property rights. As a reader may recall, Paul Schwartz distinguishes three elements of the established critique of propertisation of personal data: the "public good" nature of information privacy;

[672] Ibid., p. 2060

market failures, i.e. pointing to the impact of propertisation under current conditions; and resentment of free alienability of personal data.[673]

A number of the commentators generally see commodification (and propertisation as a legitimized commodification) of certain goods including personal data as a problem. This is a "public good" argument which generally implies that information privacy has value not only for an individual but also for a wider society. The market is unable to account for the latter. For instance, Katrin Schatz Byford submits that regarding "privacy as an item of trade … values privacy only to the extent it is considered to be of personal worth by the individual who claims it."[674] Pamela Samuelson argues that propertisation of information privacy as a civil liberty might be considered "morally obnoxious."[675] "If information privacy is a civil liberty, it may make no more sense to propertize personal data than to commodify voting rights."[676] Schwartz develops the comparison: "the interest in privacy is like the interest in receiving access to the electoral franchise, clean air, or national defense: it should not depend on socioeconomic status."[677]

Peter Swire challenges market solutions on the ground of the failures of the currently existing information market. Even if propertisation will enable individuals to negotiate their privacy, it will still be difficult to negotiate with large corporations because consumers normally have no expertise in privacy issues and bargaining costs substantial time and effort.[678] One may agree that the introduction of privacy enhancing technologies will save time and effort. However whether it will substitute the needed expertise remains a question. Other failures of the current information markets are asymmetric information available to data collectors and individuals, and "bounded rationality" of consumers which favours the strongest party to the transaction, i.e. a data collector.[679]

The argument against propertisation which aims at the core of the economic argument is made by Jessica Litman who disputes the use of the understanding of property regime introduced by Calabresi and Melamed, i.e. as protecting the entitlement and preventing the transfer of information other than within a voluntary transaction. Her argument may be characterized as the one rejecting free alienability. She refers to the definition of the legal concept of property as given in the

---

[673] Schwartz, "Property, Privacy, and Personal Data.", p. 2076

[674] Katrin Schatz Byford, "Privacy in Cyberspace: Constructing a Model of Privacy for the Electronic Communications Environment," *Rutgers Computer & Tech. L.J.* 1, no. 24 (1998).

[675] Samuelson, "Privacy as Intellectual Property?.", p. 1143

[676] Ibid.

[677] Schwartz, "Property, Privacy, and Personal Data.", p. 2086

[678] Swire, Peter P. "Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information." available online at
<http://papers.ssrn.com/sol3/papers.cfm?abstract_id=11472.>, p. 10

[679] Schwartz, "Property, Privacy, and Personal Data.", p. 2081

Restatement[680] saying that "the raison d'être of property is alienability; the purpose of property laws is [not to prevent but to encourage and – N.P.] … prescribe the conditions for transfer."[681] For Litman, something is made property in order to facilitate its sale. She draws an analogy with intellectual property which is also an intangible. Litman argues that the regulation takes the property model for intangible interests when it aims "to make it easy to sell them."[682] That being said, the control which propertisation is argued to be able to achieve, defined as a "right to exclude" others, is of the same kind as control conferred by already existing branches of law, namely, the law of torts. The law of battery protects the integrity of the body, defamation protects the reputation, even though the reputation is not property. In other words, it is unnecessary to treat an information privacy interest as one of property merely to protect it from invasion.[683]

Litman's criticism of the economic argument goes beyond the economic understanding of property. She also challenges Lessig's proposal to use property as an instrument to promote investments in privacy enhancing technologies enabling easy expression of privacy preferences and bargaining in cyberspace. She labels Lessig's argument "a fairy-tale picture" and "nonsense," since industries do not respect information privacy of the individuals "not because it is expensive to allow a customer to express her preference, but because it would be expensive to honour it."[684] Litman concludes expressing her disbelief in market solutions of the information privacy problem by stating that "the market in personal data is the problem. Market solutions based on a property rights model won't cure it; they'll only legitimize it."[685]

Criticism of the propertisation solution offered by Daniel Solove seems to combine arguments of both a market and a non-market nature. To get a better insight in Solove's standpoint, one could benefit from recalling Solove's definition of the information privacy problem as described in Chapter 5 that goes beyond information

---

[680] "Property interests are, in general, alienable. If a particular property interest is not alienable, this result must be due to some policy against the alienability of such an interest. The policy of the law has been, in general, in favour of a high degree of alienability of property interests. This policy arises from a belief that the social interest is promoted by the greater utilization of the subject matter of property resulting from the freedom of alienation of interests in it." Restatement of Property, §489 cmt. a (1944)

[681] Litman, "Information Privacy / Information Property.", p. 1295

[682] Ibid., p. 1296; In fn 63 on p. 1296 Litman brings another example of the introduction of property rights to facilitate and encourage the transfer of an item from its original holders. In 1886 in the conditions of shortage of new resourceful lands available for settlements, the US Congress passed the General Allotement Act of 1887, ch. 119, 24 Stat. 388 which divided reservation land into parcels and allotted each parcel to an individual Indian. The parcels were held in trust for a term of years, after which each Indian succeeded to fee ownership of his parcel. "In 1934, Congress repudiated the allotment program, but not before it had accomplished its purpose" and Indian land was transferred from its original owners.

[683] Ibid., p. 1296

[684] Ibid., p. 1297

[685] Ibid., p. 1301

privacy as control. After paying his dues to the market purists,[686] Solove makes his original argument that even more privacy-friendly propertisation solutions fail to resolve the information privacy problem because they neglect the core of it, namely, "the power inequalities that pervade the world of information transfers between individuals and bureaucracies."[687] Solove explains his point by, first, referring to a traditional market argument against propertisation saying that it is difficult to assign the proper value to personal information. It is problematic for an individual to adequately value specific personal information because this value is tied up to yet unknown future uses.[688] However, the essence of the problem is not in the inability of an individual to put an adequate price tag on a piece of information pertaining to him, but rather in the "aggregation problem,"[689] i.e. an aggregated inability of the masses of individuals which makes them powerless in the information society: "The value of privacy is not located in particular information and defined by the individuals to whom that information pertains; rather the value of privacy lies in its systematic effects on power and powerlessness in society."[690]

Whereas the just mentioned critical positions with regard to the idea of propertisation in the United States context certainly have their point and this study would support most of them, one important point of criticism is missing or not sufficiently represented in the US debate, namely, that the notion of property is invoked in various, also other than legal debates. In the light of the findings of Chapter 4 of this book, it becomes apparent that the US propertisation debate, both pro- and anti propertisation sides of it, is disregarding this multiplicity of perspectives and blends legal and non-legal meanings of property in, essentially, a legal argument without acknowledging this mixing of perspectives. Most US authors seem ignorant of the distinction between legal and non-legal uses of property. For instance, normative theories are often invoked to justify the introduction of property rights in personal data. From the perspective of the individual, Margaret Jane Radin advocates propertisation on the grounds that personal data is essential for one's

---

[686] Solove comments on the argument made by the information industries that that the market is already providing the optimal level of privacy protection. In Solove's opinion, the argument fails "because there are vast inadequacies in knowledge and much data collection is clandestine.… What is not given to consumers is a frank and detailed description of what will and will not be done with their information, of what specific information security measures are being taken, of what specific rights of recourse consumers have. People must rely on the good graces of companies that possess their data to keep it secure and to prevent its abuse. … Most privacy policies have no way to prevent changes in policy or a binding enforcement mechanism." (Solove, "Privacy and Power: Computer Databases and Metaphors for Information Privacy.", pp. 1450-51)

[687] Ibid., p. 1452

[688] Ibid.

[689] Ibid.

[690] Ibid., p. 1453

personhood (personhood theory). Representatives of the information industry argue for vesting property rights with the industry because they invested in building databases (labour desert theory). Both perspectives are valid and deserve consideration in the propertisation debate but, as Chapter 4 makes clear, have little to say about the content of the property rights that need to be introduced.

The economic perspective on property is the one that is most often appearing in the propertisation debate. As this chapter demonstrated earlier, propertisation arguments made from the economic perspective are most discussed. But on top of that, using an economic perspective has detrimental consequences for the legal debate because, unlike the philosophical perspective, it not only offers justifications for propertisation, but also operates with a distinct understanding of property that is different from the one in law. One may reasonably argue that the economic perspective has its value for policymaking and is allowed to develop terminology of its own. This study inclines to agree except it is detrimental a the constructive legal debate to substitute the legal notion of property with its economic counterpart since those two perspectives only share the word 'property' while they mean a totally different scope of property rights. A large part of the US argument in favour of propertisation is flawed in such a way. For instance, Murphy, Kang, and Bergelson all merge economic and legal arguments without acknowledging their different natures when they first make an efficiency analysis of propertisation as a manner of distributing resource entitlements, and consequently argue in favour of property as compared to the existing torts, or in its capacity of a constitutional value which will counterbalance the constitutional right to freedom of speech. The author who shows himself most aware of the meaning of property in law is Paul Schwartz. He rejects the myth of absolute alienability and treats propertisation as a form of regulation to address market failures. However, he never explicitly draws a distinction between his hybrid alienability model of propertisation and the economic understanding of property rights. Jessica Litman is the one who unambiguously criticises the US propertisation debate, in particular, Lessig's theory of propertisation, for being in conflict with the meaning of property in law, i.e. the language of the Restatement. However, her criticism remains largely unnoticed. In other words, the US propertisation debate is clouded by various perspectives on property, the economic perspective the most prominently. The participants of the debate engage in the discussion without agreeing on terms, do not acknowledge the differences in legal and non-legal perspectives on the meaning of property and content of property rights, and proceed to substitute the content of legal rights with the assumptions coming from elsewhere. As a result, the US propertisation discussion, first, is far from arriving at a constructive conclusion and, second, apart from the constitutional argument to counterbalance the First Amendment freedom of speech, misses out on the legal implications of creating actual property rights as discussed in Chapter 4.

8. Conclusion

This chapter overviewed the US origins of the idea to introduce property rights in personal data. This part was not meant to argue for or against introduction of property rights in personal data in the United States. Instead, both sides of the argument were introduced. First, natural rights and rhetoric justifications were considered saying respectively that propertisation would acknowledge the vital role of personal data for one's personhood and that a status of property will make people realize the importance of data protection. Further, the economic argument in favour of propertisation was considered. Since the economic argument receives most attention in the propertisation discourse, three sections were devoted to each of its three interpretations. The first interpretation argued in favour of property rights as, in economic terms, a property regime is the opposite of and the only alternative to disclosure of information. The second interpretation advocates propertisation as an alternative to the current and arguably ineffective system of privacy torts that only provide post factum remedy and have no preventive function. It was shown to draw on the understanding of property by Calabresi and Melamed as giving control over data transfer back to the individual, as opposed to the 'liability rules' providing only objectively established compensation. The third interpretation has been offered by Lawrence Lessig who argues that fixing information privacy entitlements with individuals in the form of property rights will create a system of incentives for the information industry to abide by and invest in data protection. The overview of justifications of propertisation was finalized by the argument made as a reaction to the alleged failure of the existing US legal and political system to ensure information privacy otherwise. As lawmaking and fine-tuning of the tort system seem unlikely or not sufficient to some authors due to the efforts of the lobbying groups, unwillingness of the courts or shortcomings of the common law institute of tort, propertisation looks like an option, free of those limitations: it may be executed via common law courts and in addition is able to create a uniform approach to information privacy instead of the present patchwork of laws.

Another point of discussion in the US propertisation debate is the scope of property rights, i.e. whether they should be limited by some default rules, in particular, to limit rights of alienation. Spokesmen of the information industry represented in the debate advocate against such rules, as the desired information privacy goals, it is claimed, will be achieved by market forces. Privacy advocates argue in favour of the default rules. The model of Paul Schwartz especially stands out as the one disentangling the idea of property rights from the market ideology. Namely, he rejects the idea that propertisation necessarily entails absolute alienability and argues that, after property rights secure an individual's control over personal data, regulation should intervene and address the relevant market failures associated with free alienability. The model of Schwartz is contested by Jessica

Litman who argues that the point of creating property in the legal sense is to foster alienation, not limit it.

The chapter concluded with a brief overview of the major points of criticism towards propertisation proposals. First, established critical positions were outlined. Among those is the argument that propertisation of personal data implying alienation is the problem and not the solution. According to the public good argument, propertisation is unable to account for the social value of privacy. A number of commentators oppose propertisation on the ground of the failure of the existing personal data market. Besides, they emphasize a number of other market failures, such as a weaker position of an individual in negotiating his/her privacy, opacity of the current information practices, etc., and also in view of the 'aggregation problem.'

This study added its own criticism to the US propertisation discussion in general. Namely, it broadened the criticism offered by Litman who says that the way the propertisation advocates perceive property is in conflict with its legal meaning. The chapter went further and showed that the participants of the US debate in general fail to account for the multiplicity of perspectives on property. It has been shown that a non-legal meaning of property, especially, adopted from economic discourse, is transferred into the legal debate. That introduces chaos into the propertisation discourse as it unfolds in the US and makes achievement of a constructive outcome difficult.

Despite the described criticisms one cannot deny that in the context of the US legal and political system which slows down legal reaction to new developments in information practices, propertisation, at least in theory, would have a progressive role of bringing the US legislation to the level of the second generation of data protection and, in Schwartz's model, even further. Indeed, as Chapter 5 shows, the US information privacy law applicable to the private sector struggles to secure even negative privacy rights and thereby achieve the level of the second generation otherwise, not to mention a more progressive approach required by more recent challenges.

Although due to specificities of the US legal and political system Europeans cannot fully embrace the results of the American debate on propertisation of personal data, there are quite some lessons to learn from it. The first, and by far, the most important lesson which follows already from Chapter 4 and is reaffirmed here is that the concept of property is used in a number of discourses and is attributed different meanings. The US debate - apart from Schwarts and Litman - mostly overlooks or does not aknowledge this fact, but a European discussion should take into account that introduction of property rights may serve both a market and a non-market, or protective function. In the US the latter has received expression in the proposals to introduce property rights in data but limit alienability (the scope of property rights in general) in order to avoid the limitations of the current legal and

political system. From that the European reader should learn to be open to consider property out of the 'market box', too.

Second, whether property may be invoked in its market or non-market capacity depends on the function policy-makers choose for it to perform. Market-oriented propertisation, for instance, will be a good tool to implement Lessig's theory and create a system where property creates incentives for better data protection and, arguably, gives individuals control over their data back. Non-market-oriented propertisation, characterized by limited scope of property rights, especially, to alienate, is suitable for implementing the idea of rhetoric value of propertisation. It is also possible to assume that in Europe introduction of property rights in an object does not have to mean that a free market in that object is legitimized. On the contrary, free alienability excluded, property may as well be valued for its protective function.

Third, before the choice for or against propertisation of personal data is made, Europe has to decide on a number of other fundamental issues. An important one is what its standpoint is vis-à-vis commodification of personal information, whether, in principle, it opposes market exchange of personal data or is ready to go along with it, albeit, in a (more or less) restricted form. The answer to this question, in turn, largely depends on the chosen regulatory strategy and priorities and the vision of the role of the state or supranational institutions (paternalistic versus liberal).

The fourth lesson for Europe is that to shape their view on commodification and propertisation of personal data, Europe has to come to a uniform understanding of the essence of the problem it attempts to tackle (if any). In the American literature propertisation is called upon to resolve the problem of the lost control over personal information. But does Europe want its citizens to have full control over information pertaining to them? Another function propertisation, albeit in theory, serves in the US debate is a 'back-door' introduction of data processing regulation, since a straightforward way at times is problematic. It is unlikely that Europe experiences difficulties introducing new regulations. However, possibly there is something more to that protective function of property that Europe can also use. The first thing which comes to one's mind is that a status of property rights may give data protection rights an extra set of enforcement mechanisms, but that is a subject of further research.

Finally, coming back to the first lesson, Europeans should decide on what scope of rights they prefer with regard to personal data, and then see if this is useful for them to label those 'property' or not.

Part III: The European perspective

Chapter 7: Review of the European Data Protection Regime

1. Introduction

The idea of introducing property rights in personal data emerged in the United States largely due to the limitations of the US legal and political systems, which did not enable the law to adequately respond to the challenges of new information practices.[691] This chapter will focus on the European data protection system. The analysis will aim to investigate whether current data protection law in Europe has any weaknesses in terms of both substantive principles and processes – which prevent it from dealing with the data processing problem and require action. The logic behind this approach is that a change in law, such as the propertisation of personal data, only makes sense if the data protection system is flawed in its present state. Indeed, if the system in place is sound, and there is little room for improvement, changing the old and introducing a new approach to data protection would make little sense.

The analysis will begin with a brief overview of the system itself (Sections 2.1 and 2.2) and will conclude with a comparison of the established data protection regime and the actual substance of the personal data problem (Section 2.3). It will be demonstrated that although the substantive principles of the European data protection regime receive little criticism from data protection experts, and are often perceived as the ideal model, the process-orientated rules do not bear scrutiny in a number of respects. In particular, they fail to grasp the new structure of relationships within the flow of data, are unable to control modern processing of personal data and therefore undermine the effectiveness of the substantive principles.

2. The System of European data protection law

The system of data protection in Europe is a combination of numerous national, supranational and international instruments, which vary in their effect, wording and application. To make the picture slightly less complicated, this study will first give a short introduction to the sources of European data protection law, highlighting several instruments as key points for further analysis and setting out their main characteristics (Section 2.1). Subsequently, Section 2.2 will deal with the contents of these instruments, focusing not on the individual tools, but on the substantive principles and the process-related norms as they are cumulatively expressed in supra- and international data protection law. In no way will this study attempt to

[691] See Chapters 5 and 6

provide a full account of all aspects of European data protection; this has already been brilliantly done elsewhere.[692] The overview will instead be limited to what is necessary and sufficient to achieve the goal of the chapter, namely to reveal systematic failures, if any, of the data protection mechanisms currently in place, rather than focusing on their individual details.

2.1. Sources of European data protection law: their goals and scope of application

Data protection is a highly developed area of European law, numbering many data protection instruments which have been adopted at the national, supranational and international level. In terms of the latter, the Organisation for Economic Co-operation and Development adopted the Guidelines governing the protection of privacy and trans-border flows of personal data (the OECD Guidelines), while the United Nations Assembly in turn passed UN guidelines concerning computerized personal data files (the UN Guidelines).[693] The European, supranational legal context of privacy and data protection is comprised of the EC data protection regime and the relevant laws passed by the Council of Europe. The EU regime comprises three directives,[694] one

---

[692] For a comprehensive overview of European data protection see, e.g. Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits*.; Christopher Kuner, *European Data Protection Law: Corporate Compliance and Regulation*, 2nd ed. (New York: Oxford University Press, 2007).; Alfred Bullesbach, Poullet, Yves, Prins, Corien, ed. *Concise European IT Law* (Kluwer Law International 2006).

[693] UN Guidelines adopted by the General Assembly on 14 December 1990.

[694] - Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data;
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications (as amended by Directive 2009/136/EC of 29 November 2009) repealing and replacing Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector;
- EU Charter of Fundamental Rights of 7 December 2000.
- Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC;
- Regulation (EC) 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by Community institutions and bodies and on the free movement of such data;
In addition, ther is Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (published in Official Journal L 350 , 30/12/2008 P. 0060 – 0071). This instrument is only relevant for the Third Pillar (see Recital 6 defining the scope of application "to data gathered or processed by competent authorities for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.") and has marginal significance for the conclusions regarding an overall structure ofbthe European data protection. Besides, it has

regulation, Art. 16 of the Treaty on Functioning of the European Union,[695] and Articles 7 and 8 of the EU Charter. In addition, Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) is also of relevance, since the institutions of the European Union have previously declared their adherence to the protection of fundamental rights.[696] Moreover, since December 2009, when the Lisbon Treaty came into force, it opened a possibility for the EU as a whole to acced to the European Convention. In determining the scope of the protection of fundamental rights, the European Court of Justice (ECJ) has ruled that it is bound by the ECHR and the jurisprudence of the Strasbourg court.[697] This list of the sources of data protection law is far from complete, with each EU member state having its own data protection legislation implementing the international standards. Furthermore, the general data protection instruments of inter- and supranational institutions have also passed sector legislation concerning, e.g. the use of personal data for employment purposes and in the financial services sector.[698]

Consideration of all of the sources of data protection law in Europe is beyond the scope of this study. Accordingly, the overview will be limited to a number of supra- and international instruments, which are regarded as the main reference points, but will omit national laws almost entirely. The significance of national laws in this study is marginal. Indeed, although the national legislation pioneered in the field of data protection, and despite the fact that supra- and international instruments took their contents from the existing body of national law in an attempt at harmonisation,[699] the domestic legislation currently in force in the EU member states has either been adopted or amended in order to implement multinational standards. Therefore, the supra- and international rules are the most relevant to this study.[700]

---

been stated earlier in this book that data protection issues in the Third Pillar lie beyond the scope of the present analysis.

[695] Consolidated Version of the Treaty on Functioning of the European Union

[696] E.g. paragraphs 1 and 2 of Article 6 (ex Article F) of the consolidated text of the Treaty on the European Union.

[697] Initially in the *Nold* case (ECJ 14 May 1974, *J. Nold Kohlen- und Baustoffgroßhandlung v. Commission*, case 4/73 [1974] ECR 491, paragraphs 13 and 14).

[698] E.g. the Committee of Ministers of the Council of Europe have adopted Recommendation No. R (90) 19 of the Committee of Ministers to Member States on the protection of personal data used for payment and other related operations (adopted by the Committee of Ministers on 13 September 1990 at the 443rd meeting of the Ministers' Deputies) and Recommendation No. R (89) 2 of the Committee of Ministers to Member States on the protection of personal data used for employment purposes (adopted by the Committee of Ministers on 18 January 1989 at the 423rd meeting of the Ministers' Deputies)

[699] For more on the emergence of international data protection law see, e.g. Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits*.

[700] Directive 95/46/EC on the protection of personal data had to be transposed into national laws by the end of 1998. See, however, the speech of Justice, Fundamental Rights and Citizenship Commissioner Viviane Reding, who said that "one of the main concerns expressed by businesses in

The overview in this chapter will only focus on a limited number of sources of European data protection law, namely the key elements in the data protection field which have been selected on the basis of their influence on the operation of the current European data protection system. These are:

The 1980 OECD Guidelines governing the protection of privacy and the trans-border flows of personal data, adopted in Paris by the OECD Council on 23 September 1980 (the OECD Guidelines);[701]

The Council of Europe Convention No. 108 for the protection of individuals with regard to the automatic processing of personal data, adopted by the Council of Europe Committee of Ministers on 28 January 1981 (Convention 108); and

The EC Directive on the protection of individuals with regard to the processing of personal data and the free movement of such data (Directive 95/46/EC (OJ L281, 23.11.1995, 31), adopted by the European Parliament and the Council on 24 January 1995 (the 1995 Data Protection Directive).

Although the OECD Guidelines are not binding on state parties, they do create a framework of principles which foster the adoption by OECD member states of consistent domestic data protection policies.[702] Convention 108 played a significant role in forming and harmonizing the European approach to data protection. This is firstly because it created an obligation upon which state parties[703] must comply to secure in their territory a certain level of respect for data protection rights: "respect for [an individual's] rights and fundamental freedoms, and in particular his right to privacy, with regard to [the] automatic processing of personal data" (Article 1). Secondly, Convention 108 was adopted in an acknowledgement that, at the international level, the traditional mechanisms of privacy protection in the form of negative rights are inadequate when it comes to addressing the challenges of new information practices.[704] As a result, although of no direct effect on the rights and

---

the recent consultations is the lack of harmonisation and the divergences of national measures and practices implementing our 1995 Directive." (Viviane Reding, "Towards a True Single Market of Data Protection Given at the Meeting of the Article 29 Working Party "Review of the Data Protection Legal Framework" Brussels, 14 July 2010," *Speeches of the Vice-President of the European Commission responsible for Justice, Fundamental Rights and Citizenship available on-line at http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/386&format=HTML&aged=0&language=EN&guiLanguage=en* 14 July, no. SPEECH/10/386 (2010).)

[701] Although the OECD Guidelines are not a part of a supranational EU legal order, they are still considered by this study an integral part of the data proection law operating in Europe. It has to be noted here, however, that the states signatories of the Guidelines are not limited to the European continent and include such countries as the US, Russia, etc.

[702] Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits*.

[703] Article 3(1) of the 108 Convention.

[704] In 1968, the Committee of Ministers, pursuant to Recommendation 509 of the Parliamentary Assembly of the Council of Europe, conducted a survey asking "whether the European Human Rights Convention and the domestic law of the member States offered adequate protection to the right of personal privacy vis-à-vis modern science and technology" (explanatory report to the 108 Convention, para. 4). The results of the study revealed that existing domestic and Council of Europe mechanisms

obligations of private parties, the Convention contains a state obligation to create positive rights of the data subjects, thereby providing control over and transparency in data processing (Article 8).

At the EU level, the provisions of the Charter of Fundamental Rights of the European Union of 7 December 2000 (the EU Charter) will be mentioned only briefly. It establishes a separate right to data protection and elaborates on its contents in Article 8. However, the document only came into force in December 2009 as by virtue of the Treaty of Lisbon it has been given the same legal value as the EU Treaties. Hence, the Charter has little record of application. In explaining the meaning of the right to personal data protection in Article 8, the Charter repeats previously adopted international principles and, being a document of a constitutional nature, provides few guidelines about the application and enforcement of its substantive rules. Regulation (EC) 45/2001 is only binding on EC institutions, and the directives on privacy and electronic communications, the retention of data, and privacy in telecommunications are pieces of sectoral legislation and conform to the general principles of Directive 95/46/EC. Accordingly, the latter is the key EC instrument on personal data protection,[705] and will thus be regarded as the best representative of the EU approach to data protection.

The role of Article 8 of the ECHR and the jurisprudence of the Strasbourg court should not be underestimated in any analysis of the European data protection regime. However, the language of the former does not refer to data protection, and it is the case-law that has expanded the meaning of Article 8 protected privacy to include data protection interests. This expansion follows the development of data protection standards which are already enshrined elsewhere, and therefore had little influence on the actual formation of the substance of the data protection regime. Indeed, the perspective of the literature considering the place of ECHR law in the data protection regime often highlights the principles of data protection which were developed earlier in other instruments and have gradually been incorporated into the jurisprudence of the court on Article 8.[706] For these reasons, the ECHR will be omitted from the analysis in this Chapter, but it will be referred to later on in the general line of argument, particularly in Chapters 8 and 9, which defend the human right to data protection as a limitation on the idea of the propertisation of personal data.

---

were insufficient; see also De Hert and Gutwirth, who state that Article 8 ECHR protection did not contain the transparency tools that are vital for data protection (de Hert, "Making Sense of Privacy and Data Protection: A Prospective Overview in the Light of the Future of Identity, Location-Based Services and Virtual Residence in the Institute for Prospective Technological Studies: Report Eur 20823 En.")

[705] With important reservations as to the scope of the application of the Directive under Article 3.

[706] E.g. Paul de Hert, Gutwirth, Serge, "Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalization in Action," in *Reinventing Data Protection?*, ed. Serge Gutwirth, et al. (Berlin: Springer, 2009).

The circumstances and policy concerns underlying the adoption of the instruments referred to earlier vary. However, it is safe to say that all of the data protection instruments regarded as the key elements of this analysis share two common goals: firstly, they are aimed at the harmonisation of national laws both in order to establish a common minimum level of protection and achieve the free trans-border flow of personal data; and secondly, they attempt to balance the personal data related interests of individuals against societal and business interests in the free movement and availability of data.[707] To achieve these goals, states have some degree of discretion. The margin of maneuvre under the OECD Guidelines and Convention 108 is extensive. The Guidelines are not meant to be binding, and only establish general principles of fair information practices, while the 108 Convention is an international treaty that is not meant to be self-executing and, as such, allows the signatory states a leeway in how to implement its provisions. Therefore does not ensure the complete homogeneity of national approaches. As predicted in Recital 9, although there are significant disparities in how the member states implement its rules,[708] the 1995 Directive continues to be the most comprehensive of all of the data protection instruments at hand, leaving in principle only a limited margin of maneuvre.[709]

2.2. Content of European data protection law

Like other branches of law, data protection law may be viewed as a combination of a) substantive principles and b) implementation and process-orientated rules, creating a system of compliance, monitoring, accountability and enforcement. For instance, Lee Bygrave talks about two clusters of data protection norms: the core principles of data protection laws, which directly govern the processing of personal data, and the rules establishing monitoring, supervisory and enforcement regimes.[710] This study will adopt the same classification, and will briefly introduce the cluster of substantive data protection rules (Section 2.2.1) along with the rules establishing the ways in which the former are implemented, i.e. the second cluster (Section 2.2.2). The classification may appear to be artificially imposed, since some of the rules, e.g. the

---

[707] The characteristic pointed out in, e.g. Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits*., p. 33

[708] See, e.g. Reding, "Towards a True Single Market of Data Protection Given at the Meeting of the Article 29 Working Party "Review of the Data Protection Legal Framework" Brussels, 14 July 2010."

[709] 'In principle' here refers to the fact that although theoretically member states have little margin of maneuvre implementing the Directive's rules, in practice national implementation suffers from a large number of disrepancies. For more on the status and effect of the directives in community law see Sacha Prechal, *Directives in EC Law* Oxford European Union Law Library (Oxford University Press, 2005).

[710] Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits*., p. 57 et seq. and p. 70 et seq.

consent requirement described below, under the heading of individual control, may be classified under both the substantive and process-orientated headings. In fact, as Bygrave points out, the rules of both the first and second clusters "are largely procedural in focus."[711] Nevertheless, this study will rely on this categorization because a focus on groups of rules, rather than on each rule of each data protection instrument individually, is one of the more pragmatic and concise ways to outline a body of law that is as developed as the European data protection regime.

2.2.1. First cluster of rules: substantive principles

The substantive data protection principles are the qualitative requirements for the processing of personal data. They reflect the normative choices of a legislator in terms of the values that should be respected and the substantive standards that should be maintained when dealing with personal data. In contrast to the more process-orientated rules in the second cluster, substantive principles are the goals to be achieved with regard to data protection, whereas the second cluster of rules determine the means of doing so. These principles are not always expressed in specific provisions of the many data protection laws. Instead, they are manifest in groups of legal rules in data protection instruments, varying in wording but striving to secure a common value or principle. These substantive principles are: fairness and lawful processing, minimality, purpose specification, information quality, data subject participation and control, disclosure limitation and information security. In addition, Bygrave also distinguishes the principles relating to sensitivity and data transfers to other countries, although this chapter will deal with these issues under the heading of the fair and lawful processing of data.

a. Fair and lawful processing

The principle of fair and lawful processing may be regarded as the most general principle of data protection law, since it manifests itself in all of the other principles.[712] The language that data protection instruments employ to express the principle may resemble Article 5 of Convention 108 and Article 6(1) (a) of the 1995 Directive, which prescribe that personal data "shall be processed fairly and lawfully." Principle 7 of the OECD Guidelines contains the same requirements in respect of data collection. Although the requirements of fairness and lawfulness are

---

[711] Ibid. p. 84 quoting Herbert Burkert, "The Law of Information Technology," *DuD* (1988)., p. 384-385, and further: "The predominance of procedural concerns appears symptomatic of legislators' uncertainty about the nature of the interests to be protected, together with a desire for regulatory flexibility in the face of technological complexity and change" (Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits*.).

[712] Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits*. P. 58 (The principle is "manifest in all of these principles even if […] they are expressly linked only to the means of collection of personal data […], or not specifically mentioned at all)."

interrelated, they have been interpreted in such a way that they have distinct meanings. Data processing is lawful when it is in compliance with the requirements imposed on it by law. For instance, Article 7 of the 1995 Directive envisages general conditions for the legitimate processing of personal data including, *inter alia*, the consent of the data subject, the fulfilment of contractual obligations, or compliance with a legal obligation.[713] Specific and stricter requirements apply to the processing of sensitive (or special categories of) personal data, e.g. in Article 8 of the Directive and Article 6 of the 108 Convention regarding "data on a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health and sexual life." Stricter standards have also been established with regard to trans-border data transfers in order to ensure at least a basic level of data protection in such circumstances.[714]

Apart from having a meaning that is complementary to the principle of lawfulness, and since legal standards are expected to achieve fairness, the criterion of the latter has also been interpreted as implying principles of transparency and proportionality. Recital 38 of the 1995 Directive explains that data processing is only fair when the data subject is "in a position to learn" about the data processing operation and is given full and accurate information about the facts and circumstances of the collection of his personal data. The principle of fair processing implies the prerequisite of proportionality in that, while processing data, the controller is expected to balance his interests and those of the data subject in order to avoid invading them unnecessarily, unreasonably, or excessively.[715] One of the key manifestations of the fairness principle is Article 15(1) of the 1995 Directive, which acts against the unjust usage of automated data processing. The provision, with some exceptions (Article 15(2)), requires that no person should be subjected to a decision of

---

[713] Under Article 7 of the Directive, data processing is lawful when one of the following requirements are met: "Member States shall provide that personal data may be processed only if:
(a) the data subject has unambiguously given his consent; or
(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or
(c) processing is necessary for compliance with a legal obligation to which the controller is subject; or
(d) processing is necessary in order to protect the vital interests of the data subject; or
(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or
(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1)."

[714] E.g. Article 25(1) of the 1995 Directive requires that a third country to which data is transferred must ensure an "adequate level of protection."

[715] See, e.g. Lee A. Bygrave, Schartum, Dag Wiese "Consent, Proportionality and Collective Power," in *Reinventing Data Protection?*, ed. Serge Gutwirth, de Hert, Paul, Poullet, Yves (Brussels: Springer, 2009)., p. 163

significant legal effect if it is "based solely on automated processing of personal data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc."

b. Minimality

The principle of data minimality (or data minimalization) is manifest, among others, in Article 6(1) (c) of the 1995 Directive, which states that personal data must be "relevant and *not excessive* in relation to the purposes for which they are collected and/or further processed" (italics – N.P.) or stored (Article 5(c) of the 108 Convention). Accordingly, the minimality principle has been seen as a continuation of the purpose-limitation requirement.[716] Likewise, in some national laws, e.g. §3a of the German Federal Data Protection Act, the principle has been articulated in separate legal provisions and may now be used as a separate source of legal rights and obligations.[717] The principle can also be formulated as one of proportionality, necessity, non-excessiveness or frugality as regards to the quantity of data processing.[718] Under this principle, one may argue that the information industry has an obligation to both minimize the flow of personal data to the extent that is strictly necessary and to ensure that it does not process data "in a 'leaky' or 'wasteful' way."[719]

c. Purpose limitation

The principle of purpose limitation derives from Article 5(b) of the 108 Convention, paragraph 9 of the OECD Guidelines and Article 6(1) (b) of the 1995 Directive. The latter requires that "personal data shall be collected for specified, lawful and/or legitimate purposes and not subsequently processed in ways that are incompatible with those purposes."[720] The principle sets a limit within which personal data may be

---

[716] Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits*., p. 59

[717] Kuner, *European Data Protection Law: Corporate Compliance and Regulation*., p. 74

[718] Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits*., p. 60, quoting para. 4.7 of Recommendation R(97) on the protection of personal data collected and processed for statistical purposes (30 September 1997)

[719] Kuner, *European Data Protection Law: Corporate Compliance and Regulation*., p. 74

[720] Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits*., p. 61. This distinction does not have a big significance for the present argument. It is doubtful that it has a noticeable impact on the compliance practice. Nevertheless, a brief clarification of use will be given. The 108 Convention referrs to the purposes of processing as 'lawful', whereas the 1995 Directive uses 'legitimate' to describe the purposes of processing (Art. 6(1)(b), Recital 28, 45 etc.), interests in the name of which or activities in the course of which data is to be processed (Art. 7 (f), Recitals 30, 33, 45 etc.) and 'lawful' with regard to the processing itself (e.g. Art. 5, Recital 9, 22). Kotschy interprets 'lawful processing' to mean the processing that has a legal ground, deriving from a legal competence of a controller (Alfred Bullesbach, Poullet, Yves, Prins, Corien, Serge, Gijrath, ed. *Concise European IT Law*, 2nd ed. (Wolters Kluwer,2010)., p. 51). Textual interpretation of the Directive suggests the following relationship between the two terms: a data processing operation is lawful when conducted on a ground of a legitimate purpose or individual or public interest. The terms are used accordingly by e.g. Art. 29

processed.[721] This limit manifests itself in approximately three requirements. First, the data subject should be specifically informed of the purposes of the data processing (the purposes should be defined); second, the data collected must not be further processed for purposes that are incompatible with those originally indicated; and finally, the purposes shall be lawful (or legitimate in the language of the 108 Convention).[722]

d. Information quality

The principle of information quality demands that personal data should be valid, relevant and complete with respect to the purposes of processing.[723] The principle manifests itself not in one but in a constellation of requirements that the data protection instruments impose on data quality: Article 5(d) of Convention 108 and Article 6 (1)(d) of the Directive read that data shall be "accurate and, where necessary, kept up to date."[724] Paragraph 8 of the OECD Guidelines also requires data completeness. The 1995 Directive likewise sets out that data obtained must be "adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed (Article 6 (1)(c))." Moreover, the EC Directive demands that "every reasonable step must be taken" to ensure the quality of data (Article 6(1) (d)).

e. Data subject participation and control[725]

The principle of data subject participation and control (often referred to as the principle of information self-determination) is one of the most distinctive features of the modern European approach to data protection. Unlike the administrative rules regulating databases, the introduction of individual data protection *rights* has been a milestone in the evolution of European data protection law. The principle has been formulated in the data protection literature, and requires that "persons should be able to participate in, and have a measure of control over, the processing of data on them by other individuals or organizations." This is expressed in: paragraph 13 of the OECD Guidelines; the requirement to obtain the consent of the data subject in Articles 7 and 8 of the 1995 Directive; the information obligations on data controllers; and the various other tools which enable an individual to obtain and have some

---

Working Party in its documents (e.g. Working Document Setting up a framework for the structure of Binding Corporate Rules, 24 June 2008, WP 154 referring to 'legitimate' interests, purposes, grounds of processing; or Working Document Establishing a Model Checklist Application for Approval of Binding Corporate Rules, 14 April 2005, WP 108, referring to a 'lawful authority' to process data.)

[721] Kuner, *European Data Protection Law: Corporate Compliance and Regulation*., p. 100

[722] Ibid.

[723] Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits*., p. 62

[724] Ibid.

[725] For a more detailed description of the principle of individual participation see Chapter 8, Section 3.1.3.

degree of influence over what is going on with his personal data. Although the need to acquire the consent of the data subject, which can often be avoided, is only one among a number of equally important conditions legitimizing personal data processing, individual participation and control in the form of information rights has to be respected throughout the data processing process.

f. Disclosure limitation

The principle of disclosure limitation, or the limitation of secondary transfers, implies that the disclosure of personal data to third parties should be restricted and only possible under certain conditions.[726] Paragraph 10 of the OECD Guidelines establishes a bottom line rule that personal data "shall not be disclosed [...] except: (a) with consent of the data subject; or (b) by the authority of law." The 1995 Directive and the 108 Convention transpose the principle in the general limitations and conditions of data processing in Articles 5 (a), 5(b) and 6 of the Convention, and Articles 6(1) (a), 6(1) (b), 7, and 8 of the Directive.[727]

g. Data security

The principle of data security expresses itself in the obligations of the data controller to ensure the adequate protection of personal data from any kind of unauthorized processing, including its destruction, alteration, disclosure and loss, both at the stage of designing data processing processes and during the processing itself (e.g. Recital 46 of the 1995 Directive). Article 7 of the 108 Convention imposes a similar obligation during the data storage stage.[728] The Directive establishes an objective standard of quality of security measures, and those implemented must be in proportion to the risks involved in the data processing and "the state of art and the cost of their implementation" (Article 17(1)). A controller also has an obligation to ensure – by way of a contract or other legal act (Article 17(3)) – that data processors who are acting in his interests provide "sufficient guarantees in respect of the technical security measures and organizational security measures governing the processing to be carried out" (Article 17(4)). Recital 46, which deals with the interpretation of Article 17, has been read as requiring that security measures cannot simply be added, but should already be incorporated when designing the processing system and the processing itself, a principle known as "privacy-by-design".[729]

---

[726] Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits*., p. 67
[727] Ibid., p. 67
[728] Article 7 of the 108 Convention reads: "Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination."
[729] Robinson, et al., "Review of the European Data Protection Directive: Technical Report Prepared for the Information Commissioner's Office.", p. 9

2.2.2. Second cluster of rules: the 1995 Directive's system of implementation of the substantive principles

The second cluster of rules is a constellation of the implementation tools that create a system of compliance, monitoring, accountability[730] and enforcement, and which bring the substantive data protection principles into force.

Of the three instruments chosen as the main orientation points of this chapter's analysis, the 1995 Directive is the most comprehensive when it comes to giving member states guidance into how the substantive data protection principles should be implemented in data processing practice. The role of the non-binding OECD Guidelines is limited to the requirement that states must provide for "adequate sanctions and remedies in case of failures to comply with measures" (para. 19). Similarly, the 108 Convention envisages that "each Party undertakes to establish appropriate sanctions and remedies" for violations of the data protection principles implemented by national legislation (Article 10). Article 1 of the Additional Protocol to the Convention of 23 May 2001 on supervisory authorities is similar to the respective provisions of the 1995 Directive. Consequently, the latter will be the primary point of departure for the account of the implementation of European data protection principles that follows.

The 1995 Directive is an instance of what some authors call 'the fourth generation' of the evolution of data protection legislation. The rationale behind the fourth generation instruments was to restore the power balance between individuals and data processing actors by way of state regulation, while simultaneously relying on the individual participatory rights adopted from the third generation approach.[731] Regardless of whether the reader shares the generational approach to the development of data protection regimes, or, like Bygrave, prefers to avoid talk of evolution, instead speaking of simple changes in regulatory trends, this double nature of the Directive is evident. It combines top-down and participatory methods of implementation. The subsequent sections will, thus, describe each of the Directive's implementation mechanism levels.

---

[730] As this Chapter was written in May 2010, the term 'accountability' used here has a meaning close but not identical to the accountability spelled out in the Article 29 Working Party Opinion 3/2010 on the principle of accountability of 13 July 2010 (WP 173). The Working Party suggests introduction of accountability into the Data protection directive as a general principle of data protection and understands it as a combination of two elements: the actual *implementation* of data protection measures/procedures, and the *ability to demonstrate* compliance with those measures/procedures (para. 15). The principle of accountability can be implemented both on the level of technology used for data processing ('privacy by design') and organisational level (organisational measures intended to ensure compliance with data protection, e.g. educating stuff, appointing a privacy officer, developing mechanisms to deal with individual data protection complaints etc.).

[731] For more on the evolutionary approach to the development of data protection see Chapter 1, Section 3.

a. Participatory implementation

Participatory implementation (with implementation being understood as broader than mere enforcement) refers to implementation at the grass-roots level, which involves the private parties to the data processing – the data subjects[732] - as well as the controllers themselves. The former are entitled to actively exercise their rights, including the rights to give and withdraw consent[733] and information rights, whereas the latter are expected to comply with their obligations and exercise self-regulation and self-control. Based on both the interaction between the data subjects' rights and the controllers' obligations and the system of co-regulation and self-control, the participatory aspect of the implementation mechanism of the Directive aims to put the substantive data protection norms into practice by creating a self-running system of accountable relationships between data subjects and data controllers.

i. Rights and obligations

A significant part of the Directive's system of implementation relies on the interplay of the rights of the data subjects and the obligations of the actors involved in data processing. Although the participatory model is not the Directive's primary manner of implementation,[734] the provisions establishing the data protection rights and obligations deserve close examination. Meant to prescribe what can and has to be done in the area of data protection by data subjects or controllers, the rules on rights and obligations are very straightforward tools aimed at shaping the behaviour of those involved.

As pointed out earlier in the analysis, due to the Directive's focus on the process side of data processing it is not always possible to draw a clear line between the substantive and implementation rules. In accordance with this observation, the principle of informational self-determination gives rise to the implementation-related rights of a data subject. The most important of these are the rights to give and withdraw consent under Articles 7 and 8 and the right to object to the processing of personal data under Article 14 of the Directive, which can be exercised *inter alia* when the data subject becomes aware of whether or not a particular data controller respects the substantive data protection rules. The information and data access rights under Articles 10, 11 and 12 are of similar significance, since they are meant to make the flow of data transparent and, thereby, enable the data subject to exercise his rights, i.e. to implement the substantive data protection rules.

---

[732] Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits*., p. 86

[733] W. Kotschy, 'Directive 95/46/EC' in Concise European IT law (The Hague, Kluwer Law International, 2006), p. 56

[734] Robinson, et al, "Review of the European Data Protection Directive: Technical Report Prepared for the Information Commissioner's Office.", p. 8

Another significant element of the rights and obligations' aspect of the Directive's implementation mechanism is the fact that the exercise of any data protection right – whether substantive or implementation orientated - is always directly or indirectly backed up by the obligations of a data processing actor, who is almost always a controller.[735] For instance, the consent requirements of Articles 7 and 8 are interpreted as imposing an obligation on the data controller to ask for such consent, provided that there are no other grounds for legitimate processing. The information rights of Articles 10 and 11 are phrased *verbatim* as the obligations of the data controller to provide respective information. The Article 18 obligation to notify a supervisory authority also serves to back up the data subject's information rights. Finally, Article 6(2) provides that compliance with the general substantive principles of data processing that are listed in Article 6(1) - the fairness and lawfulness of processing, purpose limitation, etc. - is to be ensured by the data controller.

The allocation of the rights and obligations according to the Directive creates the basis of accountability that is vital for both participatory and top-down methods of implementation. The actors who are vested with obligations to respect data protection rights and comply with other substantive data protection principles are answerable for their violations to the data subjects and the self-regulatory and self-control bodies at the participatory level, as well as to the supervisory authorities at the top-down level. The Directive imposes the burden of compliance almost entirely on the data controllers – who are only one of several kinds of actors involved in data processing. A data controller is a person or entity who determines the purposes and means of the processing of personal data (Article 2(d)). At the same time, the Directive itself lists three other kinds of actors who can potentially be involved: a data processor (Article 2(e)), third parties (Article 2(g)), and a recipient of data (Article 2(f)). Relationships between a controller and a processor are governed by a contract (Article 17(3)). By means of this contract, the controller must ensure that the processor implements adequate security measures to prevent data security breaches. The burdens of notification and prior checking (Articles 18 and 20) are also carried by the controller. In the case of a violation, the controller is liable to the data subject for any damages suffered as a result, unless the controller proves that he is not responsible for the events giving rise to the violation (Article 23).

[735] One of the few exceptions is the confidentiality of the processing requirement of Article 16 of the Directive, which provides that "*any person* acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data must not process them except on instructions from the controller, unless he is required to do so by law." [Emphasis added]

ii. Co-regulation and self-control

Another aspect of the participatory implementation of the data protection principles is the co-regulation and self-control exercised by the data controllers themselves, both individually and collectively.

Data controllers individually bring the system of the data subjects' rights and the respective obligations of the controllers into action via compliance programs and *ad hoc* contractual arrangements, with the data processors prescribing, *inter alia*, the security measures to be taken. With regard to individual compliance efforts, compliance programs are not required by law, but, as Kuner suggests, they are vital for the compliance and compliance culture of a company.[736] Data protection officers have a "crucial role" in implementing and supervising the introduction of the program.[737] Their responsibilities may include: developing a system of benchmarks to measure the implementation of the policies and procedures as they work in practice; monitoring relevant legal developments; updating data processing notices; and developing procedures to deal with complaints and the questions of employees and customers and the inquiries of data protection authorities.[738] A member state may exempt data controllers, either completely or partially, from notification requirements if the latter appoint a data protection officer.

Data controllers exercise co-regulation and self-control collectively via national and European codes of conduct, thus implementing data protection principles within a specific industry, trust labels, and binding corporate rules. Unlike in the US, the European model of participatory implementation is not self-, but co-regulatory, since governments and EU bodies review and approve the proposed codes of conduct and binding corporate rules. On the other hand, neither is the model based purely on government regulation, as the controllers themselves draft the rules and standards that are specific to their industry.[739]

Article 27(1) of the 1995 Directive calls on member states to encourage the drawing up of appropriate codes of conduct. These are meant to contribute to the proper implementation of the general data protection principles in the specific contexts of individual industries, such as the financial services[740] and the public

---

[736] Kuner, *European Data Protection Law: Corporate Compliance and Regulation*., p. 250

[737] Ibid., p. 250

[738] Ibid., p. 242

[739] For more on the EU model of co-regulation and its comparison with the US model of self-regulation see Dennis D. Hirsch, "The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?," *ExpressO*(2010), http://works.bepress.com/dennis_hirsch/1

[740] E.g. De gedragscode voor de verwerking van persoonsgegevens van de Nederlandse Vereniging van Banken en het Verbond van Verzekeraars (the Code of conduct of the Dutch Bank Association and the Union of the Insurance companies regarding the processing of personal data) approved by the Dutch DPA on the 13th of April, 2010

transportation sectors[741]. The codes are adopted both at the national and European level and are approved by the national DPA or Article 29 Working Group respectively.[742]

Co-regulation also applies to cross-border data transfers, in particular in the form of binding corporate rules (BCRs). BCRs are a "set of legally-binding data processing rules adopted by a company or a group of companies and which grant rights to data subjects."[743] Quite innovative and increasingly popular, BCRs reduce the compliance efforts that are characteristic of *ad hoc* contractual arrangements and instead transfer an entire corporate group into a 'safe haven' in which data can be freely transferred within the group across borders.[744]

Trust labels, or privacy certification, are a form of self-control which is exercised without the participation of national and European supervisory authorities. They are issued by independent bodies to indicate compliance with relevant data protection rules and can be withdrawn in the case of violations. Although trust labels are not mentioned in the Directive, they are said to be helpful in establishing a trusting relationship with data subjects.[745]

b. Top-down implementation: supervisory authorities

By the top-down implementation of the 1995 Directive, this study refers to implementation tools which rely on the authority of the European Union and the member states. The authority is vested in general supervisory bodies and special data protection agencies.[746] These bodies and agencies monitor, supervise and enforce compliance with the substantive data protection rules.[747] Despite the indisputable significance of, and recent advances in, the participatory implementation mechanisms, such as self-regulation and self-control, the 1995 Directive puts the main emphasis on the top-down method of implementation, with a system of specific supervisory authorities as its cornerstone.

Compliance with the data protection rules, as with any piece of national legislation, is monitored and enforced by general national supervisory bodies.

---

[741] e.g. Gedragscode verwerking persoonsgegevens OV-chipkaart door OV-bedrijven (The Code of conduct regarding processing by the public transport companies of personal data in relation to the public transport chip card) the most recent available version of which was registered by the Court of the Hague on the 13th of February 2009, no. 16/2009

[742] The Report to the Information Commissioner's Office names two European-wide codes of conduct: the International Air Transportation Association (IATA) and the Federation of European Direct and Interactive Marketing (FEDMA) (Robinson, et al, "Review of the European Data Protection Directive: Technical Report Prepared for the Information Commissioner's Office.", pp. 9-10).

[743] Kuner, *European Data Protection Law: Corporate Compliance and Regulation*., p. 219

[744] Ibid., p. 220

[745] Robinson, et al, "Review of the European Data Protection Directive: Technical Report Prepared for the Information Commissioner's Office."

[746] Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits*., p. 86

[747] Ibid., p. 70

However, the 1995 Directive also prescribes the establishment of special supervisory authorities. They are commonly referred to as data protection authorities (DPAs). Article 28(1) requires each member state to establish one or more data protection authorities, which are to "act with complete independence in exercising the functions entrusted to them".[748]

Within the ambit of the DPAs' functions, as established by the Directive, is: the handling and resolution of complaints by citizens pertaining to the processing of personal data; consultations with national governments when administrative measures or regulations concerning data protection are drawn up (Article 28(2)); and monitoring, investigating and having the power to intervene in data processing operations, hear complaints and take legal action in the event of breaches of national data protection laws (28(3) and (4)). Moreover, the DPAs are also required to maintain a publicly accessible register containing information about the data processing activities of which they are notified pursuant to Articles 18 and 19.[749]

In practice, the powers of the DPAs are said to be "broad and largely discretionary."[750] The Directive is silent on whether these bodies should have the authority to impose fines and issue compensation orders,[751] with decisions on this matter being left to the discretion of the member states. It is also not completely clear whether national DPAs are required to have the power to issue legally binding orders, but interpretations of Article 28(3) in conjunction with Recitals 9-11 (DPAs should be given effective powers of intervention) support the view that such powers are obligatory.[752] "In most cases, they have [the] power to issue legally binding orders."[753]

Subject to some exceptions, the Directive also requires data controllers to notify the DPA about any wholly or partially automatic processing operations that they intend to undertake (Article 18(1)). As well as the notification regime, there is also a system of prior checks. However, according to Recital 54, these checks only apply to a limited number of the data processing operations that are "likely to present specific risks to the rights and freedoms of data subjects (Article 20(1))."[754] Consequently, Bygrave interprets the system of prior checks as being equivalent to

---

[748] As Bygrave explains, Article 28(1) requires DPAs to be functionally independent of governments and legislatures as opposed to simply having administrative independence. This requirement "boils down to the capacity for a data protection authority to arrive at its own decision in a concrete case without being given case-specific instructions by another body as to what line it should take." (Ibid. p. 71)

[749] Ibid., pp. 71-72

[750] Ibid., p. 71

[751] E.g. Hazel Grant reports on reforms to the powers of the British DPA, including a power to impose heavy fines; in Hazel Grant, "Data Protection 1998-2008," *Computer Law & Security Report* 25 (2009).

[752] Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits*., p. 72

[753] Ibid., p. 71

[754] Ibid., p. 76

licensing, meaning that DPAs may stop and prevent planned data processing operations.[755]

Although not a part of the 1995 Directive's system, the European Data Protection Supervisor ('EDPS') is also worth mentioning. It was created by Regulation (EC) 45/2001 pursuant to Article 286(2) of the Treaty Establishing the European Community. The purpose of both is to achieve a level of data protection in European institutions that is comparable with Directive 95/46/EC. The functions of the EDPS resemble those of a DPA under the Directive. He or she: conducts prior checks of data processing operations to ensure compliance with the data protection standards set out in the Regulation; considers individual complaints; and advises European institutions on proposals of new legislation and assesses the likely impact thereof on data protection. The EDPS may also intervene in proceedings in the Court of Justice if a case has, or is likely to have, an impact on data protection.

Another institution that has been established in the area of European data protection is the Article 29 Working Party on the Protection of Individuals with regard to the processing of personal data. Article 30 states that the group is to aid the Commission by providing advice on: issues relating to the uniform application of national measures adopted pursuant to the Directive; data protection in non EU-countries; possible changes to the Directive and other instruments affecting data protection; and codes of conduct drawn up at the EC level. Unlike national DPAs, the Working Party has no direct impact on the grass-roots enforcement of data protection principles, since it only has advisory powers at this level.

2.3. Analysis of the current European approach to data protection

Following this brief overview of European data protection law, it is time for the discussion to move on to this chapter's core question, namely whether this branch of the law has any weaknesses which prevent it from properly dealing with the data processing problem.

The issue of the effectiveness of existing national and European data protection law has already been addressed in a number of studies which have focused on both the European approach to data protection overall as well as individual data protection norms, like the consent requirement and the purpose limitation rule.[756] The chosen balance between the interests of the data subjects and

---

[755] Ibid., p. 76

[756] The most recent examples of such studies are Poullet, "Data Protection Legislation: What Is at Stake for Our Society and Democracy?.", R. Brownsword, "Consent in Data Protection," in *Reinventing Data Protection?* (2009)., Bygrave, "Consent, Proportionality and Collective Power.", Wright et al, "Privacy, Trust and Policy-Making: Challenges and Responses.", Charles D. Raab, Koops, Bert-Jaap, "Privacy Actors, Performances, and the Future of Privacy Protection," in *Reinventing Data Protection?*, ed. Serge

those of society at large, and the way in which this balance is achieved, has been widely criticized in terms of: flaws in legal drafting techniques and the inelegant architecture of the instruments;[757] the vagueness of the provisions which lead to discrepancies in national implementation and undermine the effectiveness of international and supranational standards;[758] and more fundamental criticisms of the underlying principles of data protection.[759]

In 2008, the Information Commissioner's Office and the European Commission asked a multidisciplinary international team of researchers to evaluate the strengths and weaknesses of the European Data Protection Directive and make proposals for its improvement.[760] The resulting 2009 report will receive particular attention in this study. This is due to its completeness in presenting the perspectives of the various stakeholders and parties to the discourse, including data protection experts: both from the field of research and practitioners, speaking on behalf of data subjects and the businesses involved in data processing. Sections 2.3.1 and 2.3.2 of this chapter will provide a brief account of the strengths and weaknesses of the European approach to data protection, focusing respectively on the substantive principles and the norms underlying the system of implementation. Section 2.3.3 will briefly address the weaknesses, such as the imperfections of the legal technique, etc. which are difficult to classify as either principal shortcomings or failures of the implementation system.

2.3.1. Adequacy of the substantive norms of data protection

As far as the value choices embodied in the substantive principles of the data protection system in Europe are concerned, the data protection community has viewed their very existence positively. Even critics of the current data protection mechanisms mostly[761] agree that some protection is necessary in today's information-

---

Gutwirth, Poullet, Yves, de Hert, Paul (Springer, 2009)., Bert-Jaap Koops, "Law, Technology, and Shifting Power Relations," *TILT Law and Technology Working Paper Series* September (2009). etc.

[757] E.g. Brownsword criticizes the architecture of the Directive in Brownsword, "Consent in Data Protection."

[758] E.g. Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits*., p. 35 and Brownsword, "Consent in Data Protection." p. 84 (which states that the directive is "unacceptably opaque".)

[759] One of the quite radical objections to the current data protection regime questions whether the limitations on the flow of data are, in principle, consistent with the operation of a modern information society (e.g. David Brin, *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?* (1998)). Koops believes that such a radical change of approach is deserving of serious consideration if the current system proves to be impossible to apply to the actual conditions of the modern information society (Koops, "Law, Technology, and Shifting Power Relations.").

[760] Robinson, et al, "Review of the European Data Protection Directive: Technical Report Prepared for the Information Commissioner's Office.", p. ii

[761] "Abandoning the Directive as it currently stands is widely (although not unanimously) seen as the worst option" (Ibid., p. vii).

driven environment.[762] When it comes to the 1995 Directive, the 2009 report to the Information Commissioner lists a number of its positive effects. At the most basic level, and even though the actual effects of the data protection principles may be limited, the simple fact that these standards have been formulated provides a blueprint for the debate about personal data[763] and raises awareness of data protection concerns.[764] A more tangible effect of the substantive data protection rules, particularly at the international and supranational levels, is the introduction of common legal principles and concepts. These ensure the presence of a harmonized legal framework for data protection, which assists trans-border dialogue and data flow and, at least in the case of the Directive, has enabled the establishment of an internal market for personal data.[765] The reliance of the European data protection regime on abstract principles rather than more detailed rules has ensured that the flexible regulatory framework can be adjusted to reflect the specificities of national legal systems, as well as being neutral to the context of a specific sector of data processing, such as private or government processing, or new technological developments, such as emergence of RFID.[766]

Finally, with the issue of implementation put to one side until Section 2.3.2, it is clear from consideration of the substantive principles that they have been introduced as a response to data protection concerns, and were, thus, intended to have a positive impact on the provision of a solution to the data protection problem. The relationships between the substantive data protection principles and precise data related concerns are complex. One principle may target a number of concerns, while some concerns are addressed by more than one substantive principle. What follows is only a simplified account of these relationships.

---

[762] Koops, "Law, Technology, and Shifting Power Relations.", p. 31

[763] "One of the most frequently quoted positive aspects of the Directive was the impact it has had in structuring and organizing the debate surrounding data protection. While OECD Guidelines were very influential in shaping this debate, the Directive can be credited with formulating legally binding rules that have become effective law across the Member States." (Robinson, et al, "Review of the European Data Protection Directive: Technical Report Prepared for the Information Commissioner's Office.", p. 22)

[764] Ibid., p. 24

[765] Ibid., p. 23 quoting D. Korff, "EC Study on the Implementation of the Data Protection Directive - Comparative Summary of National Laws." available at <http://ec.europa.eu/justice_home/fsj/privacy/docs/lawreport/consultation/univessex-comparativestudy_en.pdf>

[766] Robinson, et al, "Review of the European Data Protection Directive: Technical Report Prepared for the Information Commissioner's Office.", p. 24, Wright et al, "Privacy, Trust and Policy-Making: Challenges and Responses.". In subsequent parts of this chapter this study will criticize the 1995 Directive for its failure to keep up with new technological developments, such as chain informatisation, cloud computing and ambient intelligence. The reader should bear in mind that the reasons for this failure, according to this study, lie not in the substantive principles but in the implementation norms.

The principles of fair and lawful processing, data security and minimality, disclosure limitation, and information self-determination are intended to guard the privacy of an individual. They are understood as relating to someone's right to ensure the secrecy of, or control over, his private information. Indeed, the presumption behind Articles 7 and 8 of the Directive is the notion that, by default, the processing of personal data is unlawful and not allowed unless certain conditions relating to legitimate processing are met. The consent of the data subject is the most important of these conditions when the processing concerns special categories of personal data which are viewed as 'sensitive' and 'private'. The principle of information self-determination, including the requirement of consent and the acknowledgement of information rights, gives an individual - albeit limited – control over the disclosure of his personal data. The other principles limit the further unauthorized distribution of personal information.

The limitations on the collection and distribution of personal data, the combination of the rights of data subjects and the obligations of data processing actors, and the general principle of fairness all contribute to the maintenance of a power balance between the two sides to a personal data related transaction. The inherently weaker position of an individual is also dealt with by the introduction of information rights and rights of control, which are exercised directly or via supervisory authorities. The secrecy of sensitive data, the limited availability of other personal information, individual control, and the right power balance are among the rules that are intended to contribute to the causes of individual freedom and autonomy.

The principle of information quality addresses the fear of errors and misrepresentation with demands that personal data should be valid, relevant and complete with respect to the purposes of processing.[767]

Quantitative limitations on the flow of data, which are imposed, for example, by the minimality and distribution limitation principles, are intended, *inter alia*, to prevent the fear of 'perfect knowledge' and the dehumanization of a data subject becoming reality. The principle of fairness, along with legality and purpose specification etc., is aimed at tackling the dangers of profiling, such as manipulation and inequality. Concerns about the lack of transparency and accountability in the flow of data are addressed by the data protection rules that are qualified as being implementation-orientated. These fears will, therefore, be addressed in the next section.

Many European data protection commentators share the opinion that the 1995 Directive's substantive norms are not perfect, but, of the alternatives available, are the lesser evil and can be improved without the need for fundamental changes. For instance, De Hert, Wright, Gutwirth and others call for the more context-sensitive

[767] Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits*., p. 62

regulation of data processing,[768] while Cuijpers and Koops, among others, argue that to provide effective protection, the current data protection principles should be effected also in the context of consumer protection.[769] Bygrave and Brownsword are among numerous authors who have examined and criticize the imperfections of the consent requirement: e.g. the vulnerability of a data subject and the effective absence of real choice; an individual's inability to fully evaluate the substance and consequences of what he is consenting to; and the excessively broad application of the consent requirement which, at times, erroneously dominates the other conditions of legitimate processing. The report to the Information Commissioner's Office criticizes the fact that privacy policies are the main way of obtaining informed consent from a data subject online, despite their failure to ensure truly free and informed consent. The report notes that these privacy policies, like standard contractual clauses concerning data protection, are not easily accessible, are not read and, even if they are, are difficult for many consumers to understand, and are also often unfair, leaving a consumer with no real choice.[770] Despite these comments, Bygrave and Brownsword conclude that, with some adjustments in interpretation and application, consent should continue to be one of the key data protection rules.[771]

Koops is one of the few authors who, in some of his work, have principal objections to the current substantive data protection principles. Koops doubts whether the principle of purpose specification is compatible with the modern information society, which runs on databases.[772] His criticism may be extended to the data minimality and disclosure limitation principles, since they impose quantitative limitations on the modern flow of data. Koops warns that if the old approach to data protection does not deal with these issues, one should consider a more fundamental switch to a much less conventional alternative, namely the complete openness of information pertaining to both individuals and the information industry, with a view to the fair rebalancing of power in today's information society.[773]

However, this study maintains the view that criticisms of the substantive data protection rules have little to do with the actual substance or value choices thereof, and relate more to the fact that compliance with these rules is poor, whether due to principal failures of the Directive's implementation system, or for other reasons, such

---

[768] Wright et al, "Privacy, Trust and Policy-Making: Challenges and Responses."
[769] C.M.K.C. Cuijpers, Koops, Bert-Jaap, "How Fragmentation in European Law Undermines Consumer Protection: The Case of Location-Based Services," *European Law Review*, no. 6 (2008).
[770] Robinson et al, "Review of the European Data Protection Directive: Technical Report Prepared for the Information Commissioner's Office.", pp. 29-30
[771] Bygrave, "Consent, Proportionality and Collective Power." And Brownsword, "Consent in Data Protection." For more on the criticism of the consent requirement and its rebuttal see Chapter 10.
[772] Koops, "Law, Technology, and Shifting Power Relations.", p. 27 ("The logic of the world that thrives on databases therefore is at odds with purpose specification and use limitation, two important principles of the data protection framework. In today's reality, I seriously doubt that purpose specification and use limitation are playing any substantial role in practice.")
[773] Ibid.

as deficiencies in legal drafting techniques. Indeed, it is difficult to argue against the qualitative and quantitative limitations imposed on data processing. Firstly, as has been pointed out earlier, a majority of the community of experts and policy-makers agrees that there should be some limitations on data processing. Secondly, the criticism is not well developed, since the communities referred to are still not completely clear about the set of values and goals that the data protection regime serves, or the final goals that this branch of the law aims to achieve.[774] When it comes to the concerns outlined in Chapter 3, and as seen above, the substantive data protection rules are able to address all of these, at least on a conceptual level.

At the practice level, however, it is also clear that data processing actors do not always prioritize these rules in their activities. Accordingly, instead of just discarding the old substantive rules for their failures, and beginning a search for new ones, the next part of this study analyzes the system for implementing the rules that are already in place. The rationale for this is that before reconsidering the old substantive choices, a careful look should be taken at how well they have been implemented and if they actually have the effect they were intended to.

2.3.2. Shortcomings of the implementation mechanisms

The following review of the European data protection regime's implementation mechanisms will draw on the 1995 Directive: it is the only European document that is detailed enough to be the primary reference point for an analysis of the relevant implementation tools. Although the Directive is commonly praised for its substantive principles, the implementation tools established in the document are frequently the focus of criticism and discontent. The 2009 report for the Information Commissioner's Office, which has already been mentioned in this study, concludes that "substantial dissatisfaction also exists [...] most notably, on the processes that the Directive has provided to make these [substantive] principles a reality."[775]

Consistent with the findings of the report, this section will demonstrate that the implementation system is failing to address the challenges of transparency and accountability at both the top-down and participatory level. This section will show that the participatory mechanisms of implementation are failing to create relationships of accountability between the data subject and the data processing actor via the interaction of their rights and obligations and the self-regulation and control tools. (3.2.1). The top-down implementation tools also suffer from a number of

---

[774] See Chapters 2 and 3 of this study; also see Bygrave, who points out that even the substantive rules of data protection are procedural in nature because the policy-makers were unsure about the substance of the problem they were trying to tackle (Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits*., p. 384-385).

[775] Robinson et al, "Review of the European Data Protection Directive: Technical Report Prepared for the Information Commissioner's Office.", p. 38

weaknesses, making it difficult to monitor compliance with, and enforce, the substantive data protection rules when they are violated (3.2.2).

a. Participatory implementation

This section will demonstrate that the Directive's model of accountable relationships between the data subject and the data processing actor does not function well when it comes to the modern flow of data. More precisely, the system of rights and obligations established in the Directive has not caught up with the complexity of the actual relationships between those involved in data processing. These implementation mechanisms are unable to cope with the intensity and opacity of the modern data flow. As a result, the substantive rules in the Directive are difficult to monitor and enforce, and there is little motivation to comply with them. The system of self-regulation and control also faces a number of challenges. The analysis herein will begin with the system of rights and obligations, which forms the Directive's model for accountable relationships.

i. Rights and obligations

The system of rights and obligations created by the Directive is rather simple. It names five actors who are active in data processing and, therefore, potentially relevant. The first such actor is a data subject, namely an identified or identifiable person who, directly or indirectly, can be identified by reference to personal data (Article 2(a)). A data controller is defined as a person or entity who determines the purposes and means of the processing of personal data (Article 2(d)). There is then a data processor, who processes the data on behalf of the controller (Article 2(e)), as well as third parties who are authorized to process personal data under the direct authority of the controller or processor (Article 2(g)), along with a recipient to whom the data is disclosed (Article 2(f)).[776] The data subject has a number of data protection rights and the data controller has a number of corresponding obligations to respect and facilitate the enjoyment thereof. Within the participatory mechanism of implementation, the data controller is accountable to the data subject for the fulfilment of the said obligations and the implementation of the rights. In other words, the Directive - with minor exceptions[777] - imposes the entire burden of compliance with the data protection obligations on the data controllers, who are only one particular type of actor involved in data processing and who can be distinguished from the others involved on the basis that they determine the purposes of the actual processing of personal data. Relationships between a controller and processor, and the obligations of the latter, are governed by a contract (Article 17(3)),

[776] Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits*., p.21
[777] See Section 2.2.2(a) of this chapter.

which is only binding on the contractual parties, and, therefore, gives no rights to the data subject. The obligations of the other actors are not mentioned in the Directive, making the controller the only accountable actor. In other words, the accountability relationship established in the Directive is quite linear and involves only a data subject and a data controller.

A thesis to be proved by subsequent analysis concerns the fact that whereas the Directive differentiates between the various actors involved in the processing of data in terms of their obligations and accountability, when it comes to the actual data processing relationships themselves there is no real difference in terms of who gets access to and controls the data. The Directive effectively enables an entire group of data processing actors to avoid accountability for their actions. As a result, it fails to shape data processing in ways, which respect the data protection principles. In other words, the accountability relationship model in the Directive is formulated as a 'data subject - data controller' link, whereas it should be 'data subject - an entity in possession of personal data' instead. So, let us now consider some instances in the Directive of when the distribution of rights and obligations between a data subject, controller and non-controller does not work.[778]

The first example relates to the technology of cloud computing. 'Cloud computing' stands for a new way to provide IT applications, platforms and infrastructure based on a a utility approach: instead of investing in its own hardware, software and needed personnel, a cloud client chooses to use these resources available on the Internet or via another network and pays only for the resources consumed. Cloud computing relies on the possibility of resource pooling, i.e. the vendor has multiple data centres located in multiple locations where all data is stored. The location of those centres is not relevant for the provision of the services. The feature distinguishing the cloud computing from regular IT outsourcing is that cloud services are virtualised and accessible via a network.[779]

The Google Documents application allows its users to create, access and edit text documents, spreadsheets, presentations, etc. online at any point in time, without having to install the more conventional Office software. When subscribing to and using the services, an individual not only provides his personal data, but also

---

[778] Given the multiplicity and variety of the business models in the sphere of computer services, the problem of distinguishing between a data controller and a data processor is rather common in the data protection law literature. See, e.g. Kuner, *European Data Protection Law: Corporate Compliance and Regulation*., pp. 70-71. The Report to the Information Commissioner's Office concludes that: "The relationship between processor and data controller envisaged in the Directive does not adequately cover all the entities involved in the processing of personal data in a modern networked economy. There is uncertainty about when a processor becomes a controller or vice versa, particularly in an online environment where the act of visiting a website might result in cookies being sent from a number of sources scattered around the globe." (Robinson et al, "Review of the European Data Protection Directive: Technical Report Prepared for the Information Commissioner's Office.", p. 36)

[779] Lieneke Viergever, "Privacy in De Cloud," *Tijdschift voor internet recht* 2010, no. 3 Junie (2010).

determines how and for what purposes it will be processed.[780] In other words, the individual has two roles: one as a data subject and one as a data controller. Google is only a provider of the services in the cloud. It is, thus, simply a processor, since it only handles personal information in order to deliver the service in question. In this role of processor, Google has obligations and is liable for data protection violations only within the scope of its contractual agreement with an individual, in this case in the form of general terms and conditions and a privacy policy. However, it is rather difficult to imagine that an individual who is using the Google Docs' service is meaningfully in control of the operations that Google undertakes with his data. It is also difficult for the individual to influence the content of Google's contractual obligations. Indeed, the negotiating power of an individual vis-à-vis a large corporation such as Google is already limited. In addition, in the case of a company's general terms and conditions, the only choices a consumer normally has is to either agree with the terms as determined by the service provider, or to not accept them and, therefore, be unable to use the services. When there is another provider offering similar services on better terms, the individual can, of course, opt for these. However, in cases, where an individual only has access to one service provider, or the service in question is unique, the only choice is to "take it or leave it."

Furthermore, the ENISA report concludes that it can be difficult for any cloud customer (including a business which is using a cloud to, e.g. administer its payroll and is thus also a controller) to check the data processing undertaken by the cloud provider, and "thus be sure that the data is handled in a lawful way"; there may be data security breaches about which the controller is not informed by the cloud provider. Indeed, the cloud customer may well lose control of the data that is processed by the cloud provider, especially in cases of multiple transfers of data between clouds. Finally, the cloud provider may possess data which has not been lawfully collected. This may also apply to its customers,[781] such as an individual who may have data pertaining to other individuals, e.g. photos of friends, and is thus a controller, and not a data subject, with regard to this data.

The reality of business models is such that the providers of online (cloud) services may act not only as processors, but may also process personal data for purposes and in ways that they themselves deem to be necessary. For instance,

---

[780] Google Documents' privacy policy of 30 October 2009 reads: "Files you create, upload, or copy to Google Docs may, if you choose, be read, copied, used and redistributed by people you know or, again if you choose, by people you do not know. Information you disclose using the chat function of Google Docs may be read, copied, used and redistributed by people participating in the chat. Use care when including sensitive personal information in files you share or in chat sessions, such as social security numbers, financial account information, home addresses or phone numbers." (available at <http://www.google.com/google-d-s/intl/en/privacy.html>)

[781] ENISA, "Cloud Computing: Benefits,Risks and Recommendations for Information Security," ed. Daniele Catteddu, Hogben, Giles (European Network and Information Security Agency, 2009)., pp. 46-47

Rebecca Wong has argued that on social networking sites such as Twitter and Facebook, individual users who post information about their friends should be regarded as controllers, as should Facebook itself.[782] It seems to be valid to further claim that Facebook applications also constitute controllers when they provide an individual with access to games, quizzes and other services in exchange for access to the data of the user and his friends.

The distribution of rights and obligations according to the Directive also seems to fail when applied to the circumstances of ambient intelligence. If, as is probably true in most cases, the individual determines the goals and means of processing in order to maintain the functioning of an ambient intelligence system in his home, the data subject will also be a data controller. Accordingly, he will be responsible for selecting a processor who will respect his data protection rights. The processor will, however, only be liable within the scope of his contractual obligations, while the individual as a consumer, but also as a controller, will probably be unable to influence these terms.

In the case of chain informatisation, as employed by co-operating governments and/or private agencies, each participating body shares the personal data it has gathered and is in its possession with other participants, and also decides its own purposes and means of data processing. A clear example would be the sharing of medical files between general practitioners, medical specialists and hospitals, all of which have their own specific interest in a patient's data. Consequently, all of the participating entities may be regarded as controllers. For instance, a group of the five largest Dutch public transportation companies have collaborated in creating a system for a national public transportation card – the 'OV chipkaArticle' This is a personalized, or anonymous, smart card, which will soon replace paper tickets and is marketed as a fast and convenient way to pay for public transport electronically by checking in and out of a vehicle. It is also meant to reduce fare dodging and improve safety at train stations by limiting access to the card holders who have checked in. A personalized card[783] allows the collection of various kinds of personal data, such as name, address, the number of the card, the routes taken and the transactions conducted when using the card, such as checking in and

---

[782] Rebecca Wong, "Social Networking: Anybody Is a Data Controller?," *Social Science Research Network* (2008). The opinion of the Article 29 Working Party of 16 February 2010 on the concepts of 'controller' and 'processor' allows the possibility that several controllers exist with regard to one piece of data (WP 173)

[783] The anonymous chip card with a number, at least theoretically, also provides an opportunity to collect personal data as long as it can be linked to the person using it, e.g. when uploading the balance on a card online or using a bank card. Although according to the Trans Link Systems' statement on personal data, the OV-companies made a commitment not to attempt to identify users of anonymous cards in case a user reveals his personal data, e.g. to request a reimbursement in the case of a delay, etc., the holder of the card becomes personally known to the relevant OV-company. (TransLinksSystemsB.V., "De Ov-Chipkaart and Uw Persoonsgegevens." available at <http://www.ov-chipkaArticlenl/pdf/22246/ovchipenuwpersoonsgegevens>)

out and uploading the balance.[784] Apart from using the data in the manner declared in the Trans Link Systems' statement,[785] namely for payments, issuing and cancelling the card, providing customer assistance etc., the representatives of the Dutch railway company – NS – are known to have admitted that its motives in signing up to the OV chip card system included, at least in part, the desire to study and then influence, *inter alia* by pricing, passenger behaviour when using trains, e.g. in peak hours.[786] From 2010, the data collected from the chip card can be also used for direct marketing purposes.[787]

The data-sharing scheme in the case of the OV-chipkaart is quite complex. At the moment it involves five major public transport companies: NS (railways), Connexxion (buses), RET (Rotterdam public transport), GVB (Amsterdam public transport), and HTM (The Hague public transport) and their joint venture: 'Trans Link Systems' (TLS), which was created to manage the public transport ("OV") system.[788] In cases where a personalized card is requested from the TLS, the data is available to the TLS. If the personalized card is obtained from an OV-company, the data is available to the TLS and that OV-company when the card-holder uses the chipkaart or other TLS services, such as for transactions and a balance overview. In cases where a holder of an OV card has uploaded to it a personalized product from an OV company, such as a discount or monthly subscription, this data will be accessible to the OV company and the TLS. Accordingly, the personal data that is linked to one OV card may be accessible to several OV companies if their personalized services are uploaded onto the card. Despite this, the TLS statement does not clarify that an OV company providing a personalized service to a card-holder may have access to the data accumulated with regard to other personalized services of other companies.

In such a complicated chain it is not easy for an individual to determine - both as a matter of fact and law – which entity in this chain is the controller who is liable when there is a violation. Paragraph 12 of the Code of Conduct[789] adopted by the public transportation companies involved with the TLS reaffirms its liability and establishes a complaints' procedure against the entity at fault if a privacy violation occurs. However, as a matter of fact, given that a piece of personal data in a chain is

---

[784] Ibid.

[785] Ibid.

[786] Presentation given by Pim Bonenkamp in the series of TILT public lectures at Tilburg University on April, 21, 2010.

[787] TransLinksSystemsB.V., "De Ov-Chipkaart and Uw Persoonsgegevens."

[788] As the card becomes more widely used and replaces paper tickets, the pressure on other public transportation companies to join in will probably also increase.

[789] Gedragscode verwerking persoonsgegevens OV-chipkaart door OV-bedrijven, vastgesteld op 21 juni 2007 door Mobis en gedeponeerd bij de Rechtbank te 's-Gravenhage op 10 juli 2007 onder nummer 50/2007. Gewijzigd op 6 februari 2009 en vastgesteld door de OV-bedrijven die de OV-chipkaart accepteren en op hun verzoek door KNV gedeponeerd bij de Rechtbank te 's-Gravenhage op 13 februari 2009 onder nummer 16/2009.

accessible to numerous actors, it would be difficult to determine where exactly in the chain the violation took place.

As a matter of law, even if the identity of the entity at fault is established, it may be difficult to prove that this body was indeed the controller determining the means and goals of the data processing when the violation occurred. The entities in a chain often determine their relationships and the distribution of liability for data processing violations in special – mostly internal - agreements. However, these agreements are rarely accessible to data subjects and are, therefore, little help in determining to which entity the data subject can address his complaint or seek damages.[790] Moreover, the internal agreements in question give rise to the rights and obligations of the parties thereto – the OV companies - and do not create rights for individuals.

In addition, as the data processing practices in cloud computing, chain informatisation and ambient intelligence become more opaque, and since the handling of personal data is outsourced and the control thereof changes hands, the roles of the various actors involved become more confused, and the opportunities for the abuse of data, without accountability, increase.[791]

In the circumstances of modern data processing, and under the Directive's system of data protection rights and obligations, the opaqueness of the scheme to an outsider, including data subjects and the authorities supervising the data practices, relationships, and business models, leads to an invalid and confusing description of who is accountable for violations. All of this has a detrimental effect on the implementation of the data protection principles at the participatory level.

It would be unfair to state that the European data protection institutions do not acknowledge the difficulties allocating data protection responsibilities in the context of modern personal data processing. In fact, on 16 February 2010 Art. 29 Working Party adopted an opinion 1/2010 on the concepts of "controller" and "processor" (WP 169) where it clarified the application of the two categories of controller and processor in the context of unprecedented proliferation and globalisation of the technologically advanced data processing. The opinion addressed such issues as a definition of the controller and a processor, a possibility of multiple (co-) controllers and their joint and several liability, liability of the processor, etc. The Working Party also concluded that they do not see a reason to eliminate the distinction between the controller and the processor regarding their

---

[790] Such an agreement regulating the distribution of responsibilities was mentioned by Pim Bonenkamp in his presentation at TILT in fn 785;

[791] ENISA, "Enisa Cloud Computing Report." p. 110 ("[T]he customer may be reluctant to see the cloud provider outsource all or part of the services to be provided to the customer.")

responsibility.[792] However, although this opinion does eliminate some weaknesses of the current European data protection system by making the distribution of responsibility less rigid, more transparent and up-to-date, this clarification does not make an evident difference regarding the position of the individual data subject and therefore does not undermine the validity of the argument developed in this study.

The most important clarification introduced regarding the application of the categories of "controller" and "processor" is that this distinction should be applied pragmatically. That is, the in deciding which actor determines goals and means of processing one should not only look at formal contractual and statutory (criminal, civil, and administrative law) arrangements but rather allocate responsibility where the factual influence is. This pragmatic approach has two important implications: firstly, an actor without lawful competence to process data, e.g. an employee or (formally) a processor acting outside an assignment of a (formal) controller should be regarded as a controller himself and found responsible. Secondly, there may be multiple co-controllers with regard to one data processing operation. Simultaneously, this does not mean that the processor cannot have any discretion in determining the (organisational and technical) aspects of data processing. The test to determine whether a particular actor qualifies as a processor or a controller is whether he would have processed data without the formal controller's assignment. In case the answer is no, the actor qualifies as a processor. The evaluation of the distribution of roles between the involved actors should be conducted on a case-by-case basis.[793]

On the one hand, the WP's opinion is welcome since it broadens the interpretation of the concept of "controller" applying the concept de facto rather than formally and thereby extending the range of the actors with a responsibility for lawful and fair data processing. In addition, it is explained that one and the same actor can be a processor and a controller of the same piece of data at the same time, e.g. in the context of various data processing operations. A cloud service vendor acting within the service contract is a processor. But as soon as he processes the same bunch of personal data for his own purposes, e.g. sells a customer database of a cloud client, it also becomes a processor. As a result of such a flexible approach, at least in theory the Working Party's clarification should improve the chance to hold an actor guilty of a data protection breach responsible and prevent him from hiding

[792] p. 33
[793] III.1.a), b)

from responsibility behind the fact that he did not have a formal competence to determine goals and means of processing.

On the other hand, the WP opinion - at least as the author reads it – does not resolve the problems of application of the two categories completely, which is, possibly, symptomatic of the fact that the distinction between the two sorts of actors does not function well in modern reality. Firstly, the WP opinion does not significantly improve the position of the data subject when he faces a data protection violation. Making the application of the controller-processor dichotomy a matter of a case-by-case evaluation and an assessment of the factual distribution of control over data processing, the WP 173 opinion does not simplify the task of the individual to establish who in a cloud or a chain was in fact in control over the unlawful processing. Indeed, given the complexity and opacity of the data flows in the world of seamless networks, even large organisations have difficulties establishing where a piece of personal data is located.[794] The individual without relevant expertise or access to the relevant information is even less expected to be able to figure that out. The situation becomes even more complex given that there may be more than one controller with regard to one data processing operation.[795]

Secondly, the functional application of the controller-processor dichotomy, although better than rigid allocation of the roles, is not consistent with the logic of use of the categories of controller and processor in the Directive and other data protection instruments. Indeed, the notion of a controller is significant not only on the stage of liability *after* a data protection violation took place. The controller also has pre-processing responsibilities, such as seeking a consent of a data subject or establishing any other legitimate ground for legal processing; notifying the DPA or informing the data subject; applying for an authorisation for a transborder data transfer, etc. The fact that knowing who a controller is *before* a violation occurs is as important as knowing it after is also manifest in the presence of two standard contractual clauses developed by the Commission: one for a transfer to a non-EEA controller[796] and another – to a non-EEA data processor.[797]

---

[794] see the presentation of the French DPA where it is stated that in cloud processing it is only possible to determine a country whene data is stored and not more (TELECOM PARISTECH, 16 November, 2010 available at <bilab.enst.fr/fichiers/cnil.pdf>).

[795] WP 173, p. 22

[796] Commission decisions of 2001 and 2004 establishing two sets of alternative standard contractual clauses for the transfer of personal data to controllers in third countries.

As has been illustrated above, in the modern data flow it is difficult to identify the specific actor processing a particular piece of personal data. Moreover, where there is a violation, determining if a certain actor is a controller may also be problematic. What is more, the current system, which relies on the obligations and the liability of controllers, does not encourage those who cannot be unambiguously classified as controllers to take steps to ensure that there is a proper level of data protection, since there is no immediate likelihood of legal action, but a delayed contractual liability instead. It may be argued that assigning liability to the controller in all cases assists data subjects by strengthening their position; indeed, if a processor is at fault for a breach, an individual in a data protection dispute may be aided by controllers who are large companies just like their opponents. This arguably serves to protect a data subject, who is a weaker party, and reassigns the burden of dispute resolution to the controller, a more powerful corporation. However, before this happens, an individual first has to face that same corporation and successfully argue his point. Moreover, whether or not to pursue the processor is at the discretion of controllers and, particularly in cases of individual and other low-profile breaches, deciding not to do so is the cheaper option. Finally, in the light of outsourcing and shifts in the control of personal data, when something goes wrong in the data flow of a social networking site, and personal data is abused, corrupted, or disclosed to third parties as a result of a security breach, knowing precisely who the controller is, within which fragment of the cloud or chain the breach occurred, and which specific controller is liable is still difficult to establish with any certainty. In other words, the current model of accountable relationships between a data subject and controller is an inaccurate description of the reality of data processing relationships and, therefore, does nothing to aid the transparency of modern data processing. Moreover, the rigid framework of roles causes confusion and undermines the effectiveness of the mechanisms of accountability.

ii. Co-regulation and self-control

The system of co-regulation and self-control is also burdened with flaws. Some of these have already been addressed in the preceding section on accountability. In brief, it has been shown that a data processing actor does not always have a clearly defined role and his data protection obligations are not necessarily obvious. Moreover, a responsible data controller is not always easy to identify. These and other factors have a detrimental effect on the motivation and ability of the processors and their data protection officers to comply with data protection standards by exercising self-control. The contracts between a data controller and data processor,

---

[797] Commission decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council

which govern their relationships, are not always accessible and transparent to data subjects, are binding only between the parties, and do not give rise to any rights on the part of the data subjects. In addition, in the case of international data transfers, Kuner points out that drafting *ad hoc* contracts for each transaction may be too burdensome and confusing, since "the applicability of which must be determined for each particular data transfer."[798] He suggests that the system of contracts in data protection would benefit from "a more integrated, holistic approach which would allow them to transfer personal data freely […], without having to determine whether a particular exception applies, or without concluding a set of contractual clauses among all their corporate entities."[799] The subsequent analysis will focus on the remaining tools of co-regulation and self-control.

Let us start with co-regulation in general. The system employed in Europe has been widely praised and has even attracted the attention of US data protection scholars for its combination of strong approaches to self and government regulation. For instance, as with self-regulation, co-regulation allows there to be unique knowledge of a particular sector when its industries have become involved in the rule-making process. The adopted rules are, as a result, superior in quality: they are more realistic and tailored to meet the realities of a particular industry.[800] Simultaneously, government involvement is supposed to transform regulatory relationships from being adversarial in nature to a collaborative partnership in which private companies prioritize public interest and governments and private actors feel accountable to each other.[801]

However, along with strong approaches to self and government regulation, the system of co-regulation has also inherited the weaknesses of these two models along with some of its own. For instance, the opponents of co-regulation doubt whether industry will be willing to reveal its secrets to a government regulator, or be governed by anything else other than self-interest.[802] As with government regulation, the participation of the supervisory authorities may also be too heavy a burden on the functioning of an industry. Hirsch names a number of objections to co-regulation arising from public administration theory: fear of agency 'capture' by the regulated industry, the industry's abuse of its knowledge to weaken the standards of protection and, at the same time, an information deficit on the part of the supervisory authorities, preventing an adequate review of the proposed rules, etc.[803]

---

798 Kuner, *European Data Protection Law: Corporate Compliance and Regulation*., pp. 218-19

799 Ibid., pp. 218-19

800 For a brief overview of the advantages of co-regulation, see Hirsch, "The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?.", pp.4-5 and p. 43 et seq.

801 Ibid., p. 43

802 Ibid.

803 Hirsch, "The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?.", p. 45 et seq.

The 2009 report to the Information Commissioner's Office confirmed some of these fears, in particular, those of regulatory burden and industry self-interest. Indeed, the report states that the former is one of the key reasons for the less than successful implementation of the concept of codes of conduct. To be fair, the codes do have some positive impact on data protection. For instance, at present, codes of conducts are the only tool to address RFID systems specifically.[804] However, the report also concluded that the bureaucracy involved in their review, especially when a code or a contract has to be amended even slightly, "is clearly a burden for authorities and controllers."[805] The fear of the bureaucracy burden is also present in cases of binding corporate rules. When giving advice on framing compliance strategies, Christopher Kuner warns that "the decision to apply for approval of BCRs is not to be taken lightly. […T]he approval process can be lengthy, and implementation can be expensive and difficult for all but large multinationals."[806]

As to the fear that industries will be guided by self-interest rather than data protection principles, the report found that the controllers, when using privacy policies to satisfy the transparency requirement, tried to meet the formal legal requirements rather than seeking to address the real transparency needs of a consumer.[807]

Given the difficulties associated with implementing co-regulation strategies, one cannot be surprised at the general observation of data protection experts that "self and co-regulation have not taken on a key role in European data protection practices, despite the emphasis given to them."[808] The popularity of codes of conduct also varies a great deal from country to country.

Moreover, in practice, codes of conduct exist almost exclusively at the national level, with only two such documents approved European-wide.[809] Another plausible explanation of their lack of popularity that is set out in the 2009 report is the perception, which is arguably quite dominant in Europe, that co-regulation is more of an enhancing than a substantive tool.[810]

Finally, the report notes that the effectiveness of self or co-regulation is determined by numerous factors, including "transparency, accountability, the prevention of information asymmetry, aligning the interests of the self or co-

---

804 Paul de Hert, Gutwirth, Serge, Moscibroda, Anna, Fuster, Gloria Gonzalez, Wright, David, "Legal Safeguards for Privacy and Data Protection in Ambient Intelligence," *Personal and ubiquitous computing* 13, no. 6 (2009).

805 Robinson et al, "Review of the European Data Protection Directive: Technical Report Prepared for the Information Commissioner's Office.", p. 36

806 Kuner, *European Data Protection Law: Corporate Compliance and Regulation*., p. 220

807 Robinson et al, "Review of the European Data Protection Directive: Technical Report Prepared for the Information Commissioner's Office.", p. 29

808 Ibid., pp. 9-10

809 Ibid. The two European codes concern the International Air Transportation Association (IATA) and the Federation of European Direct and Interactive Marketing (FEDMA).

810 Ibid., pp. 9-10

regulatory institutions with those of the public, supervision, monitoring (by the government and stakeholders), and enforcement."[811] It has already been established that the goals of transparency and accountability are still to be attained. The next section will demonstrate that the top-down system of implementation, including monitoring, supervision and enforcement, is also not without weaknesses, one of which is the confused position of the DPAs.

b. Top-down implementation: overloaded DPAs

The complexity of the modern flow of data, and the resulting lack of transparency, makes top-down implementation - government monitoring and the enforcement of data protection rules - even more difficult than it used to be. Partially due to the Directive's opaqueness on the powers of the supervisory authorities (e.g. the ability to impose penalties), data protection law has been characterized as soft law, which is enforced by persuasion and dialogue.[812] The consequential differences between national approaches to data protection compliance[813] undermine the strength of the system overall. Even in the jurisdictions where the DPAs have the necessary powers, they "appear [to be] generally reluctant to punitively strike out at illegal activity with a 'big stick'. A variety of other means of remedying – most notably, dialogue and, if necessary, public disclosure via the mass media – seem to be preferred instead."[814] Bergkamp expresses the rather extreme view that even "in the past, business could survive under European privacy legislation only because enforcement was extremely lax and the government could grant ad-hoc privileges in any event. Even in member states that have had data protection laws on the books for more than a decade, the number of sanctions imposed for violations of the legal standards is very small."[815]

As well as formal difficulties in terms of the competence of the DPAs, there is another factor making the job of supervision and enforcement difficult; these tasks are only two of the many functions of the supervisory authorities according to the Directive. This has two important implications for the quality of enforcement of the data protection rules. Firstly, the limited resources of the DPAs appear to be required to cover not one but many tasks of equal importance when it comes to achieving the goals of the data protection rules. Even before cloud computing and chain informatisation, it is easy to imagine how the attention and resources of the DPAs were stretched to deal with a very wide range of functions, such as considering individual complaints, taking action, collaborating with the information industry in

---

811 Ibid.

812 Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits*., p. 79

813 Grant, "Data Protection 1998-2008.", p. 49

814 Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits*., p. 79

815 Lucas Bergkamp, "EU Data Protection Policy the Privacy Fallacy: Adverse Effects of Europe's Data Protection Policy in an Information-Driven Economy," *Computer Law & Security Report* 18, no. 1 (2002)., p. 37

drafting codes of conduct, and advising national governments. In the age of chain informatisation, cloud computing, and the advent of ambient intelligence, all of which mean that the number of controllers requiring supervision has exploded, it is unreasonable to expect the supervisory authorities, which already have limited time and resources available to them, to cope with the task of data protection enforcement better than before.

The second implication of the wide range of tasks entrusted to the DPAs is the consequential complexity of the role they have to play in the enforcement of data protection. More precisely, the exercise of powers to advise data processing actors on the one hand, and to control and monitor or punish them when there is a violation on the other, risks of a conflict of interests. Moreover, it may also undermine the openness of the data processing actors and their willingness to cooperate and expose their practices to an agency which can punish them later. For instance, the study conducted by the Brouwer Commission into the competence of the Dutch DPA, referred to surveys into the position of the information industry to conclude that such a combination of various roles limits the body's overall control of data processing practices.[816] The 2009 report to the Information Commissioner's Office concludes that, although "it is clear that enforcement is (and should not be) not the sole responsibility of the DPAs, […] this mixed role needs to be duly considered."[817]

Bergkamp, also a practicing lawyer, pessimistically concludes that "as a result, regulated entities do not have appropriate incentives to comply with the law."[818] Otter, meanwhile, observes that data protection is also at the bottom of the list of priorities for IT companies.[819] Moreover, the 2009 report agrees that "if errors are unlikely to have serious consequences, there is no incentive for data controllers to comply with data protection provisions."[820]

---

[816] J.E.J. Prins, "Burgers En Hun Privacy: Over Verhouding En Houding Tot Een Ongemakkelijke Bezit," in *16 Miljoen Bn'ers? Bescherming van Persoonsgegevens in Het Digitale Tijdperk* (NJCM, 2009)., p. 11. The Dutch DPA was quoted as disagreeing with the conclusion of the commission (Jaarverslag 2008, Den Haag 2009, p. 14, quoted in Prins, "Burgers En Hun Privacy: Over Verhouding En Houding Tot Een Ongemakkelijke Bezit.").

[817] Robinson et al, "Review of the European Data Protection Directive: Technical Report Prepared for the Information Commissioner's Office.", p. 36

[818] Bergkamp, "EU Data Protection Policy the Privacy Fallacy: Adverse Effects of Europe's Data Protection Policy in an Information-Driven Economy." The reader should also take into account that the position of Prof. Bergkamp could have well been shaped by his background as a practicing lawyer who was mostly exposed to the industry's side of the story.

[819] Thomas Otter, "Data Protection Law: The Cinderella of the Software Industry?," *Computer Law & Security Review* 23 (2007).

[820] Robinson et al, "Review of the European Data Protection Directive: Technical Report Prepared for the Information Commissioner's Office.", p. 35

2.3.3. Other challenges

The proper implementation of the data protection principles enshrined in the 1995 Directive is also under threat from a number of other factors which do not refer to the content of the principles themselves or to the system of implementation thereof. Some of these challenges will be mentioned briefly in this section. In the main, they relate to flaws in drafting techniques which enable there to be multiple possible interpretations of the rules, some of which undermine a principle they were meant to serve. Other concerns relate to the peculiarities of European law or the global nature of data processing.

One of the challenges stemming from the special nature of European law is the growing gap between data protection in the first pillar (internal market) and the third pillar (law enforcement and judicial co-operation). The 1995 Directive, which is adopted within the first pillar, is only applicable to the internal market while, as the 2009 report to the Information Commissioner's Office points out, "the consensus seemed to be that a common vision on data protection was needed across pillars."[821] The absence of uniformity in data protection across the pillars within the European Union is said to undermine the status of the data protection principles.[822]

This, and the global nature of data processing, often exposes data controllers to several conflicting legal requirements, whether within one national jurisdiction (e.g. conflicting obligations under the relevant data protection laws and requirements to retain data for law enforcement purposes) or across borders (e.g. the SWIFT case, demonstrating a clash between European law's data protection requirements and the obligation to disclose data under US law).[823]

Another challenge that the 2009 report mentions with regard to achieving the data protection goals is the growing internationalization of data processing. Since the data protection standards in other countries are not always as high as in the EU, the report calls for "the regulatory framework adopted by the Member States [to] offer effective and tangible protections at the non-European level as well."[824]

In cases where a third country has established a high level of data protection, the legal techniques employed in the Directive often form obstacles to the free flow of

---

[821] Ibid. p. 36, referring to European Data Protection Supervisor: Opinion of the European Data Protection Supervisor on the Final Report by the EU-US High Level Contact Group on information sharing and privacy and personal data protection, Brussels, November 2008; see http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2008/08-11-11_High_Level_Contact_Group_EN.pdf

[822] Ibid., p. 36, referring to the European Data Protection Supervisor: Opinion of the European Data Protection Supervisor on the Final Report by the EU-US High Level Contact Group on information sharing and privacy and personal data protection; Brussels, November 2008; see http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2008/08-11-11_High_Level_Contact_Group_EN.pdf

[823] Ibid., pp. 37-38

[824] Ibid., p. 20

data. As a general rule, the Directive only allows transfers to a third country if it ensures "an adequate level of protection".[825] However, data protection experts and practitioners regard the adequacy requirement as "highly restrictive and polarizing," and as an equivalence test and not an examination of adequacy.[826] This is because for a data protection system to be "adequate" it has to, in effect, adopt the Directive's approach. The fact that the adequacy test does not function effectively is affirmed by the fact that after 13 years, only six non-EU countries have been found to meet this requirement.[827]

Another example of how legal drafting techniques have weakened the implementation of the data protection principles is the openness of some terms, which thus require interpretation: e.g. adequacy, identifiability of an individual, etc. Another instance of an open formulation is the prohibition of the processing of data for purposes that are incompatible with the reason for which it was originally collected. What constitutes incompatible purposes is interpreted differently in national laws, providing an uneven level of protection across member states.[828]

3. Conclusion

The aim of this chapter was to analyze whether current data protection law in Europe has weaknesses which prevent it from dealing adequately with the data processing problem, leading to calls for improvement. It has been established herein that at the level of substantive principles, the European data protection regime hits all its targets. Firstly, unlike in the US, a harmonized legal framework of protection is

---

[825] Under Art. 26 of the Directive, the exceptions are possible in case:
"(a) the data subject has given his consent unambiguously to the proposed transfer; or
(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or
(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or
(d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or
(e) the transfer is necessary in order to protect the vital interests of the data subject; or
(f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case."
Member State may also authorize a transfer if the controller ensures adequate safeguards. Such safeguards may be in a for of standard contract clauses or BCRs (Art, 26 (2) of the Directive).
[826] Robinson et al, "Review of the European Data Protection Directive: Technical Report Prepared for the Information Commissioner's Office."
[827] Ibid., p. 31; those countries are Switzerland, Canada, Argentina, Guernsey, Jersey and the Isle of Man.
[828] Kuner, *European Data Protection Law: Corporate Compliance and Regulation*., p. 100

created across the member states. Secondly, this European framework is also praised for the normative choices it reflects, such as the principle of information self-determination. Although the implementation of this principle is not without its flaws, the notion of rejecting it as a foundation of the European approach to data processing is still regarded as being rather radical. Finally, the European data protection principles are intended to tackle most of the concerns which encompass the data protection problem. The quantitative and qualitative restrictions on data processing embodied in, for example, the principles of fair and lawful processing, data security and minimality, disclosure limitation, and information self-determination, maintain the secrecy of, or control over, private information, and contribute to the maintenance of an appropriate balance of power between the two sides to a personal data related transaction. The weaker position of an individual is also strengthened with information and other rights of the data subject, which are exercised directly or via supervisory authorities. Moreover, rules of fair data processing secure individual freedoms and autonomy.

However, it has also been demonstrated that concerns about the transparency of data processing and the accountability of the actors involved are not adequately addressed. Although the bases for tackling these issues are present, for instance in the form of the information rights assigned to the data subject, notification requirements, the obligations of the data controller, and compensation for damage caused, the ways in which the principles are implemented have a number of weaknesses. At the participatory implementation level, the accountability relationships model established in the 1995 Directive is not able to keep up with the realities of modern data processing. Instead, it places sole accountability for data protection violations on the data controller, whereas the reality of the present day is such that among the multiple actors involved in data processing, it is difficult to both identify a relevant actor and then classify him as a controller. As a result, it is often the case that no data processing actor can be held responsible.

The system of co-regulation and self-control also weakens the implementation of the substantive data protection principles. Despite some success stories and the hopes invested in codes of conduct and binding corporate rules, such as access to an industry's detailed knowledge of a particular sector and the capacity to more quickly keep up with new technologies, these tools are not very popular. Moreover, privacy advocates criticize the co-regulation tools for serving the self-interests of the industry rather than the data protection goals, while industry representatives blame the supervisory authorities for imposing too heavy a bureaucratic burden in the process of review and approval. The effectiveness of self or co-regulation is also undermined by other factors, among which are a lack of transparency, accountability and enforcement.

The top-down implementation of the substantive data protection principles is also limited by the lack of resources available to national supervisory authorities in

relation to their many tasks, as well as by the conflicting roles of the co-operating advisors on the one hand and the strict safeguards on the other. As a result, and also described as a major failure of the Directive's accountability system, the impression that some data protection commentators have is that the DPAs are unwilling or unable to enforce the data protection principles with a 'long stick'. Consequently, data protection law has the reputation of being 'soft.'

To conclude, the substantive principles and fundamental normative choices of data protection in Europe are satisfactory and, despite the required improvements to legal drafting techniques and implementation, do not yet need to be reconsidered. The position of this study is that, before altering the substantive principles and normative choices, particularly the principle of information self-determination, the question that needs to be asked concerns whether these principles are, in effect, being implemented. The main conclusion of this chapter is that the implementation mechanisms currently in place are not coping with the challenges of the modern data flow. In the spirit of the evolutionary approach to the analysis of data protection, one may say the fourth generation has failed, and the time is ripe to consider a reform the results of which could form the fifth generation.

Chapter 8: The possibility of propertisation of personal data in the EU legal order

1. Introduction

This chapter will explore the possibility of introducing propertisation of personal data in the EU legal order. In other words, whether it would allow a proprietary approach to data protection and, if yes, to what extent.

As has been explained in Chapter 4, the concept of property is fluid, and its meaning varies depending on the forum and context in which a particular debate is taking place. Accordingly, the possibility to introduce property rights in a new object such as personal data depends upon the meaning – or scope – attributed thereto. Since this book is a legal study, only the legal meaning of property in personal data will be examined here. This means that while the compatibility of such an approach with the European legal order will be considered, the discourse of the layman, economists and philosophers will not. What draws the focus of the analysis in particular is the double nature of property in law - as discussed in Chapter 4 - allowing property rights to perform both market and protective functions.

Having examined Part II of this book, the reader may recall that a significant aspect of the original US argument in favour of the propertisation of personal data is based on the 'state regulation versus market solution' dichotomy, with propertisation being a part of the latter.[829] The essence of the proposed market solution to the data protection problem is, in short, that it is fair and efficient for data subjects and data collectors (both of whom are autonomous parties to a personal data related transaction) to be able to contract freely about what can be done with the data in question: an individual (data subject) should be allowed to profit from waiving (part of) his control over his personal information; and a business (data processor or controller) should be able to pursue its economic goals effectively.[830] The introduction of such property rights is, according to the market approach, intended to enable such transactions.

However, it has been demonstrated that the 'market' element is not necessarily a feature in the modern European law of property. Indeed, there is much more to the nature and function of property rights than the facilitation of market exchange; these rights also ensure that there is a specific kind of protection of one's interests against the world, the most important being the retention by a holder of

[829] The other aspect of the private law solution is to leave the data protection problem to be dealt with within the framework of contract law.

[830] For a more detailed overview of the market argument for propertisation, see Chapter 5

major property rights of a degree of control over an object. Moreover, both market and non-market perspectives may embrace the possibility of the transfer of an object for remuneration. The difference lies in the degree of freedom the parties to the transfer have; the market approach treats this freedom as a priority, while the non-market outlook regards it as secondary in relation to the main function to provide protection to a certain interest. When applied to the transfer of personal data, this means that the market approach to propertisation favours the full alienation of property rights when personal data is transferred, whereas the protective standpoint only allows the limited alienation thereof, as determined by the individual's data protection rights, which are the main interests to be protected. Since the notion of property enables the parties to a transaction to have at least some negotiating freedom with regard to personal data, it is often, along with contractual tools, referred to as a private law solution. This study will, however, show that, although open to there being some private law elements in the approach taken to data protection, the European legal order would not allow the introduction of absolute property rights in personal data if these only adhere to the market freedom of the parties and account for no other interest than the market exchange.

Since the relevant elements of the European legal order are composed of the EU system of data protection and the law of the Council of Europe, the argument herein will be made in two stages, with the possibility and boundaries of propertisation under the two regimes being considered separately. The EU regime will be examined first, followed by an analysis of the law of the Council of Europe.

Before the analysis starts, however, another disclaimer has to be made. Although the focus of this chapter is on the formal possibility of propertisation, one aspect of it – the question of competence – will not be touched upon in this study. Although, indeed, whether or not the EU has a competence to introduce property rights in personal data would be of importance, such a discussion does not contribute much to the outcome of this study. Any possible objections against propertisation on the level of EU on the grounds of a lack of competence would only concern formal propertisation (i.e. when the term 'property' is used) and have no effect on the substance of the matter in case the property-like scope of rights is introduced but the use of the term 'property' is avoided. In the end, what matters for this study is that formal or de facto propertisation of personal data is possible, either on the EU or national level,[831] or by way of shared competence.[832]

---

[831] Regarding formal propertisation, either a member state, or the EC has the competence to formally introduce the propertisation of personal data. Despite the Article 295 EC prohibition on the regulation of the property ownership laws of the member states, an argument can be made that the EC competence in the area of data protection sanctions propertisation in this area to adjust its law to the recent changes in data processing. In addition, there is a large body of the literature on the so-called Europeanization of private law exploring how and arguing that property law may be adopted on the European level (e.g. Milo, "Property and Real Rights."; Daniela Caruso, "Private Law and Public Takes in European Integration: The Case of Property," European Law Journal 10, no. 6 (2004)., Van Erp,

2. Propertisation scenarios under Directive 95/46/EC

Hypothetically, it is possible to think of two types of propertisation (and a general private law solution to the data protection problem) in relation to Directive 95/46/EC; propertisation could be introduced either within the scope of the Directive's rules, in such a way that property rights are limited by data protection requirements, or by ensuring that the property rights exercised through contractual arrangements take precedence over the regime established by the Directive. So, setting aside issues of the EU competence in the field of propertisation, let us now take a look at how viable the two scenarios are from the standpoint of the Directive. Section 2.1 will examine whether there is anything in the Directive precluding the propertisation of personal data, while Section 2.2 will consider the question of whether the Directive provides room for propertisation and private law solutions as an alternative to its mandatory rules of data processing. In other words, does it permit property rights of a scope that derogate from its provisions?

2.1. The propertisation of personal data within the boundaries set by Directive 95/46/EC

This section asserts that, although the Directive does not mention property, neither does it preclude the introduction of property rights in personal data. Moreover, several of its provisions, which reflect the principle of individual control, move the Directive closer to the possibility of the introduction of limited propertisation when an individual is the holder of the widest possible property rights.

2.1.1. Absolute exclusion of propertisation contrary to the logic of the data protection evolution

It has been established earlier[833] that the flexibility of property rights permits almost any system of rights that provides a degree of control (i.e. including data protection) to be translated into the language of property. Indeed, there are only two ways to exclude the very possibility of the propertisation of personal data: to explicitly state that personal data shall not be regarded as property; and to eliminate individual rights of control, otherwise known as informational self-determination, in favour of

---

"European and National Property Law: Osmosis or Growing Antagonism?.", etc). Concerning the competence of the member states, provided that national property rights in personal data are not in conflict with the EC's data protection regime, the propertisation of personal information is achievable because property law is traditionally a matter for national legislation.

[832] Paul Craig, De Burca, Grainne, *EU Law: Text, Cases and Materials*, 4th ed. (Oxford University Press, 2008)., p. 89

[833] See Chapter 4

administrative rules of data processing. The former is of superficial significance, since it has been shown in Chapters 4 and 6 of this book that it is not the legal label but the content of the given rights that counts; formal prohibition to use property terminology would have no significance when it comes to the content of the actual rights and would not prevent them from taking the shape of property. The latter option, on the other hand, would indeed have attacked the very core of the possibility of propertisation, since, as seen in Chapter 4, property, which is flexible, is about rights of control with regard to a particular object; with these rights eliminated, the propertisation of personal data is impossible. Whether the switch from informational self-determination to administrative rules is a desirable option is, however, another matter. The position of this book is that it is not, because such a shift would be a backwards step in the evolution of the protection of data, of which the 1995 Directive is a genuine product. Moreover, it would also be in contradiction to the relevant fundamental choices made in Europe, to which the Directive also adheres.

As to the first point – the evolutionary development of the protection of data – the reader may recall an observation made by Mayer-Schönberger, referred to in Chapter 1, namely that data protection legislation worldwide has gone through the same sequential stages of development. The first generation was aimed at a small number of data banks, and employed no abstract rules or language of rights, whereas the second generation regime came to rely on the individual right of consent – a cornerstone of control. In turn, the third generation approach added some positive rights to its predecessor, while the fourth, albeit combined with regulation, still largely relies on these rights, *inter alia*, the right to consent. The 1995 Directive belongs to this fourth generation of data protection legislation, which is based on informational self-determination. As Chapter 1 explained, one of the reasons behind the progress from technical rules of data processing and no rights, to, primarily, rights backed up by regulation, relates to the fact that the system, with no individual rights or participation, was unable to cope with the data protection challenges faced as the number of databases and data processing actors grew. Accordingly, to move away from the rights approach now, when advances in information technology put every individual potentially in the position of a data processing actor,[834] would be counterproductive, since history has demonstrated the inability of pure regulation to cope with the growing information flow. Moreover, such a step would be inconsistent with the logic of the evolution of data protection. The earlier attempts to control data processing via regulation alone have failed, and the challenges that caused this failure, namely the expansion of data processing to include a greater number of actors and delve deeper into our lives, not only remain, but have also

[834] See Chapter 2, Section 4

advanced to a new level which demands an even more modern data protection system.[835]

2.1.2. The principle of individual control suggests propertisation

When it comes to the fundamental choices already made in Europe with regard to data protection, a model based solely on administrative regulation and relying on predetermined choices made by the legislature would be contrary to the principle of individual control – a common denominator in the bulk of the data protection laws in Europe,[836] the purpose of which is to enable an individual to have a degree of freedom to choose how to deal with his personal data. Moreover, the principle of individual control as expressed in a number of European data protection instruments suggests, but does not exclude, propertisation as a possible way of achieving data protection goals. The following analysis takes a closer look at this proposition.

Lee Bygrave explains the control principle as follows:

> *A core principle of data protection law is that persons should be able to participate in, and have a measure of influence over, the processing of data on them by other individuals or organizations.*[837]

Although the importance of the principle is a matter of a wide consensus,[838] data protection laws rarely contain it in a single provision or refer to it as a principle of control. Instead, it is manifest through abstract value concepts and "a combination of several categories of rules."[839] Laws of a constitutional nature, both national and international, which contain less detail,[840] utilize these abstract value concepts. The OECD Guidelines, for example, contain the 'Individual Participation Principle'

---

[835] See Chapter 2, Section 4

[836] Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits*. at 63; Solove, *Information Privacy Law*. at 872

[837] Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits*.

[838] Para. 27 Explanatory Memorandum to the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data available at < http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html#memorandum >

[839] Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits*. At 63

[840] This book maintains a functional approach to constitutionalism. Although historically constitutionalism emerged on a national level, many legal philosophers have observed that the phenomena of globalization and simultaneous fragmentation in the international legal order call for international constitutionalization; as a result, "recent years have witnessed intensification of constitutional discourse in many sites of transnational governance." (Jeffrey L. Dunoff, Trachtman, Joel P., "A Functional Approach to International Constitutionalization," in *Ruling the World? Constitutionalism, International Law, and Global Governance*, ed. Jeffrey L. Dunoff, Trachtman, Joel P. (Cambrigde University Press, 2009). at 3-7). E.g., De Hert and Gutwirth speak, *inter alia*, of the ECHR as a document of a constitutional nature (de Hert, "Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalization in Action.").

(paragraph 13),[841] although, as Bygrave points out, "rules giving effect to it embrace more than what is articulated in that particular paragraph."[842] German data protection laws likewise revolve around a wider principle of informational self-determination, which was developed in German constitutional jurisprudence,[843] "meaning the capacity of the individual to determine in principle the disclosure and use of his/her personal data."[844] Meanwhile, the privacy case-law of the European Court of Human Rights, although terminologically ambiguous,[845] does not yet grant protection to the right of self-determination, but does guarantee a right to personal development[846] and acknowledges the importance of the principle of individual autonomy, including in data protection cases.[847] For instance, in *Pretty v. United Kingdom* (2002), a general 'respect for private life' case, the Court ruled:

> *As the Court has had previous occasion to remark, the concept of 'private life' is a broad term not susceptible to exhaustive definition. It covers the physical and psychological integrity of a person (X. and Y. v. the Netherlands judgment of 26 March 1985, Series A No. 91, p. 11, § 22). It can sometimes embrace aspects of an individual's physical and social identity (Mikulic v. Croatia, No. 53176/99 [Part 1], judgment of 7 February 2002, § 53). Elements such as, for example, gender identification, name and sexual orientation and sexual life fall within the personal sphere protected by* Article *8 (see e.g., the B. v. France judgment of 25 March 1992, Series A No. 232-C, § 63; the Burghartz v. Switzerland judgment of 22 February 1994, Series A No. 280-B, § 24; the Dudgeon v. the United Kingdom judgment of 22 October 1991, Series A No. 45, § 41, and the Laskey, Jaggard and Brown v. the United Kingdom judgment of 19 February 1997, Reports 1997-1, § 36).* Article *8 also protects a right to personal development, and the right to establish and develop relationships with other human beings and the outside world (see, for example, Burghartz v. Switzerland, Commission's report, op. cit., § 47; Friedl v. Austria, Series A No. 305-B, Commission's report, § 45). Though no previous case has established as such any right to self-determination as being contained*

---

841 Para 13 of the OECD Guidelines reads as follows: "An individual should have the right:
a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended."

842 Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits*. at 63

843 See Poullet, "Data Protection Legislation: What Is at Stake for Our Society and Democracy?."

844 de Hert, "Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalization in Action." at 14

845 Ibid. at 15 fn 64

846 See ECHR *Christine Goodwin v. the United Kingdom* [GC], no. 28957/95, § 90, ECHR 2002-VI

847 de Hert, "Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalization in Action." At 15

> *in* Article *8 of the Convention, the Court considers that the notion of personal autonomy is an important principle underlying the interpretation of its guarantees.*[848]

In its 2008 personal data related judgment, *Reklos v. Greece*, the European Court held that the right to personal development, as protected in Article 8, includes the right to control the use of one's image, which is a vital element of one's personality.

> *A person's image constitutes one of the chief attributes of his or her personality, as it reveals the person's unique characteristics and distinguishes the person from his or her peers. The right to the protection of one's image is thus one of the essential components of personal development and presupposes the right to control the use of that image.*[849]

Although the *Reklos* ruling does not mean that Article 8 includes a general right of control over personal data other than one's image, it is nevertheless an important step towards the development of such a general right.[850]

Abstract value concepts are further articulated through several categories of more specific rules,[851] all of which give an individual control over what happens to his personal data. In this respect the European Court of Human Rights has recognized, *inter alia*, rights of access to personal files,[852] the right to demand the deletion of personal data from public files,[853] the claims of transsexuals to have their 'official sexual data corrected,'[854] and the consent requirement.[855/856]

---

[848] *Pretty v. UK*, para. 61

[849] *Reklos v. Greece*, para. 40

[850] Indeed, the reasoning of the Court, which brings control over one's image under the umbrella of the personality right, leaves room to interpret control over the use of other types of personal data under Article 8 protection. Firstly, one's image, according to the Court, constitutes only "*one of the chief attributes* of his or her personality" (para. 40, emphasis added), which means that there may be others. Moreover, the criterion of the inclusion of image into the range of essential elements of a personality is very inclusive, making the notion of personality open to broad interpretation; a piece of personal data constituting a part of one's personality under Article 8 protection "reveals the person's unique characteristics and distinguishes the person from his or her peers." (ibid.) Indeed, this could be said about nearly any type of personal data. For a discussion on personal data defined as an identifier see Leenes, "Do You Know Me? Decomposing Identifiability."

[851] Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits*. At 63

[852] ECtHR, *M.G v. the United Kingdom* judgment of 24 September 2002, no. 39393/98; ECtHR, *Gaskin v. the United Kingdom*, Application No. 10454/83, Judgment of 7 July1989; ECtHR, *Antony and Margaret McMichael v. United Kingdom*, Application No. 16424/90, Judgment of 24 February 1995; ECtHR, *Guerra v Italy*, Judgment of 19 February1998, Reports, 1998-I; ECtHR, *McGinley & Egan v. United Kingdom*, Application nos. 21825/93 and 23414/94, Judgment of 28 January 2000.

[853] ECtHR, *Leander v. Sweden*, Application No. 9248/81, Judgment of 26 March 1987; ECtHR, *Segerstedt-Wiberg and others v. Sweden*, Application No. 62332/00, Judgment of 6 June 2006.

[854] ECtHR, *Rees v UK*, Judgment of 25 October 1986 Series A, No. 106; ECtHR, *Cossey v UK*, Judgment of 27 September 1990, Series A, No. 184; ECtHR, *B v France*, Judgment of 25 March 1992 Series A, No. 232-C; ECtHR, *Christine Goodwin v. the United Kingdom*, Application No. 28957/95, Judgment of 11 July

The 1995 Directive sets out a more comprehensive system relating to the rules of individual control. In order to describe the system concisely, this section will rely on the classification provided by Bygrave.[857] There is first a requirement for a general transparency of data processing, which includes a controller's obligation to publicize his data processing activities by giving notification to a supervisory authority of the fact and basic details thereof (Article 18). This notification obligation is also combined with a requirement to make this information available in a public register (Article 21(2)).

The second group of relevant rules is aimed at making people aware of the processing of data pertaining to them. To achieve this, the 1995 Directive prohibits, where other legitimate grounds are absent, the processing of personal data without the consent of data subjects (Articles 7, 8(2)(a)). It also obliges data controllers to inform data subjects directly about the fact and basic details of the processing of information relating to them (Arts 10-11), whether or not these data subjects utilized a right of access thereto.[858] The right of access is enshrined in Article 12 of the 1995 Directive and enables a data subject to not only have access to data relating directly to him, but also "to information about the way in which the data are used, including the purposes of the processing, the recipients and sources of the data, and the 'logic involved in any automated processing of data concerning [the data subject] … at least in the case of the automated decisions referred to in Article 15(1)'."[859]

The third group of rules gives an individual a right to object to the processing of his personal data and demand that it be corrected or deleted if it is invalid, irrelevant, illegally retained, etc.[860] Since consent must be freely given, it can also be revoked at any time.[861] The right to object is a product of the ban on data processing without consent.[862] However, the Directive also specifies individual instances thereof, such as the Article 14(a) right to object to direct marketing and, "most innovatively,"[863] the Article 15(1) right to object to decisions "based solely on automated processing of data intended to evaluate certain personal aspects related to him [the data subject]." In addition, there is a right to demand that incomplete or inaccurate data, or data that is not processed in compliance with the Directive's requirements, be rectified, blocked or deleted (Article 12(b)).

2002.

855 ECtHR, *Malone v. The United Kingdom* judgment of 2 August 1984, Series A no. 82

856 For an overview of the ECHR jurisprudence on data protection see de Hert, "Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalization in Action."

857 Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits*. At 63-66

858 Ibid. at 64

859 Ibid. at 65

860 Ibid. at 65

861 Kuner, *European Data Protection Law: Corporate Compliance and Regulation*. at 212, para. 4.105

862 Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits*. at 65

863 Ibid. at 66

2.1.3. Consent requirement and exceptions thereto[864]

Compared to the other data protection instruments in force in Europe, the aforementioned right of consent appears to be prominent in the 1995 Directive,[865] which is a model illustration of the fourth generation of data protection laws. Indeed, the 1980 OECD Guidelines do not mention such a right at all, apart from paragraph 10, which narrowly applies the notion of consent as a precondition for the disclosure of data to third parties. Likewise, the texts of the Council of Europe 108 Convention and its Additional Protocol contain no consent requirement and ECHR jurisprudence on consent is limited. However, nothing establishes the relationship of control between an individual and personal data – characteristic of property – as strongly and unequivocally as the consent rule does and therefore makes the EC data protection system as susceptible to the property rhetoric. The analysis that follows reveals how the relationship of control is established via the consent requirement, and demonstrates that the criticism of and exceptions to the consent rule do not rule out propertisation as a model of data protection.

a. Consent as a method of control

Article 7 (a) and Article 8 (2)(a) of the Directive specify consent as a precondition for the processing of personal information, both generally and in terms of special categories of data. Accordingly, given the broad meaning attributed to processing, the consent requirement means that an individual is not only given control over whether the data pertaining to him can be disclosed or transferred, but also over how it can be used. The 1995 Directive defines consent as "any freely given specific and informed indication of his [data subject's] wishes by which the data subject signifies his agreement to personal data relating to him being processed" (Article 2(h)). Consequently, valid consent is a "clear and unambiguous indication of wishes," "freely given," "specific," and "informed."[866] The definition is, however, quite restrictive, and is aimed at ensuring that an individual exercises meaningful control over the fate of the data pertaining to him. In other words, it implies that the data subject must be "clearly informed in advance of what he is consenting to, and that any further processing of the data will be deemed not to have been consented to."[867]

---

[864] For more on the relationship between consent and other conditions of data processing see Chapter 10, Section 2.1.

[865] Naturally, with the exception of the national laws of the member states implementing the Directive.

[866] Article 29 Working Party, 'Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995' (WP 114, 25 November 2005) 10-12

[867] Kuner, *European Data Protection Law: Corporate Compliance and Regulation*., p. 67; moreover, the conclusion that the rights of a controller do not go beyond the scope granted by consent (unless the law envisages otherwise) is confirmation of the theory that property rights in personal data are formally recognized under the Directive and the individual and not the controller is a holder of the most significant rights.

The Directive is silent on whether the consent should be expressed by an affirmative act, such as ticking the 'I accept' box on an electronic form (so-called 'opt-in') or mere inaction, such as not clearing the 'I accept' box ('opt-out').[868] Christopher Kuner concludes that the absence in Article 7(a) of the requirement of 'explicit' consent (as opposed to Article 8(2)(a) on processing of sensitive data) "indicates that opt-in consent is not required as a general matter."[869] At the same time, the opt-out model seems to fall below the standard of protection set by the Directive, since the definition of consent in Article 2 requires the data subject to 'signify' his consent and "seems to imply that simple inaction is insufficient, and that some sort of [affirmative – N.P.] action is required to constitute 'consent'."[870] Put differently, the position of the Directive on 'opt-in' or 'opt-out' forms of consent supports the proposition that in EC data protection law an individual and not a controller is in charge of his personal data by default.

b. Criticisms of and exceptions to the consent rule

Despite the importance of consent in the Directive's data protection regime, the consent rule does have its limitations: firstly, it is criticized for a number of weaknesses, such as its unreliability in some sectors and the difficulty of managing it; secondly, consent is not the sole precondition for legitimate data processing. Nevertheless, this study maintains that the reservations raised about the consent requirement, although limiting the scope of potential property rights, do not exclude the possibility of propertisation completely.

When it comes to the issue of unreliability, Kuner points out that the data protection authorities advise against data processing solely on the grounds of consent in the field of electronic commerce, employment relationships,[871] and data transfers outside the European Union. In addition, many data protection authorities do not recognize consent given by a minor or a child.[872] The reasoning behind such a position is the associated risk of forced or ill-informed consent being obtained in such circumstances and the difficulties caused by the withdrawal thereof.[873] In the context of e-commerce there is an increased risk that a data subject did not fully understand, or did not read, the standard terms and conditions, which can be too long and

---

868 Ibid., p. 68-69

869 Ibid.

870 Ibid., p. 68-69 referring to W. Kotschy, 'Directive 95/46/EC' in Concise European IT law (The Hague, Kluwer Law International, 2006), p. 35; text in square brackets added.

871 "The Article 29 Working group has taken the view that where as a necessary and unavoidable consequence of the employment relationship an employer has to process personal data, it is misleading if it seeks to legitimize this processing through consent. Reliance on consent should be confined to cases where the worker has a genuine free choice and is subsequently able to withdraw the consent without detriment." (Art 29 Working Party, 'Opinion 8/2001 on the processing of personal data in the employment context' (WP 48, 13 September 2001) 3)

872 Kuner, *European Data Protection Law: Corporate Compliance and Regulation*., p. 211

873 Ibid., p. 68

unclear. In some jurisdictions the application of the consent rule in e-commerce is even more limited by the requirement for written consent, i.e. on paper.[874] Many data protection authorities also rightly see employment relationships as being inherently dependent, meaning that employees cannot meaningfully provide consent.[875] Accordingly, the data protection authorities advise against reliance on consent as the sole legal basis for data processing, except where "it is absolutely necessary."[876] Finally, consent under Article 26(1)(a) (transfer to a country without an adequate level of protection) can rarely be unambiguous and fully informed since, *inter alia*, due to the language barrier and a poor knowledge of data practices and enforcement mechanisms in the jurisdiction in question, the data subject can hardly be expected to possess the knowhow to calculate either the potential risks related to the transfer of his data outside the European Union or, often, the irreversibility of a decision to give such consent. Consequently, in the long run, the Article 29 Working Party does not expect the consent requirement to continue to be the legal basis of such data transfers.[877]

As well as the limitations referred to, the application of the consent rule is restricted by the exceptions thereto, i.e. the other grounds for legitimate data processing listed in Article 7 (b) – (f), Article 8(2) (b) – (e), and, by way of derogation from Article 25, the alternatives to consent under Article 26. Indeed, given the present state of the law, even when the ability to make an informed and independent decision is not compromised, the individual does not have full control over his personal data and may not indiscriminately allow or disallow any processing thereof by giving or withdrawing his consent. According to some commentators, the consent

---

[874] Ibid., pp. 68-69 ("Some member state laws also restrict the possibility to give consent electronically. For instance, under the German Federal Data protection Act, consent to the processing of personal data must be given 'in writing', meaning pen on paper, unless consent is to be given in the course of using 'teleservices' under the Teleservices Data protection Act, in which case consent may be given electronically under certain conditions.")

[875] Art 29 Working Party, 'Opinion 8/2001 on the processing of personal data in the employment context' (WP 48, 13 September 2001) 3, stating '[t]he Article 29 Working group has taken the view that where as a necessary and unavoidable consequence of the employment relationship an employer has to process personal data it is misleading if it seeks to legitimize this processing through consent. Reliance on consent should be confined to cases where the worker has a genuine free choice and is subsequently able to withdraw the consent without detriment' (cited in Ibid., pp. 211-212). See also *Nikon v. Onof*, decision No. 4164 (2 October 2001), in which the French Cour de Cassation did not allow the reading of an employee's email messages, even with the employee's consent (cited in ———, *European Data Protection Law: Corporate Compliance and Regulation*., p. 212, fn 214)

[876] Kuner, *European Data Protection Law: Corporate Compliance and Regulation*. (e.g. WO, 'Working document of the surveillance of electronic communications in the workplace' (WP 55, 29 May 2002) 21)

[877] Working Document: Article 26(1),' 11 reads: "the Working Party suggests that consent is unlikely to provide an adequate long-term framework for data controllers in cases of repeated or even structural transfers for the processing in question."

requirement has no normative priority[878] and is but one of a number of equal alternative preconditions for data processing. As Bygrave observes with regard to Article 7, "most instances of processing will be able to be justified under the criteria in paras (b)-(f) of the provision."[879]

In other words, the current data protection regime reflects the position that relying on consent as the sole ground for data processing may be detrimental to individual data protection interests when the data subject is forced to make, or is incapable of making, an informed decision about his agreement to the processing of his data. Likewise, making other parties who are acting in good faith hostages to an individual's will is unfair and contrary to other legitimate public and private interests. The Directive limits the application of the consent requirement accordingly. However, these limitations of the consent rule are not specific to data protection legislation, also being common in private law, meaning that the option of propertisation cannot be ruled out.

When it comes to the unreliability of the consent rule, it is quite common in private law for minors, mentally disabled, or people otherwise unable to make informed, free decisions, to have their civil capacity to provide consent restricted in order to secure their interests. This includes the matters of the ownership or alienation of property.[880] It is also a common tradition in private law to both hold that transactions are invalid where the independence of one (usually, the weaker) party was compromised, and correct such shortcomings of individual autonomy by regulation. For instance, this is how consumer protection law came into existence.[881]

As to the exceptions to the consent rule, limitations on an individual's absolute power over an object are likewise not alien to the law of property. Just as, for example, property rights in land under English law can be limited by law or contract,[882] so can an individual's autonomy with regard to his personal data. Alternative conditions for data processing, under Articles 7, 8 and 26, state that an

---

878 Bygrave, "Consent, Proportionality and Collective Power.", p. 165-166. See, however, ———, "Consent, Proportionality and Collective Power." "However, in a small number of jurisdictions, the consent requirement has been given priority over the other preconditions such that a data controller must ordinarily obtain the data subject's consent to the processing unless this would be impracticable. [fn 18: the case, e.g., in Estonia and, to a lesser extent, Belgium and Greece. […] In Belgium, consent is given priority only with respect to processing of sensitive personal data.] It is doubtful that the Directive, as originally conceived, mandates such prioritization. However, the Directive does not disallow it." Bygrave further argues that ECtHR jurisprudence may develop to push data protection towards prioritising consent.

879 Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits*., p. 66

880 e.g. Articles 3:32 paragraph 2 and 1:234 and 1:381 of the Dutch Civil Code

881 see Clarrisse Girot, "The Development of the Protection of Weak Parties in Comparative Law," in *User Protection in IT Contracts* (2000).

882 See e.g. Cooke, *Land Law*.

individual's consent is un-necessary when the performance of a contract requires the processing of data, or when such processing is required by law.[883]

2.1.4. The holder of property rights

The principle of individual control that is expressed, *inter alia*, in individual rules of consent, the right of access to data, the right to require that data be corrected or destroyed, and the right to object to its use, also permit the stipulation that if property rights become an actual framework of data protection, it is the data subject who shall be the holder of the major rights regarding the information pertaining to him. Indeed, although the Directive does not exclude the possibility of a controller (or any other data processing actor) holding property rights in personal data, it does strive to preserve an individual's control over a piece of information throughout the entire course of data processing, regardless of whom the actor determining the goals and means of the processing in question is. Looking back at the developments in the modern law of property described in Chapter 4, fragmented ownership, which is an innovative aspect of both some national legal systems using a continental model and the EU legal order itself, one may legitimately conclude that the Directive allows both data subjects and controllers to be holders of property rights over the same piece of personal data at the same time. However, it is the individual and not the controller who is the holder of the major rights. This is because the scope of the rights of the latter is always limited by the individual's consent, or exceptions created by the legislator (e.g. in determining the purpose for which the data in question can be used), and is always subject to control, either directly by the data subject or via a supervisory authority. When regarding the Directive as a declaration of normative choices in the field of data protection, regardless of how the document functions in reality,[884] one cannot help but observe the preferred distribution of entitlements between data subjects and controllers: the entitlement of the former regarding

---

883 Although the text here does not list individual legitimate grounds of processing under respective articles, those grounds are not erroneously omitted but are implied. Namely, 'required by law or contract' here does not refer to an individual ground of processing but covers all other legitimate grounds of processing under Arts 7, 8, and 26 which were already mentioned earlier in this study. Naming each individual ground again is, in the author's opinion, an unnecessary repetition. Indeed, the point the author aspires to make is that personal data is processed lawfully in two broadly defined instances: first, when the data subject gave its concent, or, second, when the authorisation to process came from an authority other than the data subject (in case when processing is necessary to fulfil a contract to which the data subject is a party, one may argue that the authorisation came from the data subject indirectly). The latter category is referred to as 'required by law or contract' and includes processing in the name of a vital interest of the data subject or an important public interest, and other grounds. For a detailed analysis of the grounds of data processing see Kuner, *European Data Protection Law: Corporate Compliance and Regulation*., p. 76 and on.

884 Indeed, in reality the controllers and not the data subjects are the ones who often have absolute control over personal data, and the individuals exercising control are more an exception than a rule (for more a detailed explanation of this point see Chapter 2).

personal data is a default rule but is limited by means of a closed list of exemptions to the consent rule contained in Article 7. On the other hand, the rights of the controller are, by default, non-existent and created as an exception, whether by the individual's consent or by law. According to Kuner, it is "one of the fundamental principles of the General Directive […] that personal data may only be processed if one of a list of enumerated legal bases is present."[885] The rights of the controller cannot be greater than those granted to him.[886]

In conclusion, the European approach to data protection in general, and as expressed in the 1995 Directive in particular, is quite liberal. This means that it does not completely rely on the choices predetermined for a data subject by a regulator when it comes to the data processing permitted, but also significantly relies on the individual's freedom to choose for himself. Although this freedom is not absolute and is subject to exceptions, the current data protection model cannot be said to preclude the propertisation of personal data altogether. Moreover, the liberal language of the Directive, including in the consent requirement, suggests that propertisation is one possible approach to data protection and regards the data subject as the holder of the significant property rights.

2.2. *Propertisation of personal data as an alternative to Directive 95/46/EC*

Directive 95/46/EC does not preclude personal data from being treated as property. Moreover, as the previous section established, it even suggests a property approach to data protection. It is, however, a different question altogether when considering whether such an approach can deviate from the Directive's provisions. The subsequent paragraphs contain arguments suggesting that it cannot.

It is maintained that the assumption made about the mandatory nature of the Directive's provisions is correct, with there being no room for contractual deviations. Consequently, the Directive does not permit property rights to be created beyond the established data protection regime.

An argument to the contrary may not only be derived from a presumption that the Directive does not require national implementing provisions to govern all cases where personal data are processed, but also from the fact that the Directive's regime must instead be adhered to only when there is no contract governing data processing, or when the contract does not deal with this issue. On this basis Cuijpers concludes that it is possible to 'contract around' the EC data protection regime.[887] This view is significant for the European propertisation debate because if correct, and

---

[885] Kuner, *European Data Protection Law: Corporate Compliance and Regulation*., p. 75, para. 2.34

[886] E.g. see further discussion on consent, in particular, stating that "any further processing of the data will be deemed not to have been consented to" (Ibid., p. 67); also, discussion of the restrictive interpretation of other grounds for legitimate data processing.

[887] Cuijpers, "A Private Law Approach to Privacy: Mandatory Law Obliged? .", p. 306

if property rights in personal data are introduced, they will take precedence over the limitations imposed by the Directive. Cuijpers' conclusion relies on a number of factors, and these will now be considered to the extent that they are related to the Directive. After subjecting these arguments to a critical review, the conclusion will be that only a misinterpretation of the law can justify a claim that the Directive is non-mandatory in nature.

2.2.1. The internal market as a free market?

The first argument concerns the EC's capacity to adopt the Directive, and will draw the reader's attention to two of the latter's goals (or, as Cuijpers describes them, pillars): the protection of individuals with regard to the processing of personal data; and the free movement of such information.[888] With an important disclaimer that the European Community is bound by a requirement to protect the human rights of its citizens,[889] Cuijpers asserts that since the Directive was adopted on the basis of Article 95 EC (formerly Art. 100a)[890] to promote the internal market, it cannot be interpreted as limiting free transactions between private parties. The application of the Directive should favour contractual arrangements and can therefore only be binding where there are no such agreements in place.[891]

The main disagreement between the position of this book and the 'free-market argument' lies in our understanding of the "internal market".[892] The way in which Cuijpers makes her case[893] leads to a conclusion that she equates the "internal market" referred to in Article 95 to a free market. Yet such a stance is erroneous. It contradicts the traditional understanding of the internal or single market as one of the basic legal elements of EC law, which is comprised of the four freedoms and not a laissez-faire doctrine, with a heavier emphasis on the 'common' rather than on the 'market'. Steiner and Woods explain the meaning of internal market in terms of the activities that must be undertaken under the Treaty of the European Union (TEU); Article 3(1)(a) calls for the prohibition of customs duties; Article 3(1)(b) lays the groundwork for common commercial policies; Article 3(1)(g) envisages that the Community shall ensure competition in the internal market; and Article 3(1)(h) calls

---

888 Ibid., p. 307

889 Ibid., p. 308

890 The analysis of the argument of Cuijpers uses the numbers of articles as they are used in Ibid. and does not take into account the changes introduced thereto by the Lisbon Treaty.

891 Ibid., p. 308

892 Article 95 EC reads: "/…/ The Council shall /…/ adopt the measures for the approximation of the provisions laid down by law, regulation or administrative action in Member States which have as their object the establishment and functioning of the internal market. "

893 E.g. "After all, the processing of personal data on the basis of contractual agreement will by no means hamper the free movement of such data and therefore will certainly not come into conflict with the basis of the directive." Cuijpers, "A Private Law Approach to Privacy: Mandatory Law Obliged? .", p. 308

for an "approximation of laws of the Member States to the extent required for the functioning of the common market."[894] The Single European Act (SEA) introduced the term 'internal market' and defined it as "an area without internal frontiers in which the free movement of goods, persons, services, and capital is ensured in accordance with the provisions of the Treaty" (Article 14 (ex 7a)).[895]

Naturally, when the European market has reached maturity, market efficiency also becomes important.[896] During its Lisbon meeting on March 23-24, 2000, the European Council adopted a strategy aimed at making the EU the world's most competitive economy.[897] However, the efficiency goal does not imply that the EU should relinquish regulation. On the contrary, as the theory of trade-orientated competition law teaches, markets fail, with tailored regulations addressing these failures and enhancing efficiency.[898]

The fact that the objective of the European Community has been to build a common market does not necessarily mean that it relies on the laissez-faire doctrine. Indeed, EC laws on the internal market contain limits on trade provided that they are not aimed at discriminating against goods and services from other member states and apply equally to domestic and foreign traders. What is more, in the cases concerning the application of the Directive itself, the ECJ explained that the Directive's objective was "approximating the laws, regulations and administrative provisions of the Member States in order to eliminate obstacles to the functioning of the internal market deriving precisely from disparities between national legislation."[899] Accordingly, and in opposition to Cuijpers' assertion, deviation from the provisions of Directive 46/95/EC would be contrary to the purpose thereof. The overall conclusion is that Cuijpers' comprehension of the "internal market" as a free market is contrary to the established understanding thereof. Similarly, the free movement of data does not mean that data flows must be free of state regulation. Understanding the internal market as a place with no obstacles to trade between member states, but not to trade in general, does not provide the basis upon which to interpret 1995 Directive's rules, which were adopted following Article 95 EC, as being secondary to contractual arrangements.

---

894 Josephine Steiner, Woods, Lorna, *EU Law* (Oxford, New York: Oxford University Press, 2009)., p. 345

895 Although two different terms – common and internal market – are used, and some argue that the meaning of the 'internal market' is broader, the European Court of Justice does not distinguish between them, and "when the Lisbon Treaty comes into force" (as it actually did in December 2009), the difference between the terms will probably continue to be blurred. (Ibid., p. 345)

896 Alina Kaczorowska, *European Union Law* (London and New York: Routledge-Cavendish, 2009)., p. 479

897 Ibid.

898 Martic Taylor, *International Competition Law. A New Dimension for the WTO?* (Cambridge: Cambridge University Press, 2006)., p. 29

899 Case C-101/01 (*Lindqvist*), para. 41

2.2.2. A window in the Directive: no mandatory law clause?

Cuijpers' second argument in favour of the possibility of the private-law solution by-passing the rules of Directive 95/46/EC is that the Directive itself has room for an alternative solution. She makes several points to support her claim, and although she acknowledges that the Directive "is so exhaustive that almost every provision is directed towards complete harmonisation,"[900] she maintains that it is only binding on member states and not on private parties. Nothing prevents data controllers and data subjects from contracting around laws implementing the Directive if a member state chooses to leave such an option open.[901] This would not be the case, Cuijpers continues, if the Directive contained a clause "requiring the mandatory character of one or more of its provisions,"[902] and forbidding private parties from entering into contracts deviating from the Directives' rules as, for example, is common for consumer protection legislation. However, the 1995 Data Protection Directive has no such a clause, and does not, therefore, have to be implemented in the form of a "mandatory law" as described by Cuijpers.[903]

Cuijpers makes two additional points to support her argument: firstly, that Article 7 of Directive 95/46/EC allows the processing of personal data on the basis of consent provided by the data subject and, therefore, on the basis of a contract;[904] secondly, Article 27 of the Directive encourages self-regulation in data protection.[905] Both of the points made by Cuijpers here are valid. However, neither of them, whether taken together or separately, means that the Directive allows private parties to deviate from its regime. Instead, they demonstrate that when implementing the Directive's provisions, member states may also leave room for contracts to be made in the field of data processing, but only within the framework of the Directive.

As for the two secondary arguments, this chapter has already addressed the limited applicability of the consent rule. Indeed, a well-established view in the field of data protection is that the consent requirement, although important in itself and essential for the possibility of introducing the propertisation of personal data: is only one of several equally important bases of lawful data processing; is limited; and cannot override the Directive's remaining requirements. In any case, the position of

---

900 Cuijpers, "A Private Law Approach to Privacy: Mandatory Law Obliged? ."

901 "Even though governments cannot implement rules that deviate from the provisions laid down in the directive, this does not mean that data controllers and data subjects cannot deviate from the implemented rules", Ibid., p. 310

902 Ibid., p. 310

903 Ibid., p. 311

904 "The second remark concerns article 7 of Directive 95/46/EC. This article explicitly leaves room to process personal data on a contractual basis, or with the consent of the data subject." Ibid., p. 311

905 "Moreover, the Directive expressly states the advantages of self-regulation. The possibility for data controllers and data subjects to draw up data protection regulations according to the needs of a specific legal relationship must be seen as an advantage that should not be limited by mandatory rules of law." Ibid., p. 311

this study is that the consent rule alone is not enough to open a window to contractual deviations from the Directive's rules. Furthermore, the self-regulation argument is, in essence, not very different to the main claim that private parties are allowed to deviate from the Directive's regime, with the criticism of this key point being completely valid. As a consequence, the self-regulation claim will not be addressed separately herein.

When it comes to the main argument, it is indeed true that the Directive cannot, by its very nature, impose obligations on private parties directly.[906] However, "as an instrument of Community intervention,"[907] it does impose an obligation on member states to fully implement its provisions. As Sacha Prechal explains,

> *[Although] this obligation exists primarily vis-à-vis the Community and other Member States, […] from their entry into force directives form part of the law in the member States and thus constitute a source of law within the national legal system.*[908]

As a result, although the 1995 Directive is not directly binding on private entities, these parties are not immune to the substance of its data protection requirements. Prechal aptly points out that in their effect the Directives go beyond providing governments with guidelines. Instead, they are often aimed at creating "a whole conglomerate of rights and obligations [not only] between Community institutions and Member States, Member States inter se, Member States and individuals, [but also between] individuals amongst themselves."[909] Thus, the 1995 Directive aims to create an entire regime of data protection rights and obligations. From the text of such a directive – regardless of implementation – it is clear who "will be obliged or entitled at the end of the day, i.e. once the directive has been transposed."[910] As Prechal puts it:

> *[T]he substantive provisions may formulate both the persons who will be beneficiaries and the persons who will be under obligation after the transposition into national law of the directive at issue. The fact that the directive as a whole is binding upon the Member State only, is in this respect immaterial. […] In other words, it reaches the individuals through implementing measures adopted by the Member States.*[911]

---

[906] Prechal, *Directives in EC Law* at 92-96 (e.g. "As a rule, implementation of the directive requires its transposition into national law." ———, *Directives in EC Law* at 92)
[907] Prechal, *Directives in EC Law* , p. 92
[908] Ibid.
[909] Ibid.
[910] Ibid., p. 95
[911] Ibid.

The 1995 Directive provides for the rights of data subjects and imposes obligations on data controllers. There is, therefore, no doubt that it applies to private parties, albeit through state action. Moreover, if a member state permits a type of private data processing that is not in compliance with the Directive's requirements, e.g. by improper enforcement or upholding faulty contracts[912] in its courts, it can be found to be in violation of its obligations of full implementation under Article 249 (3). Such a possibility stems from the position of the Court of Justice and the Commission which, when evaluating a member state's compliance, no longer focus solely on the conformity of the national implementation measures, but also on the non-application of the directives that have been accurately transposed.[913]

2.2.3. Freedom of contract

The third argument in favour of a private law solution to the data processing problem relies on an understanding that data protection rights, with their roots in but nevertheless being distinct from a fundamental right to privacy, only overlap when data processing amounts to intrusion in an individual's "private sphere".[914] For some this means that excluding the private law solution, and sticking with the mandatory rules of the Directive, strikes an unfair balance between data protection interests, which are less than a fundamental right, and the freedom of contract, which is another interest that is key to the European Community.[915] For instance, Cuijpers writes:

> *Without this qualification, the edge is taken off the main argument regarding [the] implementation of Directive 95/46/EC into mandatory rules of law. Even if the right is considered to be rooted in a fundamental right, there is still no solid argument to hierarchically place data protection above the principle of freedom of contract, leaving room for implementation of Directive 95/46/EC into rules of regulatory nature.*[916]

---

912 By 'faulty contracts' I mean contracts where data subjects waive their data protection rights and data controllers release themselves from their data protection obligations, thereby 'contracting around' the Directive's requirements.

913 For a more detailed explanation of this point see Prechal, *Directives in EC Law* , p. 51-54.

914 "I agree with Blok that data protection and privacy are not the same. [...] As the protection of the individual with regard to the processing of personal data is in no way restricted to data concerning the private sphere of the individual, Blok comes to the conclusion that the choice to link data protection to the right to privacy is unjustly made." Cuijpers, "A Private Law Approach to Privacy: Mandatory Law Obliged? .", p. 312

915 Ibid., p. 313

916 Ibid., p. 314

This study took a different view.[917] Firstly, regardless of whether or nor data protection forms an element of the right to privacy, it has received its own recognition as a fundamental constitutional right both on the EU and national level. The article of Cuijpers was written before the relevant EU reforms took place. Therefore, this argument will not be invoked as a criticism.[918]

Second, the development of the fundamental right to privacy as defined in the case-law of the European Court of Human Rights has taken steps along the path of protecting data protection interests.[919]

Thirdly, and regardless of the formal relationship identified between privacy and data protection in the ECHR, an analysis of European law is sufficient to lead to the rejection of the notion of the invincibility of freedom of contract in its interaction with data protection interests. This point will be advanced further in this section.

A clash between the freedom of contract and other protected interests is not new in EU law discourse. Resolving the clash is, however, now even more important given the fact that the Court of Justice recognized the freedom of contract as being a European fundamental right.[920] However, despite the ECJ's ruling, giving priority to the freedom of contract would be erroneous. This view is supported by Cherednychenko's study of ECJ jurisprudence in the area of the clash of so-called EU fundamental rights on the one hand and EC freedoms on the other.[921]

Cherednychenko's study defines EC freedoms as the four freedoms which constitute the main principles of EC primary law. As she observes, they have "strong similarities with the position of constitutional rights as contained in national constitutions."[922] However, EU fundamental rights are the rights adopted from the common constitutional traditions of member states and international human rights treaties. In particular, through the ECJ's case law, the European Convention on

---

[917] To be fair to the position expressed by Cuijpers, and contrary to her earlier statement on the application of the Directive, in statements made later on, she argues more in favour of its implementation into the "rules of regulatory nature." For contradicting statements see: "By this I mean that it is assumed that the directive does not leave room for contractual deviation of the rules laid down in it. In this article I would like to question this assumption." Ibid., p. 306 and "An act of law establishing a certain kind of waiver of the rights implemented according to this directive can therefore be valid." ———, "A Private Law Approach to Privacy: Mandatory Law Obliged? .", p. 315 This study agrees with the last statement concerning the implementation of the Directive into regulatory rules. However, this correct statement made in the context of her analysis does not so much strengthen the argument as make it inconsistent, as if the author made no distinction between the private law solution complying with the Directive's requirements on the one hand and a regime that is a complete alternative to the Directive on the other.

[918] But see discussion on 'constitutionalisation' of data protection in Chapter 9, section 2.

[919] Chapter 9, Section 3.

[920] See, for example, cases C-90 and C-91/90, [1991] ECR I-3617, at para. 13 (free choice of contractual partners).

[921] Olha Cherednychenko, "EU Fundamental Rights, EC Fundamental Freedoms and Private Law," *European Review of Private Law* 1 (2006).

[922] Ibid., p. 25

Human Rights first formed a kind of unwritten bill of rights and later received recognition in the amended EU and EC Treaties.[923] Interestingly, although the ECJ does not explicitly recognize the conflict between these two groups of interests, it does not acknowledge the absolute precedence of one interest over the other.[924] Cherednychenko and Basedow interpret this position as suggesting that the conflict should be resolved by balancing rather than looking for a 'more important' right.[925,926]

Similarly, in case of data protection, freedom of contract cannot be treated as absolute but should be balanced. To apply the balancing to the case of the 1995 Directive and the argument of the precedence of freedom of contract over data protection rights, the first step is to classify the two conflicting values as the EU fundamental rights or fundamental freedoms. At this point it must be noted that the system of fundamental rights and freedoms in the EU, although without doubt closely related to the ECHR system, is different; the content of EU rights and freedoms reflects the economic roots of the Union. It has been mentioned earlier that the freedom of contract has been recognized as an EU fundamental right. The data protection rules, however, also form a part of the system of EC freedoms. As the preamble to the Directive highlights, they act as instruments to foster the free movement of information between member states and, as such, cannot be overridden by the freedom of contract. On the contrary, the two conflicting values should be balanced against each other. The *Lindqvist* judgement is important here since it also suggests the balancing of data protection interests against other values, like free speech. Moreover, according to *Lindqvist*, the Directive itself, along with national laws adopted in its implementation, provides for a necessary balance.

> *The mechanisms allowing those different rights and interests to be balanced are contained, first, in Directive 95/46 itself, in that it provides for rules which determine in what circumstances and to what extent the processing of personal data is lawful and what safeguards must be provided for. Second, they result from the adoption, by the Member States, of national provisions implementing that directive and their application by the national authorities.*[927]

Nothing suggests that the freedom of contract should take precedence over data protection interests. Instead, a fair balance between data protection and other interests, including the freedom of contract, must be achieved. Indeed, by regulating

---

[923] Ibid.
[924] Ibid., pp. 35-39
[925] Ibid., p.36
[926] Jürgen Basedow, "Freedom of Contract in the European Union," *European Review of Private Law* 16 (2008).
[927] *Lindqvist*, para. 82

the processing of personal data, the Directive has already laid the groundwork for such a balancing act to take place.

2.2.4. Power to negotiate

As well as the arguments already discussed, some assert that the Directive's mandatory prescriptions limit the data subject's ability to negotiate and obtain greater economic gain in return for the personal information revealed. Some consider this to be enough to call for the opportunity to contract around the Directive's data protection regime. The position of this study, however, is that the calls for propertisation based on this argument are more an example of wishful thinking than a correct reflection of the law; the fact that the Directive does indeed take some data protection issues off the agenda for negotiation means that while some actors may wish that the situation was different, it is not. The previous sections of this chapter have already revealed how the Directive's regime limits the freedom of contract and the ability to process personal data on the grounds of consent. By proxy these arguments imply that the mandatory rules of the Directive are off the negotiating table. It is not, therefore, necessary to return to this discussion in the current section. Instead, an argument will be made that the limits on the powers of negotiation under the Directive are justified from the perspective of defending a data subject as a weaker party.

Few scholars maintain the position that the current regime should be changed to provide greater room for negotiation. Cuijpers argues:

> *[A]lthough mandatory rules of law protect the immaterial right to privacy, they diminish the possibilities for data subjects to negotiate terms and conditions under which, in return for economic gain, they can consent to the processing of their personal data.*[928]

Berkvens' criticism of the current regime relates to the fact that data protection rules are in the hands of the "privacy regulators [… who] do not represent political or commercial interests but instead champion a single fundamental right. […T]here is little scope for traditional negotiation based on economic interests."[929] As a result, "the consumer can no longer set priorities. He has been excluded from any discussion of privacy issues."[930]

It is hard to dispute the fact that the imposition of any mandatory rules of law limits both the scope of rights and the contractual freedom of the participants to a

---

[928] Cuijpers, "A Private Law Approach to Privacy: Mandatory Law Obliged? .", p. 315
[929] Jan Berkvens, "Role of Trade Associations: Data Protection as a Negotiable Issue," in *Reinventing Data Protection?*, ed. Serge Gutwirth (Brussels: Springer, 2009)., p. 125
[930] Ibid., p. 128

transaction. Nevertheless, it would be wrong to assert that the limitations imposed on negotiations by Directive 95/46/EC are unreasonable. The analysis should depart from a presumption that in data processing transactions an individual is almost always a weaker party who is unable to protect his interests without state intervention. The vulnerability of the data subject stems from both the widely acknowledged inequality of resources of the individual and an organization,[931] and from the fact that at present most of the interactions between these two parties involve information technology, where the organization has the benefit of professional expertise and the individual is but a layman.[932] The position of the data subject may also be negatively affected in the special cases of employment relationships, international data transfers, etc.[933] Regulation is a logical way to respond to these challenges and correct the imbalance of powers by making principal matters non-negotiable.

Whether the limitation on negotiating powers is proportionate has already been addressed in the section on the freedom of contract. The freedom to negotiate and conclude contracts cannot, however, dominate the field of data protection; the rules of the 1995 Directive embody a political decision to strike a balance between the two values in a particular way. A change of this established balance should be a matter of a political discourse and not legal argument.

Furthermore, the way in which the Directive balances the possibility of negotiation and data protection interests not only preserves the latter, but also secures the former. As revealed earlier, the consent rule in Article 7 of the Directive makes it clear that the data protection regime does leave room for data subjects and data controllers to conclude contracts.[934] However, before giving the required consent to his data being processed, a data subject must be informed about the purpose thereof if he is to make an informed decision about whether permitting it is worth the potential economic benefit of, for example, agreeing a contract (e.g. a user agreement), or otherwise agreeing to the collection and use of his personal information. It is here that being able to negotiate about economic benefits is possible.

---

931 This point is often made in the field of economics and the economic analysis of law. See, for instance, Murphy, "Property Rights in Personal Information: An Economic Defence of Privacy." Including references, etc.

932 On the vulnerability of individuals in IT contracts see Girot, "The Development of the Protection of Weak Parties in Comparative Law."

933 Employment relationships are often dependent relationships, which often exclude the possibility of meaningful negotiations on the part of an employee. International data transfers weaken the position of the data subject due to the language barrier, unfamiliarity with the system of the protection of rights in the other country, and a general element of confusion. See the preceding discussion on the limitations of consent in Section 2.1.3 of this chapter.

934 E.g. Article 7 consent and contract rules. For analysis of such possibilities, see Section 2.1.2 of this chapter.

Furthermore, the mandatory rules of law make such negotiations possible, however restricted their scope is. This view is based on Basedow's observation that, generally, it was failures in the market which gave rise to regulation.[935] Accordingly, it is against the nature of the Directive to allow parties to contract around the guarantees contained in it. In the countries without developed data protection legislation, information industries often only have to inform individuals that they are collecting their personal data,[936] but are not required to mention that individuals are able to negotiate the terms of such collections. These industries are 'free-riding' and, controlled only by market forces, are able to collect data without limitations. In Europe, where data protection legislation is in force, including obligations to inform and seek consent to the processing of data if there are no other preconditions for lawful processing, these same information industries are forced to negotiate. It is true that, even with data protection legislation, the strength of the parties is still unequal at times and the conditions of negotiation unfair. However, this is a reason to improve the relevant regulations rather than abandon them altogether.

2.2.5. General contract and consumer protection law is sufficient?

The final argument in favour of a private law solution that is free from the restrictions of the Directive's approach is that, in combination with the OECD privacy guidelines, the 108 Convention, and Article 8 ECHR, the norms of the Dutch Civil Code create a data protection regime in contractual relationships that is similar to that of the Directive, meaning that the latter is, therefore, unnecessary.

For instance, Cuijpers claims that the Dutch law of obligations will often achieve the same result as the Directive by referring to, e.g. rules on the general and specific standards of care, the duties to warn and inform, the general principles of proper administration, the requirements of fairness and reasonableness, the doctrine of general terms and conditions, and the protection of a weaker party. With regard to the latter, Cuijpers proposed taking similar steps at a European level and including a clause stating that a controller is permitted to process a data subject's personal information in the list of unfair terms in consumer contracts contained in the annex

---

935 Basedow, "Freedom of Contract in the European Union."

936 For instance, in 2008, China was reported to have no developed system of data protection, except for a constitutional right to privacy still requiring implementation and a civil code provision recognizing privacy claims only when an individual's reputation is concerned. The enforcement of the only confidentiality requirement in the context of online messaging is weak and mostly reliant on the good will of the web-sites concerned (See Yu Du, Murphy, Matthew, "Data Protection and Privacy Issues in China," in *HG.org: Worldwide Legal Directories* (2008).). In 2006, the People's Bank of China was reported to have developed a nationwide database of its citizens' credit records which contained information about 97.5% of all consumer loans in the country (EPIC, *Privacy & Human Rights: An International Survey of Privacy Laws and Developments* (EPIC, 2006)., p. 192).

to Directive 93/13/EEC.[937] Berkvens also seems to have high hopes for what the contractual approach can achieve, proposing that if standard terms and conditions become the primary interface between consumers and businesses and appear to be "one-sided", "applications can be made to treat them as void or voidable under the Unfair Contract Terms Directive.[938] Consumer organizations can play a role in this connection by instituting [a] class action."[939]

Berkvens and Cuijpers undoubtedly have a valid point when calling for the use of tools of a more general application – like contract and consumer protection laws – for the purposes of data protection. Indeed, it is now a matter of common sense that these more general legal fields cannot remain ignorant of data protection requirements.[940] Combining the strengths of the two regimes will certainly benefit the data protection goals. However, relinquishing more specific data protection rules and relying solely on general contract and consumer protection instruments is not justifiable for a number of reasons.

Firstly, if data protection becomes a matter of contract and consumer protection law, the individual will have virtually no help to enforce his interests. Without any substitute for the data protection authorities commonly established in member states when implementing the Directive, individuals will face the burden of discovering and fighting faulty uses of their data themselves. Given how difficult this is for data protection authorities,[941] the likelihood of individual enforcement succeeding without the backup of state regulation and a specialized body is questionable.

Consumer organizations can certainly play a role in enforcement. However, how active and effective they are may vary significantly across the Union. For instance, in 1989 in the Netherlands, Berkvens claims that the country's consumer protection bodies were inactive in the field of data protection; although under the first Dutch Data Protection Act of 1989 "there was a statutory obligation for enterprises to consult with consumers, […t]he Dutch Consumers' Association did not attach much priority to the subject."[942] Of course, since 1989, data protection issues have gained much more prominence in the Netherlands, and Dutch consumer associations and similar organisations in other member states may be now more effective. However, until the extent of the functioning of consumer groups in the

---

937 Cuijpers, "A Private Law Approach to Privacy: Mandatory Law Obliged? .", pp. 315-316

938 Directive 1993/13/EC

939 Berkvens, "Role of Trade Associations: Data Protection as a Negotiable Issue.", p. 128

940 E.g. see Patrick Breyer's proposal to incorporate a 'right to be forgotten' into competition law and the law of product liability, also advocating the role of associations in enforcing data protection rules, presented on January 29, 2010 at the Conference "An Element of Choice" in Brussels, presentation also available at <http://ec.europa.eu/justice_home/news/events/events_2009_en.htm>

941 Bergkamp, "EU Data Protection Policy the Privacy Fallacy: Adverse Effects of Europe's Data Protection Policy in an Information-Driven Economy.", p. 37

942 Berkvens, "Role of Trade Associations: Data Protection as a Negotiable Issue.", p. 128

field of data protection is established by empirical research, it is still far too early for any data protection regime to abandon state enforcement.

Secondly, and following Cuijpers' proposal,[943] different contractual and non-contractual data processing regimes will be created if the rules of Directive 95/46/EC, which are implemented in the legislation of member states, govern the non-contractual processing of personal data and contracts govern the rest. Differences in regimes will create legal uncertainty, since for data subjects as laymen it may often be difficult to understand where a contract is formed and if and how it concerns data processing.

Finally, the argument may be criticized for its inconsistency. For instance, while opposing the implementation of the Directive into mandatory laws, Cuijpers refers to the rules governing the conclusion of contracts and consumer protection, which, just like the Directive, are rules of mandatory law and cannot be contracted around. The only difference between the Directive's regime, which is binding on contracts, and general mandatory rules of contract or consumer protection law, is that the Directive's regime is an example of specific legislation, whereas civil code provisions are of a more general nature. Sectoral law has the benefit of accounting for the special needs of the sector in question, namely automated data processing. What gains the rejection of specific rules that are more sensitive to the specificities of a particular field (information industry and data protection interests) brings remains to be seen.

To summarize, whereas data protection can indeed benefit from the mechanisms of contract and consumer protection laws, this fact alone is not enough to call for the use of these instruments as completely independent alternatives to the rules of the Directive. What makes more sense is: to use the strengths of both the Directive's regime and contract and consumer protection tools; for the latter to implement the rules of the former; and to strive to achieve the data protection goals rather than introducing uncertain laws, goals and priorities.

3. Conclusion

Once this study established the *erga omnes* effect as the common denominator enabling a common European discussion on property, and using the 1995 Data protection directive as the main reference point in the discussion on EU data protection, Chapter 8 showed that nothing in the current data protection regime prohibits or excludes introducing property rights in personal data. Indeed, in view of

[943] "[T]he directive offers a framework on how to process personal data when there is no contractual relationship, or when the contract does not concern the processing of personal data, even though processing of these data forms part of the relationship." Cuijpers, "A Private Law Approach to Privacy: Mandatory Law Obliged? .", p. 306

extreme flexibility of the concept of property in law defined by the *erga omnes* effect of the relevant rights, almost any system of rights that provides a degree of control (i.e. including data protection) can be translated into the language of property. To exclude the very possibility of the propertisation of personal data one would have to eliminate individual rights of control, or informational self-determination, in favour of administrative rules of data processing. That would require principal changes in the European approach to data protection as we know it. Such changes would be in contradiction to the evolutionary development of the European data protection which has already rejected administrative regulation as the sole mode of data protection. They would also be in contradiction to the relevant fundamental choices made in Europe, such as information self-determination, adopted on the level of OECD and Council of Europe, to which the Directive also adheres.

Even more so, the logic of property protecting one's entitlement to defend 'his own' against the world is consistent with the principle of individual information self-determination expressed in the Article 7 requirement of consent, information rights and a number of other Directive provisions. The principle of information self-determination moves the Directive close to the possibility of the introduction of limited propertisation, short of introducing de facto property rights in data with an individual as the holder of the 'biggest' property rights.[944]

Although information self-determination and control are a common denominator in the bulk of the data protection laws in Europe,[945] the purpose of which is to enable an individual to have a degree of freedom to choose what happens to his personal data, that does not suggest that the allowed degree of control allows an absolute dominion over personal data, including free and unlimited alienation of control rights.

Here comes another important conclusion as to the legal possibility of propertisation under the Directive. Chapter 8 established that although the current data protection regime does not exclude but endorses the 'property thinking' with regard to personal data, the introduction of actual property rights is only permitted within the limits established by *inter alia* data protection law. General European law and the 1995 Directive in particular do not allow any property regime of personal data to deviate from the 1995 Directive's provisions and create property rights of a wider scope than is granted by data protection rights. Most importantly, despite its goal to foster the common market and free flow of information, the Directive and the EU law in general do not adhere to the *laissez faire* ideology and pursue economic goals with the view to respect human rights. Besides, freedom of contract often invoked to justify free alienability of personal data does not have precedence over

---

944 Chapter 8, section 3.1.3; see Chapter 10, section 2.1 for a discussion on how the 1995 Directive is close to establishing de facto property in personal data.

945 Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits*., p. 63; Solove, *Information Privacy Law*., p. 872

data protection interests but has to be balanced against it. Even more so, freedom of contract cannot have a higher standing than the data protection rights as any meaningful negotiation of a contract, also in the field of personal data, seems impossible without law securing the interests of a weaker party. Therefore, the provisions of the Directive, e.g. establishing the data subject's rights, cannot be 'contracted around' with effect of the contract taking precedence over those rights.[946]

[946] Chapter 8, section 3.2 (a) through (e)

Chapter 9: Human rights nature of data protection as a limit on propertisation

1. Introduction

It has been established in the previous chapter that the 1995 Data Protection Directive allows, and in some provisions suggests, the propertisation of personal data as a possible way of achieving data protection goals, albeit only within the ambit of the Directive's regime. This chapter focuses on the permitted scope of private law solutions to the data protection problem in general, and propertisation in particular. The opportunity to waive data protection guarantees on the basis of market conditions in exchange for money, goods, or services is a cornerstone of many of the proposals reconsidering the current European approach to data protection.[947] This chapter argues, however, that human rights issues cannot be avoided or ignored in the data protection debate as a whole and the propertisation debate in particular.

A piece of evidence supporting validity of this 'human rights approach' to propertisation of personal data is a relatively recent European trend to elevate data protection guarantees to the level of constitutional rights, i.e. the so-called "constitutionalisation" of data protection (Section 2). Another piece of evidence is a strong tendency both in the relevant literature and in case-law of the European Convention of Human Rights to include positive data protection rights into the scope of protection of private life (Section 3).

The issue of the waiver of data protection rights is also considered (Section 4). It is concluded that Article 8 of the ECHR provides a basic level of data protection protection that cannot be simply given away for economic gain, which is a significant limitation on the scope of possible property rights in personal data. As a consequence, data protection guarantees which enjoy human rights protection cannot be freely contracted around or waived, and the ambit of the permitted contractual or property rights is limited by the existing 'basis' of the data protection rules.

---

[947] For recent evaluations and proposals to improve the 1995 Data Protection Directive see, e.g. Hans Graux Neil Robinson, Maarten Botterman, and Lorenzo Valeri, "Review of the European Data Protection Directive: Technical Report Prepared for the Information Commissioner's Office," (Santa Monica: RAND, 2009).

2. "Constitutionalisation" of data protection rights in national and EU law

A traditional objection to the propertisation of unconventional objects, such as personal data, is that it would encourage a free market in these sensitive objects rather than control it.[948] It has been established earlier in this study that the principle of free alienability to which this criticism refers is not a necessary element of the European concept of property rights.[949] In addition, this Section will show that data protection in Europe has been elevated to the level of a fundamental (or constitutional) right both via constitutional reforms in individual member states and recent changes in the EU constitutional treaties (development referred to as 'constitutionalisation'). Therefore the European debate on propertisation of personal data cannot disregard the limits that the human rights nature of data protection imposes on potential property rights solutions.

In the past years the right to data protection became generally recognised as a part of the national constitutional heritage of most EU member states.[950] Whether the right stands alone in a national bill of rights or was developed from another constitutional right such as privacy, autonomy, or development of personality, varies depending on national constitutional traditions. To bring some examples, data protection rights in Belgium have a constitutional basis in the right to privacy. The Belgian Constitution guarantees the right to respect of private life (Article 22). Although it does not explicitly mention data protection rights, a right to respect for private life is generally deemed to include protection in cases of data collection, registration, use and transfer. Other data protection guarantees are included into specific legislation.[951]

In Germany, data protection has evolved from the value of human dignity and a right of development of personality. The German Basic Law does not have explicit provisions on privacy or data protection. However, both have been read into 'the general right of personality', which, in turn, evolved from the interpretation of Article 2 (1) (read together with Article 1 (1) (dignity)).[952] As a result, the right of

---

[948] Chapter 4, Section 3.3

[949] Ibid.

[950] Bert-Jaap Koops, "Conclusions and Recommendations," in *Constitutional Rights and New Technologies: A Comparative Study*, ed. Ronald Leenes, Koops, Bert-Jaap, De Hert, Paul (The Hague: Asser Press, 2008)., p. 271 et seq.

[951] Eva Lievens, et al., "Constitutional Rights and New Technologies in Belgium," in *Constitutional Rights and New Technologies: A Comparative Study*, ed. Ronald Leenes, Koops, Bert-Jaap, De Hert, Paul (The Hague: Asser Press, 2008)., p. 25 et seq.

[952] Thomas Hoeren, Rodenhausen, Anselm, "Constitutional Rights and New Technologies in Germany," in *Constitutional Rights and New Technologies: A Comparative Study*, ed. Ronald Leenes, Koops, Bert-Jaap, De Hert, Paul (The Hague: Asser Press, 2008)., p. 139 et seq. referring to the decision of the Federal Court of Justice (*Leserbrief*) later adopted by the Federal Constitutional Court (*Elfes-Urteil* decision).

information self-determination enjoys a status of a fundamental right and protection of the Constitution.[953]

Data protection rights have become a part of the Dutch Constitution as a result of the 1983 Constitutional revisions. They have been 'attached' to Art. 10 general right to privacy in paragraphs 2 and 3 containing respectively an instructions to the Parliament to pass a law protecting privacy "in connection with the recording and dissemination of personal data;" and to establish individual rights "to be informed of data recorded concerning them and of the use that is made thereof, and to have such data corrected."[954]

Similar process of constitutionalisation on the EU level began with the adoption of the EU Charter of Fundamental Rights which, next to the right Respect for private and family life (Article 7) recognised a separate right to Protection of personal data (Article 8). The right guarantees that the data is to be processed "fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law;" the right of access and rectification, and is to be controlled by an independent authority. The Lisbon Treaty which entered into force on 1 December 2009, introduced the Charter into the EU primary law.

Another significant EU constitutional provision is Article 16 (ex Article 286 TEC) of the Consolidated Version of the Treaty on the Functioning of the European Union (TFEU) that effectively establish data protection rights for the EU regardless its pillar structure, and gives instructions to the EU institutions to take legislative steps to effectuate these rights throughout the Union law.

The reviewed developments in national and supra-national laws in Europe reveal that it is no longer possible to avoid human rights issues when discussing data protection matters. This conclusion is especially relevant when the data protection rights come into conflict with other interests, such as freedom of contract or free alienability of personal data for economic gain. The position of this study on the right balance between those interests and the implications for permitted scope of property rights in personal data will be considered in Section 4 of this Chapter.

---

953 Ibid.

954 Bert-Jaap Koops, Groothuis, Magda, "Constitutional Rights and New Technologies in the Netherlands," in *Constitutional Rights and New Technologies: A Comparative Study*, ed. Ronald Leenes, Koops, Bert-Jaap, De Hert, Paul (The Hague: Asser Press, 2008)., p. 166 et seq.

3. A strong tendency to include data protection rights into the Article 8 ECHR right to respect for private life

The European Convention on Human Rights is one of the pillars of the human rights system in Europe. Therefore an inquiry into how this instrument treats data protection rights is a necessary step of any analysis of data protection from a human rights perspective.

Because the language of the Convention does not explicitly recognise the right to data protection, this right can only enjoy the Convention's protection – without amending the instrument – if 'read into' one of the explicitly named rights. It will be shown that the ECHR case-law has already explicitly brought a number of data protection rights under the protection of Article 8(1). Moreover, there is conclusive evidence in favour of a broader tendency to treat data protection interests in general as an integral part of a right to respect of private. This conclusion supports the main thesis of this Chapter that, while examining the possibility and legitimate scope of property rights in personal data in the European legal order, the human rights dimension of the topic cannot be avoided.

Section 3.1 will briefly outline the debate and provide a roadmap for the further analysis of the data protection – privacy relationship. Section 3.2 will review the case-law applying Article 8 ECHR and demonstrate that the scope of the right to respect of private life at present already goes beyond protecting only secret personal information and regulates some aspects of data protection. Section 3.3 will argue that the protection afforded by Article 8 has potential to develop even further and include the entire scope of data protection rights.

3.1. The analytical framework

The text of Article 8 ECHR establishing the substantive scope and limitations of the right to respect for private and family life gives little guidance in answering the question whether data protection interests enjoy the Convention's protection. Article 8 reads as follows:

> 1. *Everyone has the right to respect for his private and family life, his home and his correspondence.*
> 2. *There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*

At the same time, the reasons not to include the right to data protection under the umbrella of the general privacy right are multiple. Privacy, at least, in the current theoretical debate, means everything and nothing. It (approximately) encompasses the entire range of interests of personal autonomy, democratic participation, bodily integrity, family life, sanctity of the home, etc. Arguably, bringing the issue of data protection into this arena further obscures 'the meaning' of privacy. Indeed, there are many opinions on the privacy–data protection relationship. The theoretical standpoints in favour of and against treating data protection as consumed by or largely intersecting with privacy, or, alternatively, treating the two categories as being absolutely distinct, rely on different ways of *conceptualis*ing the notion of privacy. Seeing data protection, as a part of privacy is consistent with it being equated to: secrecy; or a right against the disclosure of concealed information; or a right to limit access to the self; or control over information pertaining to the self. Among those supporting this approach, Daniel Solove submits that the meaning of the words ought to be understood from how they are actually used.[955] Hence, the relationship between privacy and data protection is better understood in terms of "family resemblance" rather than by some shared core characteristics.[956]

It seems unlikely that the theoretical debate on the meaning of privacy and its relation to data protection will end soon. Accordingly, this work focuses on the actual legal rules in practice. In this respect, two points of view are of special interest: the one developed by Paul De Hert and Serge Gutwirth,[957] and another proposed by Peter Blok and supported by Colette Cuijpers. Both of these approaches concern the scope of the protection in Article 8 ECHR and argue that it does not include the protection of personal data as such.

Peter Blok submits that the core element of a breach of the Article 8 right to privacy is an intrusion into one's private sphere. In the framework of information privacy, only secret, personal information is protected by privacy rules.

> *The individual right to privacy both safeguards an undisturbed private life and offers the individual control over intrusions into his private sphere. Given this definition, the boundaries of the private sphere are central to the meaning of privacy. The right to privacy guarantees individual freedom within the home, within the intimate sphere of family life, and within confidential communication channels. In combination with*

[955]Solove, "*Conceptualis*ing Privacy.", p. 1126.
[956]Ibid.
[957] Paul De Hert, Gutwirth, Serge "Making Sense of Privacy and Data Protection: A Prospective Overview in the Light of the Future of Identity, Location-Based Services and Virtual Residence in the Institute for Prospective Technological Studies: Report Eur 20823 En," *Security and Privacy for the citizen in the post-September 11 digital age: a Prospective overview* (2003).

> *physical integrity, these 'privacies' form the core of the legally protected private sphere.*[958]

Colette Cuijpers agrees, and continues that "as the protection of the individual with regard to the processing of personal data is in no way restricted to data concerning the private sphere of the individual, […] the choice to link data protection to the right to privacy is unjustly made."[959] Put another way, not all aspects of data protection are covered by the scope of the protection of privacy. As a result, data protection in itself does not enjoy the status of a fundamental right. One of the consequences is that data protection considerations are not powerful enough to serve as legitimate grounds for restrictions of freedom of contract, meaning that the latter, when balanced against data protection interests, has precedence. In other words, in a contract one is free to not abide by data protection requirements.[960]

The general feeling one gets after reading Blok's argument is that Article 8 ECHR jurisprudence should not have gone as far as extending the right to privacy beyond the text of the Convention, and in doing so diminishes the importance of the right that was originally intended to be protected. This is, in essence, a normative statement, which highlights the approach the jurisprudence should have taken. Paul De Hert and Serge Gutwirth's standpoint is more structural, and is aimed at making sense of the conceptual disorder ruling the privacy–data protection debate. This approach is based on the understanding that privacy and data protection rights are tools that are too different in nature to be treated as one.[961] These scholars consider the two categories against the background of a democratic constitutional state and as two distinct tools with which to control state power.[962] They come to the conclusion that privacy limits state power by creating a sphere of individual autonomy and self-determination that is free from state intervention.[963] Privacy labelled as an opacity tool is therefore a negative right which empowers an individual to prevent the state from intervening in his affairs, but not to require the state to take any positive steps.[964] Data protection, on the other hand, is a transparency tool. It does not prohibit state intervention, but rather channels and controls it by giving an individual positive rights and imposing affirmative obligations on the state.[965] The distinctions between these two types of instruments should not be blurred.[966]

---

[958] Blok, *Recht Op Privacy.*, p. 323.
[959] Cuijpers, "A Private Law Approach to Privacy: Mandatory Law Obliged?."
[960] Ibid., p. 312-315.
[961] De Hert, "Making Sense of Privacy and Data Protection: A Prospective Overview in the Light of the Future of Identity, Location-Based Services and Virtual Residence in the Institute for Prospective Technological Studies: Report Eur 20823 En."
[962] Ibid., p. 134.
[963] Ibid.
[964] Ibid., p. 138.
[965] Ibid., p. 144.
[966] Ibid., p. 146.

Despite the normative nature of Blok's argument and De Hert and Gutwirth's more conceptual stance, both approaches may be reduced to one key element: the protection from intervention of the private sphere (whatever that is) is an opacity tool, while the right to privacy is a negative right. Data protection is a transparency instrument implying positive obligations, and cannot, therefore, be dealt with by the protection of privacy.

The following analysis will use the 'opacity - transparency tools' dichotomy as a road-map and will show that, regardless of the arguments of Blok, Cuijpers, De Hert and Gutwirth, when it comes to actual application of law, the European Court of Human Rights in Strasbourg does not limit the scope of Art. 8 ECHR to the private sphere only, and the provision on protection of private life has been applied as giving individuals positive rights and imposing on states affirmative obligations. Consequently, in legal practice there is no ground to treat data protection distinctly from privacy rights.

When relying on De Hert and Gutwirth's approach to the functions of privacy and data protection in a democratic constitutional state, one could argue that data protection should be viewed as being beyond the scope of Article 8. There are two possible reasons in support of such a claim. The first relates to the substance of the protection; Article 8 ECHR protects only privacy as secrecy, i.e. it only concerns concealed personal information, and prevents its collection, but does not apply to other information practices. The second reason relates to the mode of protection; Article 8 ECHR does not apply to private parties and does not contain affirmative obligations. The following sections argue against both these claims.

3.2. Article 8 (1) ECHR: beyond privacy as the secrecy of information

This section demonstrates that it would be contrary to the developments of the ECHD case-law and doctrine to exclude data protection rights from the scope of protection of private life under Article 8 (1) on the ground that this protection is only afforded to secret 'private' information. A number of factors support this conclusion.

The first factor is the dynamic nature of the Convention. Indeed, in the 1950s, when the Convention was adopted, or in 1968, when its applicability to data protection was evaluated, the respect for private and family life as enshrined in Article 8 ECHR might have contained only a negative right protecting an individual's private sphere from state intervention. However, an opposite interpretation has gained support since than, based on the assumption that "the Contracting Parties signed in full knowledge that ideas and morals [behind the Convention's interpretation – N.P.][967] would change and that the meaning of the Convention would keep pace."[968]

[967] Text in square brackets is added.

Another piece of evidence in favour of understanding data protection as a part of the right to respect of private life is the practice of the European Court of Human Rights to interpret the interest of private life broadly. The lack of precision in Article 8 (1) allows the case-law to develop dynamically and adequately to social and technological developments.[969]A survey of the case-law which O'Boyle and Harris refer to, shows a generous, non-exhaustive approach to the definition of the personal interests protected,[970] including such at the first glance unrelated interests as environmental rights.[971]

In addition, the meaning of private life was interpreted so broadly that commentators, among others, O'Boyle and Harris, explicitly refute to equate Article 8 (1) protection to protection of privacy as secrecy of information:

> *Private life thus extends beyond the narrower confines of the Anglo-American idea of privacy, with its emphasis on the secrecy of personal information and seclusion.*[972]

Already in the European Commission's decisions[973] and later Court's judgements ECHR jurisprudence has recognized that the right to respect for "private life" does not end with the protection of secret information, but also comprises rights to develop relationships, also beyond one's family circles. In *Niemietz v Germany*, the Court explained that the respect of private life under Article 8 (1) went beyond protection of the 'inner circle' and secret information and "must also comprise to a certain degree the right to establish and develop relationships with other human beings."[974] Decisions in other cases go as far as acknowledging the connection between "the right to establish and develop relationships with other human beings

---

968 R. Beddard, *Human Rights and Europe*, 3rd ed. (Cambridge University Press, 1994)., p. 96.

969 See, e.g. *Rees v. UK,* A 106 (1986), para. 47

970 D.J Harris, O'Boyle, M.O., Bates, E.P., Buckley, C.M., *Harris, O'boyle & Warbrick Law of the European Convention on Human Rights*, 2nd ed. (Oxford University Press, 2009)., p. 361; see e.g. Peck v UK, 2003-I, 36 EHRR 719, para. 32 where the Court established that private life is a broad concept incapable of exhaustive definition.

971 Ibid., e.g. the *Guerra* case (EHRC58) where a failure to provide information about environmental conditions was considered a violation of the right to respect for private life.

972 Harris, O'Boyle & Warbrick Law of the European Convention on Human Rights, p. 364 referring to *I. v Iceland,* No 6825/74, 5DR 86 (1976)

973 Although the European Commission has been abolished, this study uses the Commission's decisions because the Court itself attributes weight to them. As Karen Reid explains, "it is only recently that the Court has openly given weight to Comission precedent. It is therefore not irrelevant to refer … to Commission case-law which was particularly percuasive […]" (Karen Reid, *A Practitioner's Guide to the European Convention on Human Rights*, 3rd ed. (Thomson, Sweet & Maxwell, 2008)., p. 61, I-081). Reid continues that the references to the Commission's case-law become less necessary as the Court builds up "its own bank of precedents" (Ibid.). It is the author's opinion that the Court's bank of case-law on the issues of individual autonomy, data protection and positive state obligations under Article 8 is still in the process of development. Therefore, reliance on a number of the Commission's decisions seems justified.

974 ECHR,1992, para. 29

especially in the emotional field," and "development and fulfilment of one's own personality."[975]

The relevant literature as well read such general values as development of personality and individual autonomy into the scope of Article 8 (1) protection. As early as in 1994, Beddard wrote that although the European Convention "does not talk of the right of personality, … particularly within Articles 8 to 11 are found the rights which go towards the fulfilment of personal hopes, aspirations, and ideals."[976] More recently, after reviewing recent ECHR case-law on decisional autonomy, e.g. the case of *Pretty*, De Hert and Gutwirth have also updated their views on the privacy-data protection relationship, writing that the Strasbourg court's case-law on the issue of privacy, although terminologically ambiguous,[977] does not yet grant protection to the right of self-determination, but does guarantee a right to personal development,[978] and acknowledges the importance of the principle of individual autonomy, including in data protection cases.[979]

> *We do not think that conceptually all is clear but the ruling of the Court shows that the principle of personal autonomy has gained considerable importance within the right of privacy. Whether Article 8 ECHR also entails a right of determination, including informational self-determination, remains unanswered at this point.*[980]

Rouvroy and Poullet also bring examples of the Article 8 (1) ECHR case-law acknowledging the interest of individual decisional autonomy in various sectors: sexual life, right to die, right to access to full information about a place of residence, etc.[981]

A recent example of a case where the value of personal development was affirmed is the 2009 case of *Reklos* and *Davouris v. Greece*.[982] The court held:

---

[975] Commission Report *X. v. Iceland* (Application No. 6825/74) of 18 May 1976 in Decisions and Reports, Vol 5 at p 87; David Harris Donna Gomien, Leo Zwaak *Law and Practice of the European Convention on Human Rights and the European Social Charter* (Strasbourg: Council of Europe Publishing, 1996)., p. 231; *Oosterwijck v. Belgium*, Comm. Report 1.3.79, para. 51, p. 36.

[976] Beddard, *Human Rights and Europe*., p. 95.

[977] De Hert, "Data Protection in the case-law of Strasbourg and Luxembourg: Constitutionalization in Action.", p. 15 fn 64

[978] See ECHR *Christine Goodwin v. the United Kingdom* [GC], no. 28957/95, § 90, ECHR 2002-VI

[979] De Hert, "Data Protection in the case-law of Strasbourg and Luxembourg: Constitutionalization in Action.", p. 15

[980] De Hert, "Data Protection in the case-law of Strasbourg and Luxembourg: Constitutionalization in Action.", p. 15

[981] Rouvroy, "The Right to Information Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy.", p. 62

[982] ECHR, 15 April 2009, *Reklos and Davourlis v. Greece*, Application no. 1234/05 (unauthorised photos of a baby)

> *… [A]ccording to its case-law "private life" is a broad concept not susceptible to exhaustive definition. The notion encompasses the right to identity (see Wisse v. France, no. 71611/01, § 24, 20 December 2005) and the right to personal development, whether in terms of personality (see Christine Goodwin v. the United Kingdom [GC], no. 28957/95, § 90, ECHR 2002-VI) or of personal autonomy, which is an important principle underlying the interpretation of the* Article *8 guarantees (see Evans v. the United Kingdom [GC], no. 6339/05, § 71, ECHR 2007-..., and Pretty v. the United Kingdom, no. 2346/02, § 61, ECHR 2002-III).*[983]

De Schutter argues that Article 8 case-law – like the interpretation of Article 2 (1) of German Basic Law - may extend to include the protection of a broader right to the free development of personality.[984] The latter, in turn, provided the case-law of ECHR takes the same path the German Constitutional Court took, may in future give birth to a general ECHR right to data protection as it happened in German constitutional law.[985]

Whether such a general data protection right is already a part of the right to respect for private life is unclear. On the one hand, there is a body of relevant case-law where individual data protection rights were afforded protection under Article 8.[986] To name only few examples, the 'principal case' *Gaskin v UK*, although did not confer any general right of access,[987] acknowledged that a refusal by public bodies to grant access to information stored by public bodies constitutes a violation; simultaneously, the Court did not find such a violation where security files were concerned.[988] *McVeigh v UK* concerned the issues of collection (fingerprinting, taking photos, questioning and searching was found a justified interference);[989] *Z v Finland* recognised disclosure of personal data to the third parties covered by the right to respect for private life.[990] In *Leander*, the Court found that not only storage and release of personal information constituted an infringement of the right to private life, but also refusal to provide an opportunity to refute the content of a personal file.[991]

---

[983] *Reklos*, para. 39

[984] Olivier De Schutter, "Waiver of Rights and State Paternalism under the European Convention on Human Rights," *N. Ir. Legal Q.* 51, no. 3 (2000)., p. 498

[985] 1983 census decision: BVerfGe 65, 1: "This basic right warrants in this respect the capacity of the individual to determine in principle the disclosure and use of his/her personal data." See section 2 of this Chapter.

[986] Chapter 8, section 2.1.2.

[987] Reid, *A Practitioner's Guide to the European Convention on Human Rights*., p. 487

[988] Ibid., p. 488

[989] *McVeigh v UK*, 8022/77, March 18, 1981, 25 D.R. 15

[990] para. 95

[991] *Leander*, para. 48 (the infringement was found justified)

On the other hand, it is impossible to draw any general conclusions from those cases, also the conclusions on whether or not a general right to data protection is (potentially) found in the Article 8 (1) right to respect for personal life. Indeed, any generalisations about the ECHR jurisprudence should be made with caution as the Court does not have a competence to make law but to solve cases and, as Harris and O'Boyle put it, "the outcome of any particular case may not tell as much beyond its own facts."[992] Therefore, until a case comes before the Strasbourg Court and it expressly pronounces that the general data protection right is an element of private life under Article 8 (1), it is premature to state that it is already the case. However, on the same ground it is also premature to refute such a possibility in principle, as the 'privacy-as-secrecy' interpretation of Article 8 (1) does. Finally, there is a clear tendency to read a right to personal development and individual decisional autonomy into Article 8 (1). The position of this study is that it is a likely way for the general data protection right to enter the ECHR jurisprudence.

3.3. Affirmative obligations and a horizontal effect of Article 8 ECHR

This section refutes the second principal objection to treating data protection as an element of respect for private life, i.e. that the privacy protection under Article 8 only contains negative obligations (by virtue of paragraph 2) whereas data protection rests on positive or affirmative obligations. It will be demonstrated that Article 8 protection also implies affirmative, or positive, obligations of a state with regard to personal data. Moreover, by means of the 'affirmative obligations' reasoning, the effect of the Convention is extended to the behaviour of private parties (i.e. the horizontal effect of Article 8 ECHR).

One may observe evolution of the ECHR case-law on affirmative state obligations in general, and in the context of private life in particular, leading to recognition of the state positive obligations. In the early years of applying the Convention, its institutions interpreted the right in Article 8 (1) in conjunction with Article 8 (2), which requires that "there shall be no interference by a public authority with the exercise of this right." Indeed, the doctrine of state non-intervention used to be dominant in understanding of the substance of the right to privacy under Article 8 (1),[993] is consistent with the literal meaning of the second paragraph of Article 8 and the classical conception of fundamental rights as negative. However, the subsequent application of the Convention was clearly based on the understanding that an entirely negative approach to state responsibility is "inadequate to secure the

[992] Harris, *Harris, O'boyle & Warbrick Law of the European Convention on Human Rights*., p. 362

[993] Donna Gomien, Harris, David, Zwaak, Leo *Law and Practice of the European Convention on Human Rights* (Strasbourg: Council of Europe Publishing, 1996)., p. 231.

effective exercise of the individual's freedoms."[994] The principle is known as a principle of effective protection - as opposed to the theoretical enjoyment of rights – and was first set out in *Golder v. UK*[995] and *Airey v. Ireland*.[996]

Based on the principle of the effective enjoyment of rights, Article 8 ECHR jurisprudence has further evolved to reveal signs of acknowledging that recognition of the positive obligations of the state under the Convention is possible. Harris and O'Boyle distinguish three lines of ECHR case-law and three corresponding kinds of positive state obligations:[997]

> *1) the obligation of the authorities to take steps to ensure that the enjoyment of the right is effective (e.g. Marckx case[998]);* [this obligations include the obligations to pass laws that grant legal status, rights and privileges to be ensured under the Convention];[999]
>
> *2) the obligation of the authorities to take steps to ensure that the enjoyment of the rights is not interfered with by other private persons (e.g. in Young, James, and Webster v. UK[1000] and von Hannover v Germany*[1001]*); and*
>
> *3) the obligation of the authorities to take steps to ensure that private persons take steps to ensure the effective enjoyment by other individuals of the rights (e.g. X v. UK).*[1002]

The latter line of case-law in the data protection context may be interpreted as calling for the adoption by state-signatories of data protection measures which reflect ECHR principles and, as a result, impose ECHR rules on private parties.

Let us now revisit the three types of cases in their order of appearance.

3.3.1. Affirmative obligations in the first line of case-law

Gaskin v. UK is an example of the affirmative obligation set out in the first line of case-law, i.e. the requirement that a state must ensure the effective enjoyment of

---

[994] Michael O'Boyle David Harris, Edward Bates and Carla Buckley *Harris, O'Boyle & Warbrick: Law of the European Convention on Human Rights* (Butterworths Tolley, 1995). 1995), p. 284. See also Harris, *Harris, O'boyle & Warbrick Law of the European Convention on Human Rights*., p. 362

[995] ECHR 21 February 1975, *Golder v. UK* Application No. 4451/70.

[996] ECHR 09 October 1979, *Airey v. Ireland,* Application No. 6289/73.

[997] Harris, *Harris, O'boyle & Warbrick Law of the European Convention on Human Rights*., p. 342

[998] ECHR 07 July 1979, *Gaskin v. UK,* Application No. 10454/83.

[999] Harris, *Harris, O'boyle & Warbrick Law of the European Convention on Human Rights*., p. 342, fn 8

[1000] ECHR 13 August 1981, *Young, James, and Webster v. UK* Application No. 7601/76; 7806/77. *paras. 55-56 (1981)*

[1001] 2004-VI; 43 EHRR 2

[1002] *ECHR 05 November 1981,* X v. UK, *Application No. 4515/75, cited in Gomien, Law and Practice of the European Convention on Human Rights. 284.*

fundamental rights. The case concerned the accumulated records of Mr Gaskin's childhood, which he spent in care. The authorities refused to disclose the records to protect the confidentiality of those who had provided the information. The Commission found that respect for private life "requires that everyone should be able to establish details of their identity as individual human beings" and the court decided that the failure of the state to develop procedures whereby the files could be available to the applicant constituted a violation of a positive obligation on the state under Article 8.

In *Klass*,[1003] another example of the first type of positive obligations, the court found that there was a positive obligation on the state to protect personal data from being abused by private parties. The applicants challenged the 1968 legislation, which authorized surveillance in certain circumstances without the need to inform the individual concerned. The court found that such a procedure was contrary to Article 8 ECHR. Although the interference was found to be necessary in a democratic society in view of the threat posed to democracy by highly sophisticated forms of espionage and terrorism, the court also noted that adequate and effective guarantees against abuse must be put in place:

> *As concerns the fixing of the conditions under which the system of surveillance is to be operated, the Court points out that the domestic legislature enjoys a certain discretion. It is certainly not for the Court to substitute for the assessment of the national authorities any other assessment of what might be the best policy in this field. […]*
>
> *Nevertheless, the Court stresses that this does not mean that the Contracting States enjoy an unlimited discretion to subject persons within their jurisdiction to secret surveillance. The Court, being aware of the danger such a law poses of undermining or even destroying democracy on the ground of defending it, affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate.*
>
> *The Court must be satisfied that, whatever system of surveillance is adopted, there exist adequate and effective guarantees against abuse.*[1004]

3.3.2. Affirmative obligations in the second and third lines of case-law

The types of case-law 2) and 3) on affirmative obligations are of special interest in the context of data protection, since they bring data processing in the private sector within the scope of Article 8 ECHR. The decisions in the second line of authorities

---

[1003] ECHR 06 September 1978, *Klass and Others v. Germany,* Application No. 5029/71.
[1004] Paras. 49-50

have been interpreted to support a claim that a state is obliged to ensure that private individuals do not violate the right to privacy as protected by Article 8. It is difficult to distinguish the cases of the second type from the cases of the third type. Often they are both brought under one heading.[1005] This is how they will be considered here.

One of the first examples is *X and Y v. the Netherlands,*[1006] and has to do with bodily privacy. A mentally disabled girl and her father complained that it was impossible for either of them to commence criminal proceedings against a man who had sexually assaulted her. The court found that the girl's right to privacy under Article 8 had been violated, and agreed that the state had a positive obligation to ensure that all individuals have effective ways of vindicating their right to privacy which, in this case, was violated by a private person.

> *The Court recalls that although the object of* Article *8 (*Article *8) is essentially that of protecting the individual against arbitrary interference by the public authorities, it does not merely compel the State to abstain from such interference: in addition to this primarily negative undertaking, there may be positive obligations inherent in an effective respect for private or family life (see the Airey judgment of 9 October 1979, Series A no. 32, p. 17, para. 32) These obligations may involve the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves.*[1007]

The *Von Hannover v Germany* is an important ECHR judgement that applied state positive obligations to the relationships between private parties in the area of personal data. The applicant, a member of Monaco royal family, claimed a violation of her right to respect of private life because German authorities restricted her right to privacy in her function of a public figure when they did not ban press from taking and publishing her photographs. The Court found that the infringement constituted a violation of Article 8 (1) in that the German government did not strike a right balance between privacy interests of the plaintiff and alleged interest in free speech. The Court held that the photos in question were private, did not contribute to any public debate but only served financial interests of the involved media. However, more important for the purposes of the present analysis is paragraph 57 of the decision where the Court reaffirmed that the obligations of authorities under Article 8 (1) are not only to abstain from but also to take measures to prevent privacy violations, even in relationships between private parties.

The *I. v. Finland*[1008] decision has already been labelled as a "landmark" ruling, which highlighted "the importance of security measures in the protection of personal

---

[1005] Harris, *Harris, O'boyle & Warbrick Law of the European Convention on Human Rights*., p. 342

[1006] ECHR 26 March 1985, *X. and Y. v. The Netherlands*, Application no. 8978/80.

[1007] Ibid., para. 23

[1008] *ECHR 17 July 2008,* I v. Finland*, Application no. 20511/03.*

data in a manner that ought not to leave any uncertainties at least for the governmental actors."[1009] Formally, *I v Finland* should be classified under the second heading, because the infringement in question involved a public hospital which is regarded as a government authority. At its minimal potential, this case spells out a positive obligation of the government authorities to make sure that there are no violations of the protected rights in the relationships between private parties, in case at hand, Ms I and hospital personnel.

The applicant, a Finnish citizen, worked as a nurse in an eye clinic between 1989 and 1994. During the course of her employment, after being diagnosed as HIV-positive, she regularly visited another clinic in the same hospital. She became suspicious that her colleagues knew of her condition and that someone in the hospital had unlawfully had access to her medical files in the hospital database. The database's management system enabled all staff to have free access to patients' files. After she made a complaint to her superiors, the system was changed. She was also given a new record under a false name. When the term of her employment expired, the applicant asked an administrative body in the field of social and healthcare services to investigate who had had access to her file. Due to the technical limitations of the system, this was impossible, since it only kept records of the last five log-ins and contained no references to the names of individuals, but only to their departments. Moreover, after files were returned to the archive, all records relating to how they had been accessed were cleared. The system was changed after the state body drew the hospital's attention to these problems. The applicant initiated civil proceedings against the hospital and claimed damages. The claim was unsuccessful since the national court did not find conclusive evidence of unauthorized access to I's medical file. After exhausting national measures, the plaintiff thus filed a complaint with the European Court of Human Rights.

The applicant claimed that there had been a breach of Article 8 ECHR on the grounds that the district health authority "had failed in its duties to establish a register from which her confidential patient information could not be disclosed"[1010] and "the measures taken by the domestic authorities to safeguard her right to respect for her private life had not been sufficient."[1011] The court upheld the applicant's claim.[1012]

A cumulative consideration of the aforementioned cases in general, and the decision in *I. v. Finland* in particular, leaves the reader in no doubt that the right to

---

[1009] Jari Råman, "European Court of Human Rights: Failure to Take Effective Information Security Measures to Protect Sensitive Personal Data Violates Right to Privacy – I V. Finland, No. 20511/03, 17 July 2008," *Computer Law & Security Review* 24(2008)., p. 562.

[1010] *I. v. Finland,* para. 26.

[1011] *I. v. Finland,* para. 29.

[1012] *I. v. Finland,* para. 36.

privacy, as protected by Article 8 ECHR, also imposes positive state obligations and, thus, incorporates data protection interests.

As well as its great significance to the acknowledgement in Article 8 jurisprudence of the doctrine of positive state obligations, *I. v. Finland* has opened another door to the notion that data protection rights are covered by the Article 8 ECHR right to privacy. As a result of the positive obligation reasoning therein, this judgement took one more step towards creating a horizontal effect of Article 8 protection, i.e. it moved towards making its provisions relevant to the private sector.

I. v. Finland first affirmed the current, second type of case-law regarding positive obligations "even in the sphere of the relations of individuals between themselves."[1013]

But the court also went further:

> *[T]he mere fact that the domestic legislation provided the applicant with an opportunity to claim compensation for damages caused by an alleged unlawful disclosure of personal data was not sufficient to protect her private life. What is required in this connection is practical and effective protection to exclude any possibility of unauthorised access occurring in the first place.*[1014]

In other words, although at the time of the violation there was a national law in place which made unauthorized access to medical files unlawful, and despite the fact that the violation of that law led to a breach of Article 8, the mere existence of general data protection rules is not enough to meet the positive state duty. The state is also obliged to create an effective system of data security to ensure that other (including private) actors do not violate the right to privacy protected by Article 8. Consequently, the *I. v. Finland* judgement may first be interpreted as a call, if not for a more detailed system of state regulation of data processing, surely for its better enforcement. However, most importantly, it may also be regarded as a call for state application to the private sector of the ECHR principles of privacy protection (including data protection). Such an impact, with reservations,[1015] may be called the horizontal effect. As a result of the *I. v. Finland* judgement, states signatories to the Convention may be found liable for failing to ensure that private parties take positive steps to prevent privacy violations by other private parties. Accordingly, the decision at hand lays the groundwork for the application of the ECHR privacy principles to the national systems of data protection that are set up to prevent such breaches.

[1013] Ibid. para. 36.

[1014] Para. 47.

[1015] A clarification has to be made here: the term 'horizontal effect' cannot be used unconditionally to describe the effect of Article 8 ECHR on the relations between private parties, since the latter cannot draw rights and obligations from the text of the Convention directly; nevertheless the Convention's principles still *unavoidably* influence those relationships, albeit *via* the state, since the state is obliged to implement the principles in the data protection measures that are relevant to private parties.

The case of *K.U. v. Finland*[1016] is another example of the ECHR's influence on the content of the states' positive obligations under Article 8, and, consequently, also on the content of the data protection rules and the obligations of private parties. However, this case is different from the ones considered previously in this Chapter in that the judgement defined limits of data protection rights not of the applicant, but of the third party – suspect in a criminal case.

In the 2008 case of K.U. v. Finland, the Strasbourg court seems to have made explicit use of the opportunity set up in *I. v. Finland*. Indeed, not only did the court clarify the content of states' positive obligations to protect privacy in general by criminalizing any interference with children's privacy, but it also, albeit through the back door of an interest that counterbalanced the vindication of privacy, provided guidelines for the parties to the Convention about the content and extent of their data protection obligations regarding the issue of anonymity on the Internet.

K.U. was a 12 year old boy when the events in question occurred. In 1999, an unknown person, without the applicant's knowledge, placed an advert containing the applicant's personal details on a dating website. The advertisement claimed that the applicant was seeking an intimate relationship with a boy of his age or older "to show him the way."[1017] The boy found out about this after receiving an e-mail from a man who wished to arrange a meeting. The applicant's father asked the police to identify who the man was. However, the service provider refused to disclose the IP address of the alleged offender due to a statutory obligation to maintain confidentiality. The police failed to secure a court warrant to order the provider to disclose the necessary information, since malicious misrepresentation – which was how the act in question was qualified in Finnish national law – was not among the offences giving rise to an exception to the confidentiality requirement. The man who answered the advertisement was identified on the basis of his e-mail address and was charged with a criminal offence. However, the managing director of the service provider could not be charged since his alleged offence had became time-barred (seeking civil redress was still possible). This director was allegedly guilty of a violation of the provision of the Finnish Personal Data Act, which required a service provider to verify the identity of someone publishing a defamatory comment. At that time, processing and publishing sensitive personal data concerning sexual behaviour on an Internet server without the subject's consent was a criminal offence.[1018] The applicant claimed that the failure of the state to impose criminal liability for the violation of privacy was in breach of Article 8 ECHR. In other words, the government failed to ensure the consistency of the provisions of the national law requiring the consent of the data subject to the processing of data referring to his sexual behaviour. Furthermore, making it a criminal offence to not verify the sender

[1016] ECHR 2 December 2008, *K.U. v. Finland,* Application no. 2872/02

[1017] *K.U. v. Finland,* para. 7

[1018] Ibid., paras. 7-19

of such data on the one hand, but not including malicious misrepresentation on the list of exceptions to the duty of confidentiality on the other, was also a failure by the Finnish government. As a result, the balance between the anonymity of Internet users and privacy was erroneously struck in favour of alleged offenders.[1019]

The court reaffirmed the existence of positive obligations on states under Article 8,[1020] holding that "these obligations may involve the adoption of measures designed to secure respect for private life even in the sphere of relations of individuals between themselves."[1021] The court continued that although the choice of means of fulfilling positive obligations is, in principle, within a state's margin of appreciation, state discretion is limited by the Convention's provisions.[1022] However, the court's analysis concluded that although states have a margin of appreciation in terms of precisely how they exercise their positive obligations, the extent of their discretion is limited by the Convention. In other words, the Convention is a human rights instrument, and for the sake of "effective deterrence against grave acts, where fundamental values and essential aspects of private life are at stake, [requires] efficient criminal-law provisions,"[1023] which are reinforced "through effective investigation and prosecution." [1024] This is especially the case when the welfare of children and other vulnerable individuals necessitates criminal law protection.[1025]

The court acknowledged that states' positive obligations must not impose "an impossible or disproportionate burden on the authorities,"[1026] and noted that other counterbalancing interests should also be taken into account, i.e. guarantees of Articles 8 and 10 ECHR.[1027] Indeed, in the case at hand, an effective criminal prosecution for the breach of the child's privacy was in conflict with the interests of confidentiality on the part of Internet users. However, the latter interest cannot be absolute and is outweighed by the interests of being able to conduct meaningful criminal prosecutions.[1028]

The court concluded that although it is up to national legislators to create a regulatory framework reconciling these competing claims, in the case in question it had to be achieved in a different way. In other words, the failure of the state to provide consistent rules relating to criminal investigations, and the interpretation of its confidentiality duties, which favoured the anonymity of Internet users above child

---

[1019] Ibid., paras. 36-39
[1020] Ibid., para. 43 ("These obligations may involve the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves.")
[1021] Ibid.
[1022] Ibid., para. 44
[1023] Ibid., para. 46
[1024] Ibid.
[1025] Ibid.
[1026] Ibid., para. 48
[1027] Ibid.
[1028] Ibid., para. 49

welfare, hindered the criminal prosecution of an alleged offender.[1029] By doing so in *K.U. v. Finland*, the Strasbourg court did not simply reaffirm the existence of states' positive obligations under Article 8, but did so in a way which essentially amounted to giving state parties to the Convention guidelines as to the content of data protection rights (in the case at hand – those of a suspect whose IP address was requested) and the obligations of private parties. In effect, this may qualify as The ECHR regulating private behaviour. This is quite a remarkable step for an international treaty like the ECHR which is directly binding only on state parties when it comes. Indeed, under the law as it now stands, one cannot say that the ECHR imposes obligations on private parties which can be compared to the constitutional rights in Germany, for example, which have a horizontal or third-party effect.[1030]

However, the case-law relating to the ECHR suggests that Article 8 of the Convention not only prevents a state from introducing bad information practices, but also implies the creation thereby of rules governing the information practices of both itself and private parties. State signatories are found to be in violation of the Convention not for breaches by private parties, but for the failure to channel the behaviour thereof. This system implies the imposition of positive obligations on private parties, which must be consistent with the Convention, i.e. they must be adequate and properly reconcile Article 8 interests with conflicting claims.

Here, as well as with regard to the interpretation of Article 8 (1) in Section 3.2, a qualification is due. It is impossible to draw any general conclusions from the cases which were just considered about a general and absolute nature of state positive obligations under Article 8 (1), since, again, any generalisations about the ECHR jurisprudence should be made with caution as "the outcome of any particular case may not tell as much beyond its own facts."[1031] Moreover, the doctrine of margin of appreciation interferes into determining the scope of a protected right, and the content of a respective state positive obligation, already on the stage of analysis under paragraph 1. This requires balancing of the involved privacy interest with competing government interests and the results of such a balancing differ depending on the circumstances of the individual case. Nevertheless, the goal of this section was to demonstrate that data protection cannot be refuted as an element of the protected right to respect for private life on the principal grounds and this has been done.

[1029] Ibid.

[1030] For an explanation of how the horizontal effect of human rights in German Constitutional law works see, e.g. Basil S. Markesinis, "The Applicability of Human Rights as between Individuals under German Constitutional Law," in *Protecting Privacy*, ed. Basil S. Markesinis, *The Clifford Chance Lectures* (Oxford University Press, 1999).

[1031] Harris, *Harris, O'boyle & Warbrick Law of the European Convention on Human Rights*., p. 362

4. Waiver of the right to data protection: the limited scope of private law solutions to the data protection issue

As already mentioned, the proposals to re-examine current data protection mechanisms in Europe, and substitute or complement them with private law tools relating to contract and property, have received considerable attention in European data protection literature.[1032] The cornerstone of such proposals is the opportunity for an individual to either trade data pertaining to him for money or services, or waive his data protection rights on the basis of market conditions. The position of this study is that the waiver of (and, hence, the unlimited private law approach to) data protection rights is only possible if one is deprived of the protection of a fundamental right to privacy. This work has, however, shown that privacy, as protected by Article 8 ECHR, is a much wider right, which extends beyond a negative interest in protecting secret information, to a positive right of personal development (and possibly even information self-determination), along with affirmative obligations imposed on a state to secure data protection interests effectively.

This section challenges the claim made by some authors that since data protection is not a fundamental right, freedom of contract takes precedence over the rules of the 1995 Data Protection Directive and the right to data protection may be waived or contracted around.[1033] It has already been argued earlier herein that there are no sufficient grounds for divorcing the legal right to data protection from Article 8 ECHR privacy. The next step in the reasoning is to demonstrate that the Convention does not contain the right, in the fulfilment of freedom of contract, to waive data protection interests for remuneration.

It must first be acknowledged that, although not mentioned in the text of the Convention, the phenomenon of the waiver of rights is known to the ECHR system. In fact, there are two lines of jurisprudence on this matter. Firstly, Article 6 ECHR (right to a fair trial) case-law confirms that, in their defence, contracting states may rely on the waiver by applicants of their rights guaranteed by the Convention, provided that the waiver was well-informed, unequivocal, given freely, and does not contradict public interest.[1034] However, whether individuals may seek the Convention's protection when a state interferes in market transactions involving the waiver of a protected right is an entirely different matter, and, it is argued herein, should be answered in the negative. The latter issue is addressed by the Strasbourg court in the second type of authority on the application of Article 1 of the First

---

[1032] See Chapter 8

[1033] Cuijpers, "A Private Law Approach to Privacy: Mandatory Law Obliged? ."

[1034] For more detailed analysis of the ECHR case-law on waiver see De Schutter, "Waiver of Rights and State Paternalism under the European Convention on Human Rights.", referring, *inter alia*, to *Bulut v. Austria*, Application No. 17358/90, Judgement of 22 February 1996, para. 30, *Deweer v. Belgium*, Judgement of 27 February 1980 published in Ser. A, Vol. 35, p. 56, etc.

Protocol to the Convention.[1035] It is this line of case-law that the following passage will focus on.

The first part of the argument is that the Convention, unlike the EU law considered in Chapter 8, does not in general guarantee the freedom of contract, or any other economic freedom, except in so far as it relates to property.[1036] What is more, De Schutter asserts that the right to the peaceful enjoyment of possessions that is protected by Article 1 of Protocol 1 does not implicitly guarantee the freedom of contract.[1037] De Schutter bases his conclusion on the Mellacher judgement of the European Court of Human Rights.[1038] The facts of this case were that the Mellachers and others filed a complaint against Austria. The applicants were all owners of apartments which they rented out. In 1981, the state of Austria introduced a law limiting the maximum rent for such properties on the basis of their quality. As a result, the amount of rent that the applicants received was reduced dramatically. The Mellachers and others claimed that the state's intervention amounted to the deprivation of their possessions, or at least a violation of the right to receive payment of the agreed rent in violation of Article 1 Protocol 1. The court disagreed:

> *The Court finds that the measures taken did not amount either to a formal or to a de facto expropriation. There was no transfer of the applicants' property nor were they deprived of their right to use, let or sell it. The contested measures which, admittedly, deprived them of part of their income from the property amounted in the circumstances merely to a control of the use of property.*
>
> *The fact that the original rents were agreed upon and corresponded to the then prevailing market conditions does not mean that the legislature could not reasonably decide as a matter of policy that they were unacceptable from the point of view of social justice.*[1039]

[1035] Article 1 of the Protocol – Protection of property – reads as follows:

> "Every natural or legal person is entitled to the peaceful enjoyment of his possessions. No one shall be deprived of his possessions except in the public interest and subject to the conditions provided for by law and by the general principles of international law.
>
> The preceding provisions shall not, however, in any way impair the right of a State to enforce such laws as it deems necessary to control the use of property in accordance with the general interest or to secure the payment of taxes or other contributions or penalties."

[1036] Bernhard Wegener, "Economic Fundamental Rights," in *European Fundamental Rights and Freedoms*, ed. Dirk Ehlers (Berlin: De Gruyter Recht, 2007)., p. 148.

[1037] De Schutter, "Waiver of Rights and State Paternalism under the European Convention on Human Rights.", p. 505.

[1038] ECHR 19 December 1989, *Mellacher and Others v. Austria*, Application No. 10522/83 ; 11011/84 ; 11070/84.

[1039] *Mellacher*, paras. 44, 56.

De Schutter correctly interprets the Mellacher decision as meaning that "the protection afforded by the Convention to the property […] does not extend to the right to exchange that property against some other advantage, under the conditions reigning in the market."[1040] The same, he also claims, is true for the other rights and freedoms guaranteed by the Convention, including the Article 8 right to privacy:

> *[T]he right one has to freedom of expression or to respect for private life does not extend to the right to obtain, under the mechanisms of the market, a remuneration for the sacrifice of that right, or even for agreeing to that right being limited in some less complete way.*[1041]

To summarize, both case-law and doctrine suggest that the ECHR does not protect an individual's right to obtain remuneration, under reining market conditions, for forgoing a fundamental right. This means that although a state respondent in its defence may rely on the fact that an applicant waived the right in question, an individual cannot claim that his right was violated when the state prevents him, e.g. via regulation, from waiving a fundamental right.[1042]

An important remark must be made here. This study does not argue that contractual arrangements concerning personal data, or the propertisation thereof, are completely impossible under the Convention. However, it is argued that the classification of data protection as a fundamental right protected under Article 8 ECHR limits the scope of the contractual arrangements and possible property rights that are allowed. To understand this point better, one has to consider the content of the right being discussed here. Data protection does not mean the complete non-disclosure and total secrecy of personal information. As Gutwirth and De Hert explained in the piece mentioned earlier, data protection is not a defensive but a transparency tool. It does not prohibit a state (or other body) from collecting information, but rather channels and controls it by giving an individual positive rights and imposing on a state affirmative obligations.[1043] Only one example of a tool which channels information practices in the 1995 Data Protection Directive is the requirement to obtain the consent of a data subject. The ban on the waiver of data protection rights does not mean that there is a ban of the voluntary exchange of personal information for money, goods, or services, but is instead a prohibition of the giving away for remuneration the right to consent, to name just one example. Accordingly, the commercial exchange of personal data is not, in principle, outlawed.

[1040] De Schutter, "Waiver of Rights and State Paternalism under the European Convention on Human Rights.", p. 506.
[1041] Ibid.
[1042] Ibid.
[1043] De Hert, "Making Sense of Privacy and Data Protection: A Prospective Overview in the Light of the Future of Identity, Location-Based Services and Virtual Residence in the Institute for Prospective Technological Studies: Report Eur 20823 En.", p. 144.

However, treating data protection as anything less than a fundamental right under Article 8 ECHR will lift the restrictions which follow from the fundamental right status, and will allow the complete waiver of a right, thus opening the door to a dramatic change in approach to data protection. Whether the European approach to personal data protection will become in any way better if a market approach thereto (by contract or the propertisation of personal information) is adopted is another issue entirely.

5. Conclusion

This chapter has demonstrated how the legal categories of privacy and data protection correlate in the European legal system, and has also revealed what the effects of such a correlation are on a particular mode of data protection. Since the norms of EC data protection law did not provide a conclusive answer, this work turned to the ECHR for guidance. As a roadmap for the analysis herein, the dichotomy between privacy and data protection based on negative rights and positive obligations, as explained by De Hert and Gutwirth, was utilized. The analysis of Article 8 case-law led to the conclusion that the European Court of Human Rights does not limit the application of Article 8 to only the private sphere, while the provision on privacy protection has been applied as giving individuals positive rights (for instance, to refute false information about oneself) and imposing affirmative obligations on states to create and ensure the functioning of an effective data protection system. The conclusion was reached that the European legal approach treats data protection as a privacy interest.

Moreover, it has also been shown that the legal recognition of such a close relationship is much more than just a matter of conviction based on the philosophical meaning of privacy. The protection of personal data benefits significantly from the enjoyment of its status as a fundamental right, and the removal of data protection from the scope of privacy rights is neither necessary nor desirable. Firstly, the development of ECHR case-law has extended the protection of privacy beyond a negative right against state intervention to include affirmative obligations on a state to create a data protection system. Moreover, treating data protection as anything less than a fundamental right under Article 8 would enable its waiver and, thereby, open the door to an unnecessarily and undesirably dramatic change in the European approach to data protection.

Chapter 10: The property rights solution[1044]

1. Introduction

This chapter completes the discussion of the European perspective on the idea to introduce property rights in personal data. Following the conclusions reached in Chapters 8 and 9 on the possibility of propertisation in the European legal order, this Chapter examines whether the introduction of property rights in personal data is not only possible, but also has the potential to make a positive difference in how the personal data problem is tackled given the recent changes in the personal data flow. More precisely, according to the logic of legal pragmatism, the propertisation of personal data is only justified when it addresses the data processing problem more fully, or in a way that is better in other respects, than the data protection mechanisms already in existence. Chapter 7 has revealed that the approach currently employed in Europe to tackle the problem is not effective, especially so far as transparency and accountability are concerned. The operation of the European data protection mechanism leaves room for improvement which is sufficient to consider a principally new approach to assigning accountability for data protection matters, monitoring and enforcement of the data protection standards, as explained in Chapter 7. Indeed, depending on the view one takes on the development of data protection laws, such a new approach may also be regarded as a possible fifth generation of the data protection regime. The final piece of the puzzle for this chapter to examine is the issue of whether the introduction of property rights in personal data would actually make sense from the legal pragmatism perspective. In other words, in comparison to the mechanisms already in place, would property rights be a more effective way of addressing the personal data problem?

The position of this study leads to the conclusion that in the age of cloud computing, chain informatisation, and ambient intelligence, a property rights regime, combined with non-property regulation not only deserves a second look but might even capture, and hence channel, new and otherwise difficult to control relationships with regard to personal data. Section 2 will demonstrate how this is possible thanks to the *erga omnes* effect of property rights. Meanwhile, Section 3 will deal with the limitations of the propertisation solution as a data protection tool, and Section 4 will

---

[1044] Earlier versions of the argument made in this chapter may be found in Nadezhda Purtova, "Property in Personal Data: Second Life of an Old Idea in the Age of Cloud Computing, Chain Informatization, and Ambient Intelligence," in *Privacy and Data Protection. An Element of Choice.*, ed. Paul de Hert, Gutwirth, Serge, Poullet, Yves (Springer, 2011-forthcoming). The original publication is available at www.springerlink.com.

address some loose ends, i.e. various other questions often raised in discussions of property rights in personal data.

2. What propertisation offers

As Chapter 7 has established, the data protection community is generally satisfied with how the substantive data protection principles tackle most data protection concerns.[1045] However, the major weakness of the current approach lies in its implementation mechanisms. Accordingly, the analysis in this Chapter will focus on how the introduction of the property rights may improve the system of implementation.

2.1. Property rights as a framework for personal data management that is respectful of information self-determination

From the perspective of an individual's rights, what the propertisation of personal data can offer to the data protection cause, in the complex conditions of the modern data flow, is to create a coherent and more articulate framework for personal data management that is respectful of the principle of information self-determination.[1046] This is consistent with the protective as opposed to the market function of property rights as outlined in Chapter 4.[1047]

As already established in Chapter 8, the principle of information self-determination is understood as "the capacity of the individual to determine in principle the disclosure and use of his/her personal data."[1048] Although this principle already constitutes one of the fundamental elements of the current European data protection regime, its role and application are not set out clearly enough. This lack of clarity is particularly visible in discussions of the role of the consent requirement among the other conditions of legitimate data processing.[1049] According to some commentators, the consent requirement has no normative priority[1050] and is but one

---

[1045] Chapter 7, section 2.3.1.

[1046] The author is of the opinion that property can perform the same function with regard to other cases of self-determination, e.g. regarding body parts in general and reproductive material in particular. However, although many analogies with the body parts' regime are possible, this study does not go further than making the case for property rights in personal data.

[1047] Chapter 4, section 3

[1048] de Hert, "Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalization in Action.", p. 14

[1049] See Chapter 8, Section 3.1.3.

[1050] Bygrave, "Consent, Proportionality and Collective Power.", p. 165-166. See Chapter 8, Section 2.1.3 (b)

of a number of equal and alternative preconditions of the processing of data.[1051] The data protection authorities advise against reliance on consent as the sole legal basis for such processing, except where "it is absolutely necessary."[1052] Simultaneously, in a small number of jurisdictions, a default rule is that a data controller must obtain the data subject's consent to the processing of his personal information, and this has been interpreted as giving priority to the consent requirement.[1053] The position that this study takes is that, from the perspective of individual rights adopted by the author, the principle of information self-determination and the consent requirement should have a normative priority, and be regarded as a default rule of data processing, unless the law provides otherwise. This will reaffirm a normative statement already made in Europe that the individual should always retain some degree of control over what is happening with regard to his personal data.[1054]

One important disclaimer should be made at this point. The thesis on the normative priority of information self-determination is in no way meant to imply that the consent rule should be the only condition to legitimate data processing. Since the current rules provide for a number of alternative conditions, such as authorization by law,[1055] the propertisation approach defended in this study only regards consent as a default rule, which can be limited by provisions of law or contract. Indeed, disagreement on the interpretation of the existing relationship between consent and the other conditions to legitimate data processing is, in its nature, quite similar to the dilemma over whether a glass is half-empty or half-full; the side one takes is a matter of attitude and does not have any impact on the quantity of liquid in the vessel. At the same time, the side chosen does reflect whether the individual is a pessimist or an optimist. Similarly, in the case of consent and the other preconditions to data processing, whether the consent rule has or does not have a normative priority should not, theoretically, have an impact on the scope of the data processing that is permitted. However, when priorities are not unequivocally set out in favour of consent, it enables the interpretation of other, often vague and inclusive, preconditions to the processing of data, as if they have a priority over information self-determination. For instance, Article 7(f) of the Directive allows data processing "for the purposes of the legitimate interests pursued by the controller […], except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1(1)." The way in which this provision has been formulated clearly requires

---

1051 ———, *Data Protection Law: Approaching Its Rationale, Logic and Limits*., p. 66

1052 Kuner, *European Data Protection Law: Corporate Compliance and Regulation*. (e.g. WO, 'Working document of the surveillance of electronic communications in the workplace' (WP 55, 29 May 2002) 21)

1053 Bygrave, "Consent, Proportionality and Collective Power."

1054 For a detailed explanation of the European standpoint on information self-determination, see Chapter 8, Section 3.1.3.

1055 See, e.g. the conditions of legitimate processing in Articles 7 and 8 of the 1995 Directive.

interpretation, namely, the balancing of any legitimate business interests, such as making a profit, with data protection rights, such as consent. As Kuner explains, the various member states conduct this balancing act differently and "data controllers must examine local law in detail to determine if the exception applies."[1056] From this it follows that some member states may come down on the side of business interests. This study maintains that such an interpretation contradicts the established normative foundations of the European data protection approach and should therefore be prevented by, *inter alia*, making the consent rule a default requirement for legitimate data processing. This consent by default would shift the burden of proof to a controller, who must demonstrate that his interests, and not the information self-determination right of the data subject, should prevail in a particular case. The proposed shift towards the consent rule as default can be achieved by means of the propertisation of personal data.

To achieve greater insight into how the property regime could grasp the complexity of the modern relationships vis-à-vis personal data, and form a regulatory framework for the data flow that is respectful of the leading role of the information self-determination and consent, it is helpful to look at the system of English land law. Chapter 4 has already explained the English system of real rights in land. Briefly, English land law governs what a continental lawyer would call 'property rights in immovables'. Like personal data, land is a valuable resource that is transferred to multiple actors, who put it to many uses.[1057] To accommodate these uses, and grant protection to respective interests in land, modern land law developed into a pyramid-like system of rights and interests, with the right with the widest scope - fee simple - at the bottom, and leases – property rights of a narrower scope – at the top.[1058] The content of these rights has been tailored to account for the most popular uses of land, and, according to the principle of *numerus clausus*, no other rights in land, save for those on the list, receive *erga omnes* protection.[1059] The transfer of leases – the 'lesser' rights in a piece of land - does not undermine, although it does limit, the 'greater' right of fee simple. However, at all times, until the fee simple is transferred in full, its holder retains some control over his property, e.g. the right of access in order to maintain an object of property rights in a proper state.

In a search for this quality, namely the capacity to exercise control over a transfer and retain some control thereafter, a similar system of property rights could

---

[1056] Kuner, *European Data Protection Law: Corporate Compliance and Regulation*., p. 76

[1057] Chapter 4 has shown that in modern property law whether an object is physical, like land, or intangible, like personal data, does not matter.

[1058] As well as common law rights in land (property in law), there are also rights in equity developed by the courts within the English system, albeit by those of a different jurisdiction (e.g. covenants prohibiting a certain use of land for future buyers). It is not, however, the purpose of this chapter to go into the details of English land law.

[1059] As Akkermans explains, there is a slim chance of the inclusion of a new right on the list of property interests. Akkermans, *The Principle of Numerus Clausus in European Property Law*.

be built around personal data. An individual – the data subject – could be said to have the widest property right possible (although it would not be unlimited), including a right to transfer his personal data for remuneration (known as a right to 'sell'). The most important limitation on the possible scope of this right would be a prohibition on the waiver of the data protection guarantees, e.g. consent.[1060] On this basis, it would not be possible for this right to be completely alienated. The element of the rights relating to personal data being transferred from a data subject to data controllers and processors is comparable to leases in land law; the alienable 'leases' in personal data could be tailored to reflect most common practices with regard to personal information, and could also vary in type, depending, for instance, on the duration and purpose limitations thereof, e.g. excluding the use of the data for profiling. These 'leases,' like those in land law, could also be transferable, and in this way their introduction would be a response to the calls of the information industry to protect their investment in collecting data by recognizing their property rights; the system of 'leases' would protect the investments (by granting *erga omnes* protection, including against data security breaches). Moreover, pursuant to the principle of *numerus clausus*, recognizing only a closed list of 'lesser' property rights in personal data would be one step further along the road to ensuring that, as often happens now, individuals are not forced into relinquishing total control over their personal information. At present this is often done by service providers by giving individuals a choice to either provide their data or be unable to use certain services which are difficult to do without, e.g. an email account or a plane ticket.[1061]

Further transfers of personal data within a cloud or a chain could take the shape of the transfer of – also 'lesser' – property rights or contractual relationships. It would be a matter of policy as to whether actors other than a data subject should be permitted to enjoy property rights over personal data, or whether a situation in which the individual is the only holder of property rights over his personal information should be maintained. In the latter case scenario the exercise of transfers from one actor to another will be on the basis of a contract. The view of this study is that, based on the pragmatic application of the *numerus clausus* principle, such a decision should depend on whether or not a policy-maker wants to support the interests of the information industries with *erga omnes* protection, e.g. protecting their investments in building databases that are free from security breaches and data leaks. If this latter scenario is preferred, it could be implemented via a system of licences (a possible type of the 'lesser' property rights in personal data), the content of which could be tailored to match the specificities of particular sectors and could vary in terms of validity, permitted usage, limitations on further transfers, etc. The

[1060] For more on the limitations on the alienability of personal data, see Chapter 9 on the permitted scope of propertisation.

[1061] See Brownsword, "Consent in Data Protection.", pointing out such a shortcoming of the consent requirement.

content of these specific licences could be determined in co-operation with the relevant industries and DPAs, as well as with representatives of data subjects. Such a system of property rights could, in theory, be implemented through the use of so-called 'sticky technologies' which enable the rights relating to a piece of data to 'travel' with it and verify the legitimacy of a particular data processing operation.[1062]

2.2. The erga omnes effect given to data protection rights holds all actors accountable

The first and probably the most important effect of the propertisation is that it would tackle the inequality that currently exists between various actors in terms of their accountability for what they do with personal data. In other words, the *erga omnes* effect of property rights would ensure the same degree of accountability for every actor involved.

It has been asserted earlier in this study that the 'data subject - controller' model of accountability implied in the 1995 Directive does not account for the new complexity of relationships within the modern flow of data.[1063] In brief, data protection obligations are effectively only imposed on, and are only enforceable against, one group of actors involved with personal data, namely the data controllers. This means that other actors, who are either difficult to identify or do not fit into the Directive's rigid definition of a controller, despite being involved with an individual's personal data, are not held to account over the violations they may be involved in. It has thus been established that the 'data subject – data controller' model should be substituted with a 'data subject - entity in possession of personal data' relationship.[1064] The introduction of property rights with the *erga omnes* effect does precisely this.

As the reader may recall from Chapter 4, the *erga omnes* effect is a feature which distinguishes property ('real') rights from personal rights[1065] and, in the author's opinion, should be the defining element of the pan-European discourse on property.[1066] The *erga omnes* effect means that property rights have an effect against everyone by imposing negative obligations on an unidentifiable number of people without their consent.[1067] In contrast to the limited effects of the current data protection obligations, the transformation of rights relating to personal data into

---

[1062] E.g., see Cohen, "Examined Lives: Informational Privacy and the Subject as Object.", p. 1391

[1063] See Chapter 7

[1064] Chapter 7, section 2.3.2.

[1065] Personal rights create obligations only for the parties to a contract. Bartels, *Content of Real Rights*.; Milo, "Property and Real Rights."; Van Erp, "From "Classical" To Modern European Property Law?."; Gray, "Property in Thin Air."

[1066] See Section 3.3.3 of Chapter 4

[1067] Van Erp, "From "Classical" To Modern European Property Law?."

property rights by attributing the *erga omnes* effect thereto would eliminate differences in accountability between data controllers and data processors or other non-controllers. It would do this in such a way that maintaining a legal division between a data controller, processor and other actors would no longer make sense. All categories of actors, or better still all of the actors potentially or actually involved with personal data, would be bound by a negative obligation to respect the rights of a data subject regarding information pertaining to him.

By way of example, imagine yourself walking down the street and seeing your face on a billboard advertising, say, a local rehab for drug and alcohol addicts. After recovering from the shock you vaguely remember the party where that not flattering picture of you could have been taken, a series of e-mails to everyone who attended the party circulating this and other photos of you, and your cousin posting the photo on his profile at the social network site. Who is responsible for the public appearance of the photo is not clear. However, it is not your burden to discover how the picture made it to the billboard. Due to the *erga omnes* effect of your property right in your image, anyone involved with the photo is accountable for its unauthorised use. Therefore, you approach the advertising agency, or the owner of the billboard – whoever is easy to establish as an involved party.

In this way, the propertisation of personal data not only clarifies the obligations of the actors involved, but also addresses the challenge of the opacity of the modern data flow, at least when it comes to identifying those who are accountable. More specifically, whatever the position of any given actor is within an information chain of any degree of complexity, he would be expected to make sure that his actions are not in violation of an individual's, or another actor's, property rights in personal data. As a result of propertisation, handling personal data in any way would be prohibited unless the holder of the property rights, or the law, stipulates otherwise. Accordingly, the burden of finding the right actor to initiate proceedings against is removed from the data subject. In other words, when there is a violation of data protection principles, there would be no need for a data subject to identify the particular violator in an information chain; action could be taken against any actor involved with the piece of data in question (whatever the extent of this involvement) if it is unclear precisely where the data protection regime was violated and which actor was 'at fault.' Moreover, action could even be taken against the actor who was 'caught' using the personal data in question without proper authorization. The burden of ensuring that data transfers occur without violations would be on each and every actor 'in the cloud' or 'in the chain', as would accountability in general and liability for damages. The resulting mechanism would resemble the distribution of accountability in product liability.[1068]

[1068] E.g. the Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective

The property mechanism could also be of particular relevance in the context of transborder data transfers to countries outside EU. While contemporary discourse is occupied with discovering better ways to ensure the existence of the desired level of data protection beyond the borders of the EU, *inter alia*, by means of binding corporate rules, the propertisation solution may offer a ready answer. Regardless of the arrangements between EU and non-EU actors, or the national differences in approach to and level of data protection, in the case of a violation of his data protection rights, and if a non-EU actor at fault is beyond jurisdictional reach, a data subject could address his claim to the EU-based actor to whom he disclosed the relevant data in the first place, letting one sort out the burden of responsibility with the other (non-EU actor). After paying the appropriate damages, the actor in question would have the chance to search further 'down the chain' for the source of the violation. The resulting system would resemble the current system of enforcement of the binding corporate rules. When applying for authorisation of a transborder data transfer, a corporate group appoints a EU-based lead member of the group to be responsible to a national DPA and for the compliance of the other members and liable for damages.[1069] The difference, however, is that the propertisation system will spare the administrative burden of drafting the BCRs and having them approved by a DPA. Besides, the binding effects of property rights will extend far beyond one corporate group and the erga *omnes effect* and *nemo dat* rule wil be far more accessible and transparent to the data subject than the BCRs at times can be.

2.3. Co-regulation and self-control

The clarity of an obligation to 'stay away from personal data unless explicitly allowed otherwise', which would be imposed on every involved actor by propertisation, would remove the confusion arising from the controller–non-controller dichotomy. It would also positively affect the motivation and capacity of actors and their data protection officers to comply with data protection standards. However, propertisation may also have other positive effects on participatory implementation in the form of co-regulation and self-control.

In particular, propertisation could tackle the limited effects of the contractual instruments of co-regulation. As Chapter 7 explained, the relationships between the various actors involved with personal data, as well as their respective rights and obligations, including the implementation of the substantive data protection principles and the distribution of accountability, are often governed by agreements

---

products [Official Journal L 210 of 07.08.1985] creates strict product liability, i.e. liability without fault, for damage arising from defective products.

[1069] See Working Party documents on the BCRs, e.g. Working Document Setting up a framework for the structure of Binding Corporate Rules, 24 June 2008, WP 154

which are, essentially, contracts. Examples range from *ad hoc* contracts between a data controller and a processor, to the agreements regulating more complex business relationships. However, the downside of contracts is that they are binding only on the parties thereto and do not as a rule give any rights to data subjects.[1070] For instance, even though a processor might be obliged by a contract with a controller to ensure data security and respect other data protection principles, in the case of a violation of these obligations a data subject cannot claim an infringement of his rights by the processor; only the controller can claim a breach of contract. However, when transformed into property rights, data protection rights will always provide a legal basis for a data subject's claim against any actor involved with his personal information. This is because these rights would be effective against the world.

Propertisation also has the potential to tackle another shortcoming of co-regulation and self-control, opacity. An example is the case of the Dutch transport companies involved with the OV-chip card,[1071] since the agreements between the various data processing actors about the distribution of obligations and accountability are not always obvious to data subjects or even supervisory authorities. The introduction of property rights in personal information would mean that the opaque arrangements between the data processing actors were irrelevant. Firstly, from the perspective of accountability, the data subject would not need to base his claim on any agreement between third parties, since the property right he would have over his data provides a ground for action by default. Secondly, and regardless of how an agreement between data processing actors distributed their control over an individual's personal data, as a result of propertisation the data subject would always have certainty that, legally, no-one has greater rights over the data in question than he has granted to them.[1072]

Finally, in the context of international data transfers, Kuner points out that drafting *ad hoc* contracts for each might be too burdensome and confusing as "the applicability [of such contracts] must be determined for each particular data

---

[1070] This follows from the principle of privity of contract. It is true that the application of this principle in some jurisdictions is less strict. For instance, the English Contracts (Rights of Third Parties) Act 1999 has as its main purpose to enable third parties equire rights under a contract "if and to the extent that the parties so intend" (Guenter Treitel, "Contract: In General," in *English Private Law*, ed. Andrew Burrows (Oxford University Press, 2007)., p. 735, para. 8.303). However, such a third party effect in scale cannot be compared to the *erga omnes* effect that the real (property) rights have. First, because third parties do not have a claim that follows from the nature of a right in question. The third-party effect has to be established either by parties (s. 1 of the Act) or by statute (e.g. rights against insurers (1930 Rights Against Insurers act) (Treitel, "Contract.", p. 739). Second, the range of the third parties who can have rights this way is limited (an additional beneficiary has to be named in the contract or statute (Ibid., p. 735)). Once a right that derives from a contract gains the *erga omnes* effect, it is doubtful that it is, in substance, a personal right and not a property right.

[1071] See Chapter 7, section 2.3.2 (a)(i)

[1072] An individual cannot transfer more rights than he has and deny the title to the owner pursuant to the *nemo dat* rule (see Chapter 4, Section 4.3.3.1).

transfer."[1073] The property rights regime has the potential to satisfy Kuner, who suggests that "a more integrated, holistic approach" to the corporate treatment of personal data is needed "without concluding a set of contractual clauses among all their corporate entities."[1074] In other words, data transfers can be exercised not on the basis of *ad hoc* contractual arrangements that have to be affirmed by the supervisory authorities each time, but on the basis of types of licences of the content which are predetermined by a legislator. The system of licences, not unlike model contracts, would address both the challenge of too heavy a bureaucratic burden and the fear that the information industry's self-interest would take over the mechanisms of co-regulation and self-control. The bureaucratic burden would be reduced because data processing actors operating on the basis of licences would not need to have their contracts checked before each data transfer. Moreover, self-interest would be prevented from dominating because the influence of the industry would be limited to the stage of cooperating with a legislator in developing a sector-specific licence.

2.4. Improved top-down implementation

Propertisation would also be expected to contribute to the quality of the top-down implementation of the substantive data protection principles, primarily by bringing clarity to the system of rights and obligations and dotting the i's and crossing the t's with regard to determining who the accountable actors are. Moreover, it is likely that monitoring and enforcing compliance with data protection standards would be easier for supervisory authorities once the burden of conformity is clarified.

However, there are other benefits, too. For instance, the impact of propertisation on the opacity of the data transfers described in the preceding paragraphs and sections should reduce the resources required for monitoring and compliance. What is more, if a system of fragmented ownership and licences is introduced, the DPAs would be required to exercise their advisory function towards businesses on a much smaller scale. Indeed, the DPAs currently have to both deal with a body of abstract notions in need of interpretation and apply these same notions to the circumstances of individual sectors. Propertisation, in contrast, would produce a system of data protection standards expressed in a clearly defined scope of property rights, clearly demarcated scopes of licences defined by term of authorised data processing, as well as a purpose. The abstract norms and notions would still be in play, but at the level of a legislator working in cooperation with the DPAs and the industry to create the appropriate types of licences. As the advisory function of the DPAs became less prominent, the conflict between the various functions of the supervisory authorities should decrease too.

[1073] Kuner, *European Data Protection Law: Corporate Compliance and Regulation*., pp. 218-19
[1074] Ibid., pp. 218-19

By way of example, if property rights in personal data are introduced, every random piece of personal data that an organisation possesses or has access to will have to be accompanied by a licence and will have to be stored, used or transferred strictly within the scope of authorisation of the licence. This follows from the application of the basic rule of property to the context of data processing, namely, that one cannot transfer more rights than one has and deny the title to the owner (*nemo dat*). There are at least two advantages of this system. First, organisations themselves, at least, those acting in good faith, will be enabled and motivated to keep track of the presence, scope and term of the licenses containing relevant authorisations, much like they do now with patents and copyright. This will trigger creation of organisational rights management systems and use of privacy by design facilitating compliance from the first stages of data processing rather than creating emergency checks few days before audit of a data protection authority takes place. This is quite similar to the principle of accountability recently proposed by the Commission and Working Party as a new basic principle of data protection.[1075] The second advantage is that enforcing compliance with such a system will be less demanding on the DPAs as, thanks to the organisational nature of the measures organisations would have to take to ensure a valid authorisation is present, or, put differently, respect for data protection rules inbuilt into the organisational structure, compliance or non-compliance with the data protection rules will much more transparent: simply put, either there is a licence or there is not. A possibility of random audits by DPAs and high fines would provide incentives to comply for the bad faith actors.

3. Limits of propertisation: the necessity of additional regulation

Several times in the course of the argument contained herein a claim has been made that property in personal data, *complemented with regulation*, would be able to achieve the desired level of control over the modern data flow. Introducing property rights alone is not enough and regulation is necessary.

A minor reservation with regard to propertisation is that it is a tool aimed at providing an individual with greater control over his personal information. However, a feature of the modern personal data problem is the fact that thanks to profiling and the excessive availability of personal data, an individual does not need to reveal his personal information to be subjected to personal data related treatment, such as price discrimination. As long as there is enough data available about people

[1075] Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions "A comprehensive approach on personal data protection in the European Union" of 4 November 2010 and Working Party Opinion 3/2010 on the principle of accountability (WP 173)

like the individual in question to create a profile, a very small piece of information, like an IP address, is enough to identify a citizen or a consumer with a particular group and treat him accordingly.[1076] Regulation - as a supplement to propertisation – may thus be a better way of addressing this collective dimension of the personal data problem. Nevertheless, propertisation is able to make some contribution to regulating profiling practices. Firstly, propertisation may limit the collection and use of personal data for profiling or discrimination purposes to reduce the pool of data available for building profiles. Secondly, propertisation will be able to limit access to and use of a piece of personal data that is needed in order to tie an individual to a profile, such as an IP address or a date of birth.

The main limitation of the notion of propertisation is that by virtue of its *erga omnes* effect it only carries negative obligations, e.g. not to process personal data unless permitted by a data subject or otherwise provided by law. Simultaneously, positive obligations are a vital aspect of data protection.[1077] This is where the idea of propertisation of personal data can clearly benefit from further regulation introducing positive obligations. At the same time, such principles of data protection as data minimality that requires proportionality, necessity, non-excessiveness or frugality as regards to the quantity of data processing,[1078] may as well be accommodated by the systems of licences which scope may be limited by the purposes and period of authorised processing.

4. Additional Qualifications

This section addresses some of the loose ends relating to the idea of propertisation that the author has come across during discussions, conferences, or workshops, and which are difficult to classify under any of the headings above but are too important to be disregarded in the analysis. This section will be built around short questions or queries and brief responses thereto.

4.1. How does the propertisation solution relate to other proposed solutions?

Often during conferences and workshops members of the audience react to the presentation of the idea of the propertisation of personal data with a question about how it relates to the existing data protection model. In other words, and using Burkert's classification, does propertisation reform the principal basis of data

[1076] Lessig, *Code 2.0*. at 217
[1077] de Hert, "Making Sense of Privacy and Data Protection: A Prospective Overview in the Light of the Future of Identity, Location-Based Services and Virtual Residence in the Institute for Prospective Technological Studies: Report Eur 20823 En."
[1078] Chapter 7, section 2.2.1(b)

protection by making only minor changes to the data protection mechanism on the same principal grounds, or does it contribute to resolving the data protection problem caused by technology?[1079] A sub-question is: can the same results be achieved by simply making the Directive's obligations apply to non-controllers as well?

In brief, the answer is that, as has been demonstrated in this chapter and Chapters 8 and 9, propertisation does not aim to change the substantive data protection principles. On the contrary, it relies on them, with the principle of information self-determination being an example. Consequently, the propertisation solution belongs to the final two groups of reform proposals, combining changes to one segment of the current data protection regime and using technology to implement them.

The answer to the sub-question is yes. Similar results can be achieved by eliminating the differences between the data protection obligations imposed on the various types of actors distinguished in the Directive. However, such reform would effectively achieve quasi-property rights; they would not be labelled as such but would function in exactly the same way via the effects they have on the rest of the world. Moreover, it was not the aim of this study to argue that propertisation is the best or the only possible way of creating a regulatory regime for personal data. Nwambueze when defending his "remedial framework" of property in dead bodies, body parts and reproductive materials, refers to the work of Nedelsky and her standpoint on property that "the choice of legal categories [property vs regulation – N.P.] is strategic and there is nothing in one category that makes it inherently better than the other."[1080] Consistent with the earlier statements made about the pragmatic nature of law, "the regime of property is adopted on the basis of its practical utility compared to the other frameworks."[1081] Provided the political will is there, propertisation and regulation could achieve roughly the same results.

Formal propertisation, though, may still have its competitive advantages. Proponents of Lessig would mention the rhetorical effect of the word 'property.' Indeed, it is possible that the introduction of propertisation would heighten the interest that people have in their data protection rights. However, no conclusions can be made without empirical research being conducted on the influence of property rhetoric.

Among the factors making formal propertisation less practical is the possible unwillingness of national governments, especially in continental Europe, to change their traditional property laws, even more so when they are under international or

---

[1079] Herbert Burkert, "Towards a New Generation of Data Protection Legislation," in *Reinventing Data Protection?*, ed. Serge et al. Gutwirth (Berlin: Springer, 2009).

[1080] Jennifer Nedelsky, Property in Potential Life?, p. 44, cited in Nwabueze, *Biotechnology and the Challenge of Property*., p. 39-40

[1081] Jane Churchill, Patenting Humanity at 281 cited in Ibid., pp. 40-41

supranational pressure to do so. This reluctance has been demonstrated during the debates on Article 295 of the TEU and Article 1 Protocol 1 of the ECHR. Nevertheless, the goal of the contribution herein was merely to take a second look at the idea of property rights in personal data in view of the new challenges posed by information technology.

4.2. What if a data subject changes his mind about the transfer of a 'lesser' property right in his data?

Pursuant to the principle of information self-determination, the withdrawal of consent should be possible at all times, unless such an act is limited by law in a manner consistent with the human rights standards, established, for example, in Article 8(2) of the ECHR, that are necessary in a democratic society to achieve a legitimate goal. Given that the scope of property rights can be tailored by lawmakers depending on what propertisation is intended to achieve, it would be understandable if the 'lesser' property rights given, e.g. to the information industry, would be limited by the capacity of an individual to 'seek the return of his data', possibly with some sort of compensation to be paid to the relevant data processing actor, the amount and manner of which could be determined by a regulator.

4.3. Would propertisation make data protection easier in practice?

The criticism that the notion of propertisation often faces is that instead of making the control of personal data easier, it would instead place an unbearable burden on an individual to confront the information industry on a much more frequent basis, resulting in a high cost of both time and resources.

The position of this study is that individuals already deal with the information industry on a daily basis now, although they may not always realize this. It may indeed appear that the individual would have to make decisions with regard to his data more often if property rights therein were introduced. However, Chapter 7, in the sections concerning consent, and Chapter 8, in the sections about information self-determination, explained that absolute reliance on the decisional capabilities of an average individual is never without its drawbacks. Nevertheless, this burden can be relieved and the individual can be helped to negotiate and make decisions with the use of technology, e.g. PETs and TETs, as well as with legal tools, for instance with the improved application of the consent requirement via the collective exercise thereof, as suggested by Bygrave et al.[1082]

[1082] Bygrave, "Consent, Proportionality and Collective Power."

4.4. What about personal data created by other people?

Another common question concerns how the theory of the propertisation of personal data would treat personal information created by other people, e.g. conclusions, opinions, results of analysis, and observations of bystanders.

The answer to this question can be given with a reference to Chapter 4 of this study. The theory of propertisation offered herein in no way denies the legitimate claims of other actors involved with personal data. Moreover, these claims reflect the logic that the nature of property rights is not absolute and, in property language, they could be regarded as a servitude or easement, which is defined in the French Civil Code as "a real right, which is accessory to a piece of real property and which burdens another piece of real property" (Article 637).[1083] In essence, these rights would constitute a burden imposed on the property of a data subject for the benefit of another legitimate interest, e.g. the free speech of another.[1084]

4.5. Would the proposed property regime violate freedom of expression?

An understandable concern is the effect propertisation of personal data would have on freedom of expression. Indeed, introduction of the property rights system based on the *erga omnes* effect and reinforced control of the data subject over his data will hinder some information transfers. However, the system of property rights proposed in this study is meant to mirror the substantial principles of data protection already in force. Consequently, the effect of the regime of propertisation on freedom of expression will be no different that the effect current data protection rules have.

Article 9 of the 1995 Directive specifically addresses the relationship between data protection and freedom of expression and allows exemptions or derogations from the data protection provisions "for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression." These derogations can be translated into the property language as servitudes already mentioned in 4.4.

Propertisation will also make no difference in how the right to respect for private life (Article 8) and freedom of expression (Article 10) are balanced under the ECHR. Indeed, property is meant as a mere legal instrument to improve implementation of the data protection rules, and, in part the data protection interests are already recognised as a part of Article 8 (1) interests, will not take them out of the

---

[1083] Aynes, "Property Law ". p. 167
[1084] Ibid. p. 167

scope of Article 8 protection. The same balancing act between the interests of privacy and free speech as in, e.g. *Von Hannover*, will have to be performed.[1085]

A question that deserves special consideration is whether restrictions on commercial data processing introduced by propertisation would constitute a violation of freedom of speech under Article 10 ECHR. In brief, Article 10 (1) also offers protection to so-called 'commercial speech' that includes transferring and receiving information in economic interests. Telecom transmissions are one of instances of protected expression.[1086] Protected speech does not always have to constitute exchange of ideas.[1087] Mere data transfers, therefore, also fall under Article 10 (1) protection. Therefore, any regulation of data transfers, such as the existing EU measures or the system of property, in principle, will constitute interference. The position of this study, however, is that this is a legitimate interference in the meaning of Article 10 (2) as it is: a) introduced by law b) with a legitimate purpose to protect (data protection) rights of others and c) necessary in a democratic society. With regard to the last element of the test, one may argue that introduction of the consent rule as default is not a least intrusive measure possible for achievement of the legitimate purpose. However, one should keep in mind that the scrutiny of the limitations on commercial speech is significantly lower than in case of speech in public interest.[1088]

5. Conclusion

This chapter sought to re-examine the familiar idea of property rights in personal data in view of recent developments in information technology and practices. It has been demonstrated in the previous chapters that, as a result of chain informatisation, cloud computing, and ambient intelligence, the number of actors involved in the processing of personal data, and the relationships between them, have increased and widened respectively, and will continue to do so. The resulting structure of the data flow is too complex for the existing data protection approach to manage; in other words, the paths that personal data take and the participation of individual actors are hard to trace and, hence, regulate. Property, with some limitations thereof resolved by regulation, and due to its *erga omnes* effect and the fragmentation of property rights, has the potential to better reflect and control these complex relationships.

[1085] see Chapter 9, section 3.3.2.; paras. 58-60 of the decision

[1086] *Markt Intern Verlag GmbH v Germany*; Harris, *Harris, O'boyle & Warbrick Law of the European Convention on Human Rights*., p. 461; Reid, *A Practitioner's Guide to the European Convention on Human Rights*., IIB-165

[1087] *Von Hannover*, para. 59, balanced privacy and speech in form of photos.

[1088] Harris, *Harris, O'boyle & Warbrick Law of the European Convention on Human Rights*., p. 461; *von Hannover*, para. 59

The *erga omnes* effect of property rights is key in this transformation as, thanks to it, propertisation introduces the ultimate clarity of rights and obligations. The resulting clarity of how the accountability for the data protection violations is distributed has a positive influence on the level of compliance with and enforcement of data protection.

The propertisation of personal data complemented with some additional regulation may be regarded as an example of how property exercises its protective rather than its market function by ensuring that even after the transfer of a tiny proportion of rights, a data subject always retains basic control over his personal information.

Chapter 11: Conclusion

1. Introduction: questions

The central question of this study was whether, from a legal perspective, propertisation of personal data is a pragmatically sound direction for Europe to move to in its data protection legislation. The question implied two sub-questions: first, to what extent propertisation of personal data is legally possible, and second, if and to the extent it is possible, what would be the benefits and limitations of the property regime when used to resolve the personal data problem.

In contrast with the already existing literature, this study offered a comprehensive approach to the topic and concluded that the idea of property rights in personal data in Europe is not only formally possible, but offers some advantages in dealing with the personal data problem. The study therefore concludes that the property approach should not be ruled out as a possible next step in developing data protection. In fact, it should be carefully considered further. This last chapter explains in a nutshell how the study arrived at these conclusions. One way to do that is to give summaries of the arguments and findings of all the chapters that led to the study's main conclusions in order of their appearance. Indeed, the specific findings of the individual chapters are the building blocks of the perspective that this book developed on property in personal data. However, in order to present the bird's-eye view on this perspective in a consequent manner it seems more helpful to go over the findings by grouping them into the blocks, first explaining how the idea of propertisation came into the European discourse (section 2) and then giving answers to the two research sub-questions (section 3). The chapter will conclude with some final remarks concerning the main message of the study and its addressees, as well as some suggestions for the policy-makers' agendas.

2. Background

Before restating the answers to the two research questions and explaining in short the perspective this study developed on the idea of property rights in personal data, let us briefly return to the two issues that laid the foundation of the present study: the personal data problem and the origin of the idea of propertisation.

2.1. Personal data problem

True to the idea of legal pragmatism explained in the introductory chapter,[1089] this study examined property in personal data as a means to address a particular problem referred to here as the personal data or data processing problem. Therefore, defining the substance of that problem took a central place in the argument above.

The personal data problem presents a combination of developments and concerns with regard to personal data.[1090] Plainly, the developments are the events and processes that have been taking place in the post-industrial societies since the so-called Information Revolution in the 1960s and that have changed the nature of data processing. The developments are many and various and occurred in technology, public and private institutions, markets and the society in general. Two trends, however, appear more prominently. The first is the constantly growing need for more information, characteristic of both state and private organisations, in the state-citizen and business-consumer relationships. The increase in volume of data processing allows organisations to be more efficient in achieving their goals, such as greater obedience of the law and social rules and better security. On the other hand, it also enables control over the population at times turning to manipulation. People's private lives have also become more dependent on sharing personal data. The second trend is the growing capacity of technology to accommodate the desire for more information and better communication. Shrinking size and falling prices of hardware made computers open to a wider range of applications and accessible to a wider range of actors from a large multinational corporation to everyone owning a cell phone. Software has also been developed to perform various types of analysis of personal data.[1091] In the last decade, the increase in the number of data processing actors, and the relationships between them in information chains, computer clouds, and in the context of ambient intelligence have made the paths that personal data take ever more complex and difficult to predict or channel.[1092]

Given the increased scope and, often, the sensitivity of the personal information processed as a result of institutional, market, societal and technological developments, it comes as no surprise that the actual and potential effects of data processing raise numerous concerns in academic and political circles, as well as among the general public. The concerns are many and various, at times poorly articulated and often lacking agreement regarding their nature and validity. Some of them such as breach of secrecy of personal information have traditionally dominated the data protection debate. Apart from the intrusion into one's solitude, breach of secrecy of information is also argued to lead to a misbalance of powers between

[1089] Chapter 1, section 3.1.
[1090] Chapter 2, section 1
[1091] Chapter 2, sections 2.1-2.5
[1092] Chapter 2, section 2.6

governments or private organisations and an individual, jeopardising his freedom and autonomy. Another conventional concern is related to the errors in personal records, data being taken out of context, and misrepresentation. Besides, possession of personal data may enable unjust treatment, discrimination, economic segregation and general inequality.[1093] Next to the traditional list of concerns, this study articulated the concerns which derive from the changes in the structure of the modern data flow. The complexity and multiplicity of the data processing relationships have raised concerns about the lack of transparency of data flow and the accountability of the actors involved in it. Simply put, when a piece of personal data is sent to an information chain or information cloud, it is difficult to trace how it made it from point A to point B. It is also difficult to identify who is responsible if something goes wrong. Opacity and a lack of accountability not only aggravate the more traditional personal data related concerns, but also impede the enforcement of the current data protection rules.

The rapidly developing technology and ever growing concerns about its application have always raised the questions of whether the data protection laws in place are capable of meeting the challenges and, if not, whether a different approach, such as propertisation, will do better. The US debate on information privacy was the first forum where the idea to address the personal data problem via propertisation took a prominent place.

2.2. The US origins of the idea of propertisation

Following the logic of the functional comparison, this study looked at the proposal to create property rights in personal data as it emerged in its 'mother-jurisdiction', the United States. In brief, the idea in a large part owes its birth to the various peculiarities of the US legal system leading to many difficulties in addressing the personal data problem adequately. For instance, the formation of information privacy laws, especially privacy torts and US constitutional case law, was channelled by a one-sided *conceptualis*ation of the personal data problem as one of the secrecy of personal information. As a result, the relevant legal norms mainly provide protection in the form of negative rights, which, in terms of the evolution of data protection law, are substantially inferior to the current European data protection regime. In the case of constitutional remedies, these are also only applicable against the government. A number of statutes adopted since the 1970s took a part of the information privacy law forward by introducing positive rights and administrative regulation tackling the personal data problem. However, in a large part the effects of the information privacy laws are limited to the public sector and some parts of the private data processing industry. A significant part of private data processing, thus, continues to

[1093] Chapter 3, sections 2-4

be unregulated. Due to the specificities of the US political system, the strength of the information industry lobby and the shortcomings of torts as a common law institution, critics of US information privacy law point out that improving the situation via legislation or the retooling of the system of privacy torts is unlikely to be a solution.[1094] The predicted failure of the alternative tools drew attention to the idea of propertisation as property rights in personal data promise to be able to perform where other solutions, arguably, fail. Most importantly, in the US discourse propertisation of personal information was expected to give individuals some control over personal information where there was none or little control before. Namely, natural rights theory presented propertisation as the way to acknowledge an inherent connection between an individual and his data.[1095] Other commentators drew their understanding of property from law and economics. One groups of scholars supports propertisation because, in economic terms, the language of property describes the desired degree of control they aim to give to the individuals over their data. Another group draws their understanding of property from the dichotomy "property rule vs. liability rule." The existing system of privacy torts equals the liability rule. Either way, economic analysis considers property as the only alternative to disclosure of personal information. The last significant line of argument supports propertisation because, giving individuals control over data and in the absence of regulatory intervention, it will generate incentives for private companies to respect privacy and, as a result, a better system of data protection.[1096]

3. Answers

3.1. Propertisation of personal data, to a degree, is legally possible

The European discussion on propertisation would not have many prospects if in one or another way the option to introduce property rights in personal data were excluded by law. Therefore, the innitial step phase of answering the main research question is to establish whether propertisation of personal data is legally possible in Europe and if yes, to what extent. A short answer to this question is "it depends". Crucially, it depends on how one construes propertisation, or what scope of property rights in personal data a certain theory effectively means to introduce. Therefore, in order to answer the research question this study specified what it means by propertisation.

[1094] Chapter 5

[1095] Chapter 6, section 3

[1096] Chapter 6, section 4

3.1.1. Property in law implies real rights with erga omnes effect

Arguments from several fields using the concept of property - economics and philosophy among others - have been brought for and against property in personal data, each of them having a value of its own but also deriving from different assumptions about property. Therefore, the first step this study took to specify its understanding of property was to define the field it identified itself with and the resulting perspective on the concept of property. The perspective of choice was the one of the law.

Chapter 4 made several basic observations about the meaning of property in law. First is that although the layman's, normative and economic perspectives inform the content and rationale of the property rights in law, the legal perspective has its own distinctive meaning. While the layman's property talk equates property with tangible objects, economic analysis is concerned with achieving efficiency or predicting behaviour of a rational utility-maximizer, and normative theories are occupied with the moral justifications of propertisation, the law distinctly is concerned with the content, scope and consequences of the involved enforceable rights in the context of a given legal system.[1097] This study acknowledges that the decisions to introduce property rights of a new scope or in a new object are mostly political and as such are often taken on the basis of economic, normative and other extra-legal considerations. Nevertheless, the meaning of property as a system of certain enforceable rights, their content, scope and consequences in a legal system remain not accounted for by the non-legal theories. Therefore, the perspective of law, albeit related to and informed by other discourses, is rather unique and deserves separate consideration.

Another key observation of this study regarding property is the fluidity of the concept. For the reason of fluidity, even after narrowing down the discussion at hand to property in law and then to property in Europe, it is still not a straightforward task to state unequivocally what property is. The law in general, and property law in particular, are largely political phenomena. The meaning of property rights in law, as well as their objects and scope, are influenced by the conditions of a given society, varying across both time and space.[1098] Europe comprises a variety of national legal systems, each determining the scope and objects of property rights in different ways and making a common European approach to propertisation difficult to achieve. This study however demonstrated that a common European propertisation talk is possible. It showed that some common principles of property, along with the recent developments in modern property law in some EU member states and at the EU level, if not point to the possibility of the unification of property law, at the very

[1097] Chapter 4, Section 2.
[1098] Chapter 4, Section 3.1.

least, enable a dialogue on property matters in Europe, including the matters of new property rights and objects such as personal data.[1099]

This study points at what could be the common European concept of property rights by analysing property law in continental and common law systems based on unitary and fragmented ownership respectively. The conclusion reached is that despite the dominant perceptions of the two systems as two extremes difficult to compare, they in fact share a common historical point of departure - the feudal system of land ownership, and ultimately are built of the same building blocks.

More precisely, in the feudal system the entitlements in the same piece of land varied in scope and duration were distributed among different holders simultaneously. Such a system continued and evolved in the common law legal tradition and was deliberately rejected in the continental law. However, despite the rejection, fragmented ownership remains the historical basis of the property law in both legal systems.[1100] What characterised some land holds in the feudal system was their effect on third parties, an indefinite number of people who were otherwise not bound by a contract with the holder. Such an effect is also referred to as the *erga omnes* effect. Arguably, such a fragmentation of the rights in land maintained the strata structure of the feudal society that the French revolution and resulting civil law of continental Europe strived to prevent. Therefore, the choice of the Continental Europe was against a division of the unitary land holding and at present in civil law only unitary ownership enjoys the *erga omnes* effect. As the property law systems of some Continental European countries move to give the *erga omnes* effect to the rights 'lesser' than the full ownership, it becomes clear that the only truly defining feature of the property rights is that they are erga omnes, i.e. have effect against an indefinite number of people.[1101] This is what distinguishes property rights, also referred to as real rights, from contractual, or personal, rights that – as a rule - only bind the parties of a contract. To sum up, in the present discussion on the European perspective on property in personal data the author used the term 'property' or more precisely, 'property rights' in its legal meaning, that focuses primarily on the content of the relevant rights and their effects in a legal system, the *erga omnes* effect being the key defining denominator.

Therefore, when talking about propertisation of personal data in Europe this study meant introduction of property or real rights distinguishable from personal rights by their *erga omnes* effect.

[1099] Chapter 4, Section 3.2.

[1100] Chapter 4, Section 3.2.3(a).

[1101] Chapter 4, Section 3.2.3(b).

3.1.2. Current EU data protection law does not exclude propertisation within the limits established by data protection regime

Once this study established the *erga omnes* effect as the common denominator enabling a meaningful European discussion on property, it moved to the issue of the legal possibility of propertisation of personal data, first, under the EU law. Using the 1995 Data protection directive as the main reference point in the discussion on EU data protection, Chapter 8 showed that nothing in the current data protection regime prohibits or excludes introducing property rights in personal data. Indeed, in view of the flexibility of the concept of property in law defined by the *erga omnes* effect of the relevant rights, almost any system of rights that provides a degree of control (i.e. including control over personal data) can be translated into the language of property.[1102] To exclude the very possibility of the propertisation of personal data one would have to eliminate individual rights of control, or informational self-determination, in favour of administrative rules of data processing. That would require principal changes in the European approach to data protection as we know it. Such changes would be in contradiction to the evolutionary development of the European data protection approach which has already rejected administrative regulation as the sole mode of data protection. They would also be in contradiction to the relevant fundamental choices made in Europe, such as information self-determination, adopted on the level of OECD and Council of Europe, to which the Directive also adheres.[1103]

Even more so, the logic of property protecting one's entitlement to defend 'his own' against the world is consistent with the principle of individual information self-determination as expressed in Article 7 of the 1995 Directive on the requirement of consent, information rights and a number of other provisions of the Directive. As seen in Chapter 4, property, which is flexible, is about rights of control with regard to a particular object. The principle of information self-determination moves the Directive close to the possibility of the introduction of limited propertisation, short of introducing de facto property rights in data with an individual as the holder of the 'biggest' property rights.[1104]

3.1.3. Propertisation is possible on condition of limited alienability

One of the important messages this study tried to convey is that the principal possibility to introduce property rights in personal data and the allowed scope of those rights are two different issues. Although the existing data protection

---

[1102] See Chapter 4, section 3.3.

[1103] Chapter 8, section 3.1.3 (b).

[1104] Chapter 8, section 3.1.3; Chapter 10, section 2.1 describes how the 1995 Directive is close to establishing de facto property in personal data.

framework does not rule out and, even more so, encourages the introduction of rights in personal data that have *erga omnes* effect, it is an entirely different question what the allowed scope of those rights would be. The allowed scope of property rights is of even more significance since the proposals to re-examine current data protection mechanisms in Europe in favour of private law tools of contract and property rely on the opportunity for an individual to either trade data pertaining to him for money or services, or to waive his data protection rights on market conditions.

a. … under the 1995 Directive and the EU legal order

As to the limits of propertisation in the EU legal order, although information self-determination and control are a common denominator in the bulk of the data protection laws in Europe,[1105] the purpose of which is to enable an individual to have a degree of freedom to choose what happens to his personal data, that does not suggest that the allowed degree of control allows absolute dominium over personal data, including free and unlimited alienation of control rights. The thesis of this study on the normative priority of information self-determination is in no way meant to imply that the consent rule is or should be the only condition to legitimate data processing. Since the current rules provide for a number of alternative conditions, such as authorization by law, the propertisation approach defended in this study regards consent merely as a default rule, which can be limited by law.[1106]

Here comes another important conclusion as to the legal possibility of propertisation under the Directive. Chapter 8 established that although the current data protection regime does not exclude but endorses the 'property thinking' with regard to personal data, the introduction of actual property rights is only permitted within the limits established by *inter alia* data protection law. General European law and the 1995 Directive in particular do not allow any property regime of personal data to deviate from the 1995 Directive's provisions and create property rights of a wider scope than the granted data protection rights. Most importantly, despite its goal to foster interests of the common market and free flow of information, the Directive and the EU law in general do not adhere to the laissez faire ideology and pursue economic goals with the view to respect human rights. Besides, freedom of contract often invoked to justify free alienability of personal data does not have precedence over data protection interests since the latter form part of the Article 8 ECHR right to privacy and the former does not enjoy human rights protection. Even more so, freedom of contract cannot have a higher standing than the data protection rights as any meaningful negotiation of a contract, also in the field of personal data,

---

[1105] Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits*. at 63; Solove, *Information Privacy Law*. at 872

[1106] Chapter 10, section 2.1.

seems impossible without law securing interests of a weaker party. Therefore, the provisions of the Directive, e.g. establishing the data subject's rights, cannot be 'contracted around' with effect of the contract taking precedence over those rights.[1107]

b. ... under the ECHR

Chapter 9 reached similar conclusions with regard to the allowed scope of property rights. It rejected the idea of free alienability and waiver of data protection rights as conflicting with the human rights nature of those interests.

It was established that in Europe it is impossible to divorce the data protection discourse from human rights. Namely, as a result of the Article 8 ECHR jurisprudence recognising the right to individual development and acknowledging the importance of autonomy, privacy, as protected by Article 8 ECHR, has gained a wider scope of protection. It extends beyond a negative interest in protecting secret information, and includes a positive right of personal development (and possibly even information self-determination), along with affirmative obligations imposed on a state to secure data protection interests effectively.[1108]

As the next step to challenge the claim that property rights in personal data necessarily imply free alienability Chapter 9 has shown that the Convention does not contain the right, in the fulfilment of freedom of contract, to waive data protection interests for remuneration. Firstly, freedom of contract is not guaranteed by the Convention explicitly nor is it implied by Protocol 1 Article 1 as a part of the property rights. Second, under the *Mellacher* decision, as far as the protection of property rights is afforded, it does not extend to the right to exchange that property against some advantage under the existing market conditions. The same holds for the other rights and freedoms guaranteed by the Convention, including the Article 8 right to privacy.[1109]

Both case-law and doctrine suggest that the ECHR does not protect an individual's right to obtain remuneration for forgoing his data protection rights. In the context of the propertisation of personal data debate this means that an individual cannot claim that his right was violated when the state prevents him, e.g. via regulation, from waiving any such right. Therefore, although, unlike the 1995 Directive, the ECHR itself does not set a limit on the scope of allowed property rights in personal data, a too wide scope is 'suspect' and, in case a nation state chooses to ban or limit certain aspects of the property trinity of usus, fructus and abusus with regard to the waiver of his data protection entitlements, the Convention does not contain grounds to grant an individual a claim of a violation.[1110]

[1107] Chapter 8, section 3.2 (a) through (e)
[1108] Chapter 9, sections 2.3-2.4.
[1109] Chapter 9, section 3
[1110] Chapter 9, section 3

3.2. Propertisation of personal data is a sound direction for development of the European data protection

Next to the findings on legality and limits of propertisation of personal data, this study also came to conclude that the introduction of property rights in personal data would actually make sense as a sound and even better alternative for the current European data protection. This conclusion has been made for two reasons: firstly, the existing data protection regime in Europe does leave significant room for improvement; secondly, introduction of property (real) rights has the potential to fix some shortcomings of the current regime without causing negative consequences that cannot be addressed with minimal additional regulatory measures.

3.2.1. The current European data protection regime fails to channel modern data processing

As Chapter 7 has established, the data protection community is generally satisfied with how the substantive data protection principles tackle most data protection concerns.[1111] The 1995 Data protection directive, as the primary point of reference of this study when it comes to bringing those substantive principles to reality, relies on two models of implementation: participatory and top-down. That is where the major weakness of the current approach lie.

Participatory implementation refers to implementation at the grass-roots level, which involves the private parties to the data processing – the data subjects as well as the data processing actors. The former are entitled to actively exercise their rights, including the rights to give and withdraw consent and information rights, whereas the latter are expected to comply with their obligations and exercise self-regulation and self-control.[1112] In a perfect world, the cornerstone of the participatory implementation model is a system of accountability, i.e. a set of clear data protection rights and corresponding obligations easy enough to invoke, comply with, monitor and, if necessary, enforce. This is not the case with the accountability system established by the 1995 Directive. This is so mainly because the system of rights and obligations established in the Directive as a basis for its participatory implementation has not caught up with the complexity of the actual relationships between those involved in data processing. As the readers recall, in the past decade as a result of the growing popularity of information technology, the number of actors involved with personal data went up in geometric progression. Together with the number of actors and new data practices, the level of complexity of the relationships between them also increased. The data flow has become less transparent to the involved actors

[1111] Chapter 7, section 2.3.1.
[1112] Chapter 7, section 2.2.2(a)

themselves and external observers – individuals and data protection authorities. When a piece of personal data is sent to an information chain or information cloud, it is difficult to trace how it made it from point A to point B. It is also difficult to identify who is responsible if something goes wrong. The Data Protection Directive drafted in the 1990s was intended to deal with a different, simpler kind of relationships. They were more 'linear' and included a smaller number of more clearly distinguishable data processing actors. Therefore, the Directive imposes the burden of accountability almost entirely on one type of actors involved in data processing – the controllers, whereas at least three more types are lisled. Theoretically, it is the controller who will be liable although the actual responsibility may lie with any other actor in a chain where the controller is only a link, or even in a totally different segment of the information dandelion as long as that segment is connected by a single link. The controller then may choose to pursue the other party at fault by means of contractual responsibility, as those are mostly contracts that govern the controller-non-controller relationships. This model of accountability, however, fails to capture the actual dynamic of the data processing relationships and therefore cannot channel it either. Firstly, due to advances in information technology, and its growing availability, it does not make sense presently to distinguish a controller as a separate and the only accountable actor from non-controllers; in fact, arguably, any actor involved with personal data, including the data subject himself, can nowadays in certain situations be classified as a controller. Besides legal qualifications, identifying the de facto controller or any data processing actor at fault in the context of cloud computing or chain informatisation proves to be difficult if not impossible for a data subject. Contractual arrangements between various involved actors do not secure the interests of the data subject either as they generally establish rights and obligations for their parties and rarely give grounds for third parties' (e.g. data subjects') claims.[1113]

Unclear distribution of accountability also hinders the top-down implementation, as without clear grounds and standards of supervision and enforcement the supervisory authorities often find themselves overloaded with at times contradictory tasks: they have to advise on and enforce the compliance with unclear rules against invisible actors. The lack of clarity of obligations and meagre perspectives of enforcement are among the factors undermining the good will and ability of the data processing actors to comply with the data protection regime, e.g. in their daily operation as well as via self- and co-regulation.[1114]

[1113] Chapter 7, section 2.2.2 (a)
[1114] Ibid., section 2.2.2 (a)(ii)

3.2.2. Real rights in personal data alter the system of accountability and improve implementation of the data protection rules

Two features make property important for present-day data protection challenges: its *erga omnes* effect and its flexibility. *erga omnes* means, as indicated earlier, that property gives protection against everyone else in the world.

The clarity of an obligation to 'stay away from personal data unless explicitly allowed otherwise', which would be imposed on every involved actor by propertisation, would remove the confusion arising from the controller–non-controller dichotomy. It would also positively affect the motivation and capacity of actors to comply with, and of the supervisory bodies to enforce, data protection standards.

Introduction of real rights with the *erga omnes* effect will mean that a data subject will not have to look for a controller to enforce his rights. The resulting system will resemble consumer protection: if one bought a product and it does not work, one can go to a shop where the product was bought, or directly to a manufacturer. This way, the consumer does not have to find out whose fault it is that the product is out of order: his rights are nevertheless protected. The same holds for personal data rights. If they are *erga omnes*, a person will have a valid claim against everyone with access to the data.

Flexibility of property rights is the second characteristic relevant for the debate on property in personal data. Flexibility manifests itself in the fact that the property rights can contain any set of rights and privileges, including but not limited to full ownership. Those rights fit most to achieve a certain regulatory purpose while still being called property rights, provided they retain *erga omnes* effect. Two components of the flexibility attribute are of special relevance for the discourse on property in personal data. Firstly, the definition of property – especially in its widest form of full ownership – as an absolute dominion is a fiction, for any proprietary interest is always limited, either by a public interest, e.g. in law prescribing whether a plot of land may be used for agricultural purposes, construction, etc., or by somebody else's proprietary interests, e.g. a servitude. Secondly, divisibility, or, in the language of the private law literature, fragmentation of ownership is another factor contributing to the flexibility of property rights. Fragmentation of ownership is a phenomenon that presently is more characteristic of the concept of property in common law but has entered a number of the continental law jurisdictions and a trans-European property discourse. It describes the idea that next to the full ownership – the widest in scope property right encompassing the holly trinity of usus, fructus, and abusus – there exist 'lesser' property rights narrower in scope and given the *erga omnes* effect by the competent authorities – judiciary or a legislator. They may encompass one or two of the three full ownership rights, and can be further limited in time or by other

conditions, making sure that, in case of transfer of a property right, a holder of any smaller right cannot give away more rights than he has.

4. Conclusion

This study has shown that propertisation of personal data can be meaningfully discussed in Europe. In fact, it also has some important advantages over the current system of EU data protection law.

The limited nature of property rights as well as fragmentation of ownership both imply that, once property rights in personal data are introduced, transfer of personal data from an individual does not have to mean full alienation of all control power over the data. By virtue of regulation, e.g. implementing European human rights and data protection standards, or due to the fragmentation of ownership, some degree of control will always remain with the individual, *inter alia* allowing him to decide on the possibility and extent of the secondary transfer of the data, and its use by any actor in the chain of further transfers. From the perspective of an individual's rights, what the propertisation of personal data can offer to the data protection cause, in the extremely complex conditions of the modern data flow, is to create a coherent and more articulate framework for personal data management. Such a framework would be respectful of the principle of information self-determination, and consistent with the protective as opposed to the market function of property rights.

English Summary

The central question of this study was whether, from a legal perspective, propertisation of personal data is a pragmatically sound direction for Europe to move to in its data protection legislation. The question implied two sub-questions: 1) to what extent propertisation of personal data is legally possible, and 2) if and to the extent it is possible, what would be the benefits and limitations of the property regime when used to resolve the personal data problem.

Concept of property

The first step towards answering the main research question is whether propertisation of personal data is legally possible in Europe and if yes, to what extent. A short answer to this question is "it depends". Crucially, it depends on how one construes propertisation, or what scope of property rights in personal data a certain theory effectively means to introduce. Therefore, the first step this study took in answering the research question was to specify what it means by propertisation.

The concept of property used in this study was defined from a legal perspective. The perspective of choice was the one of the law and focused on the content of the legal rights and their binding effects. It was established that the concept of property in law is fluid. The meaning of property rights in law, as well as their objects and scope, are influenced by the conditions of a given society, varying across both time and space. Europe comprises a variety of national legal systems, each determining the scope and objects of property rights in different ways and making a common European approach to propertisation difficult to achieve. This study demonstrated that a common European propertisation talk is possible. Some common principles of property, along with the recent developments in modern property law in some EU member states and at the EU level, if not point to the possibility of the unification of property law, at the very least, enable a dialogue on property matters in Europe, including the matters of new property rights and objects such as personal data.

This study pointed at what could be the common European concept of property rights. The conclusion reached is that despite the dominant perceptions of the two systems of property in continental and common law based on unitary and fragmented ownership respectively as two opposites difficult to compare, they in fact share a common denominator – the erga omnes (against an indefinite number of people) effect of property rights. This is what distinguishes property rights, also referred to as real rights, from contractual, or personal, rights that – as a rule - only

bind the parties of a contract. To sum it up, in the present discussion on the European perspective on property in personal data the author used the term 'property' or more precisely, 'property rights' in its legal meaning, that focuses primarily on the content of the relevant rights and their effects in a legal system, the erga omnes effect being the key denominator.

Legal possibility of propertisation

As to the legal possibility of propertisation of personal data under the EU law nothing in the current data protection regime prohibits or excludes introducing property rights in personal data. Given extreme flexibility of the concept of property in law, almost any system of rights that provides a degree of control can be translated into the language of property. To exclude the very possibility of the propertisation of personal data one would have to eliminate individual rights of control, or informational self-determination, in favour of administrative rules of data processing.

The logic of property protecting one's entitlement to defend 'his own' against the world is consistent with the principle of individual information self-determination expressed in Art. 7 of the 1995 Directive on the requirement of consent, information rights and a number of other Directive's provisions. The principle of information self-determination moves the Directive close to the possibility of the introduction of limited propertisation, short of introducing de facto property rights in data with an individual as the holder of the 'biggest' property rights.

One of the important messages this study tried to convey is that the principal possibility to introduce property rights in personal data and the allowed scope of those rights are two different issues. Although the existing data protection framework does not rule out and, even more so, encourages the introduction of rights in personal data that have erga omnes effect, it is an entirely different question what the allowed scope of those rights would be. The allowed scope of property rights is of even more significance since the proposals to re-examine current data protection mechanisms in Europe in favour of the private law tools of contract and property rely on the opportunity for an individual to either trade data pertaining to him for money or services, or to waive his data protection rights on market conditions.

The benefits and limitations of the property regime

The introduction of property rights in personal data would be a sound addition to the current European data protection: firstly, the existing data protection regime in Europe does leave significant room for improvement in how it deals, or better, does not deal with the globalisation and proliferation of data processing; secondly, introduction of property (real) rights has potential to fix the shortcomings of the current regime without causing negative consequences that cannot be addressed with additional regulatory measures.

The data protection community is generally satisfied with how the substantive data protection principles tackle most data protection concerns. The 1995 Data protection directive as the primary point of reference of this study when it comes to bringing those substantive principles to reality relies on two models of implementation: participatory and top-down. That is where the major weakness of the current approach lie.

Participatory implementation refers to implementation at the grass-roots level. In a perfect world, the cornerstone of the participatory implementation model is a system of accountability, i.e. a set of clear data protection rights and corresponding obligations easy enough to invoke, comply with, monitor and, if necessary, enforce. This is not the case with the accountability system established by the 1995 Directive. This is so mainly because the system of rights and obligations established in the Directive as a basis for its participatory implementation has not caught up with the complexity of the actual relationships between those involved in data processing. When a piece of personal data is sent to an information chain or information cloud, it is difficult to trace how it made it from point A to point B. It is also difficult to identify who is responsible if something goes wrong.

Theoretically, it is the controller who will be liable although the actual responsibility may lay with any other actor in a chain where the controller is only a link, or even in a totally different segment of the information dandelion as long as that segment is connected by a single link. The controller then may choose to pursue the other party at fault by means of contractual responsibility, as those are mostly contracts that govern the controller-non-controller relationships. This model of accountability, however, fails to capture the actual dynamic of the data processing relationships and therefore cannot channel it either.

Unclear distribution of accountability hinders the top-down implementation, as without clear grounds and standards of supervision and enforcement the supervisory authorities often find themselves overloaded with at times contradictory tasks: they have to advice on and enforce the compliance with unclear rules against invisible actors. The lack of clarity of obligations and meagre perspectives of enforcement are among the factors undermining the good will and ability of the data

processing actors to comply with the data protection regime, e.g. in their daily operation as well as via self- and co-regulation.

Two features make property important for present day data protection challenges: its erga omnes effect and its flexibility. The clarity of an obligation to 'stay away from personal data unless explicitly allowed otherwise', which would be imposed on every involved actor by propertization, would remove the confusion arising from the controller–non-controller dichotomy. It would also positively affect the motivation and capacity of actors to comply with and of the supervisory bodies to enforce data protection standards.

Introduction of the real rights with the erga omnes effect will mean that a data subject will not have to look for a controller to enforce his rights. The resulting system will resemble consumer protection: if one bought a product and it does not work, one can go to a shop where the product was bought, or directly to a manufacturer. This way, the consumer does not have to find out whose fault it is that the product is out of order: his rights are nevertheless protected. The same holds for personal data rights. If they are erga omnes, a person will have a valid claim against everyone with access to the data.

Two components of the flexibility attribute are of special relevance for the discourse on property in personal data. Firstly, the definition of property – especially in its widest form of full ownership – as an absolute dominium is a fiction for any proprietary interest is always limited, either by a public interest or by somebody else's proprietary interests. Secondly, divisibility, or, in the language of the private law literature, fragmentation of ownership is another factor contributing to the flexibility of property rights.

The limited nature of property rights as well as fragmentation of ownership both imply that, once property rights in personal data are introduced, transfer of personal data from an individual does not have to mean full alienation of all control power over the data. By virtue of regulation or due to the fragmentation of ownership, some degree of control will always remain with the individual, inter alia allowing him/her to decide on the possibility and extent of the secondary transfer of the data, and its use by any actor in the chain of further transfers. From the perspective of an individual's rights, what the propertisation of personal data can offer to the data protection cause, in the extremely complex conditions of the modern data flow, is to create a coherent and more articulate framework for personal data management that is respectful of the principle of information self-determination, consistent with the protective as opposed to the market function of property rights.

Conclusion

In contrast with the already existing literature, this study offered a comprehensive approach to the topic and concluded that the idea of property rights in personal data in Europe is not only formally possible, but offers some advantages in dealing with the personal data problem. Namely, it introduces ultimate clarity as to the allocation of the data protection obligations.

The study therefore concludes that the property approach should not be ruled out as a possible next step in developing data protection without further careful consideration.

Bibliography

Acquisti, Alessandro, Gross, Ralph. "Information Revelation and Privacy in Online Social Networks (the Facebook Case)." In *ACM Workshop on Privacy in the Electronic Society (WPES)*, 2005.

Agre, P. E., Rotenberg, Marc eds. *Technology and Privacy : The New Landscape*. Cambridge: MIT Press, 1997.

Ahmed, Murad, Burgess, Kaya "Four Million British Identities Are up for Sale on the Internet." *TimesOnline*,no. July, 18 (2009), http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article6718560.ece.

Akkermans, Bram. *The Principle of Numerus Clausus in European Property Law*. Antwerp - Oxford - Portland: Intersentia, 2008.

Allen, Alchian and. *Exchange and Production*. 2nd ed1977.

Aynes, Laurent. "Property Law " In *Introduction to French Law*, edited by G.A. Bermann, Picard, E., 147-71. Austin, Boston, Chicago, New York, the Netherlands: Wolters Kluwer, 2008.

Bartels, Steven, et al. *Content of Real Rights*: Wolf Legal Publishers, 2004.

Barzel, Yoram. *Economic Analysis of Property Rights*. 2nd ed: Cambridge University Press, 1997.

Basedow, Jürgen. "Freedom of Contract in the European Union." *European Review of Private Law* 16, (2008).

Becker, Gary. "Is Ethnic and Other Profiling Discrimination?" In *The Becker-Posner-Blog*, 2005.

Bennett, Colin J. "Convergence Revisited: Toward a Global Policy for the Protection of Personal Data? ." In *Technology and Privacy: The New Landscape* edited by Philip E. Agre & Marc Rottenberg, 1997.

———. *Regulating Privacy - Data Protection and Public Policy in Europe and the United States*1992.

Bentham, Jeremy. "Security and Equality of Property." In *Property: Mainstream and Critical Positions*, edited by C.B. Macpherson. Toronto: University of Toronto Press, 1978.

Bergelson, Vera. "It's Personal, but Is It Mine? Toward Property Rights in Personal Information." *U.C. Davis L. Rev.* 37, (2003): 379.

Bergkamp, Lucas. "EU Data Protection Policy the Privacy Fallacy: Adverse Effects of Europe's Data Protection Policy in an Information-Driven Economy." *Computer Law & Security Report* 18, no. 1 (2002): 31.

Berkvens, Jan. "Role of Trade Associations: Data Protection as a Negotiable Issue." In *Reinventing Data Protection?*, edited by Serge Gutwirth, 125-31. Brussels: Springer, 2009.

Bignami, Francesca. "The U.S. Privacy Act in Comparative Perspective." In *Public Seminar on PNR/SWIFT/Safe Harbour: Are Transatlantic Data Protected?* Brussels, 2007.

Bing, J. "Informatics of Public Administration: Introducing a New Academic Discipline." *Informatica ediritto* 1-2, (1992).

Blok, P. *Recht Op Privacy*: Boom, 2002.

Brown, Duncan H., Blevins, Jeffrey Layne. "The Safe-Harbor Agreement between the United States and Europe: A Missed Opportunity to Balance the Interests of E-Commerce and Privacy Online." *Journal of Broadcasting & Electronic Media* 46, no. 4 (2002): 565 — 85.

Brownsword, R. "Consent in Data Protection." In *Reinventing Data Protection?*, 2009.

Bruce, J.W., Ely, James W. Jr. *Cases and Materials on Modern Property Law*. 6th ed: Thomson West.

Bullesbach, Alfred, Poullet, Yves, Prins, Corien, ed. *Concise European IT Law*: Kluwer Law International 2006.

Bullesbach, Alfred, Poullet, Yves, Prins, Corien, Serge, Gijrath, ed. *Concise European IT Law*. 2nd ed: Wolters Kluwer, 2010.

Burkert, Herbert. "The Law of Information Technology." *DuD* (1988): 384-85.

———. "Towards a New Generation of Data Protection Legislation." In *Reinventing Data Protection?*, edited by Serge et al. Gutwirth, 333-40. Berlin: Springer, 2009.

Butler, Brian E. "Legal Pragmatism: Banal or Beneficial as a Jurisprudential Position?" *Essays in Philosophy* 3, no. 2 (2002).

Bygrave, Lee A. *Data Protection Law: Approaching Its Rationale, Logic and Limits*. Vol. 10, Information Law Series: Kluwer Law International, 2002.

Bygrave, Lee A., Schartum, Dag Wiese "Consent, Proportionality and Collective Power." In *Reinventing Data Protection?*, edited by Serge Gutwirth, de Hert, Paul, Poullet, Yves, 157-73. Brussels: Springer, 2009.

Calabresi, Guido, Melamed, A. D. "Property Rules, Liability Rules, and Inalienability: One View of the Cathedral." *Harv. L. Rev.* 85, (1972).

Caruso, Daniela. "Private Law and Public Takes in European Integration: The Case of Property." *European Law Journal* 10, no. 6 (2004): 751-65.

Cate, Fred H., Litan, Robert "Constitutional Issues in Information Privacy." *Mich. Telecomm. Tech. L. Rev.* 35, no. 9 (2002): 35.

Cavoukian, Ann. "Privacy in the Clouds - a White Paper on Privacy and Digital Identity: Implications for the Internet ": Information and Privacy Commissioner of Ontario, 2008.

Chemerinsky, Erwin. "Substantive Due Process." *Toronto Law Review* 15, (1999): 1501.

Chen, Brian X. . "If You're Not Seeing Data, You're Not Seeing." *Wired*,no. August 25, 2009 (2009), http://www.wired.com/gadgetlab/tag/augmented-reality/.

Cherednychenko, Olha. "EU Fundamental Rights, EC Fundamental Freedoms and Private Law." *European Review of Private Law* 1, (2006): 23-61.

Clark, Amy S. "Employers Look at Facebook, Too: Companies Turn to Online Profiles to See What Applicants Are Really Like." *CBS Evening News*,no. June 20, 2006 (2006), http://www.cbsnews.com/stories/2006/06/20/eveningnews/main1734920.shtml.

Coase, Ronald H. "The Problem of Social Cost." *J.Law & Econ.* 3, (1960): 1.

Cohen, Julie. "Examined Lives: Informational Privacy and the Subject as Object." *Stan. L. R.* 52, (2000): 1373.

Cooke, Elizabeth. *Land Law*. Oxford: Oxford University Press, 2006.

Craig, Paul, De Burca, Grainne. *EU Law: Text, Cases and Materials*. 4th ed: Oxford University Press, 2008.

Cribbet, John E. "Concepts in Transition: The Search for a New Definition of Property." *U. Ill. Law Rev.* no. 1 (1986).

Cribbet, John E., Finfley, Roger W., Smith, Ernest E., Dzienkovski, John S. *Property. Cases and Materials*. 9th ed. New York: Foundation Press, 2008.

Cuijpers, C.M.K.C., Koops, Bert-Jaap. "Het Wetsvoorstel 'Slimme Meters': Een Privacytoets Op Basis van Art. 8 Evrm." (2008).

———. "How Fragmentation in European Law Undermines Consumer Protection: The Case of Location-Based Services." *European Law Review* no. 6 (2008): 880-97.

Cuijpers, Colette. "A Private Law Approach to Privacy: Mandatory Law Obliged? ." *SCRIPT-ed* 4, no. 4 (2007): 304-18.

"De Burger in De Ketens: Verslag van Nationale Ombudsman over 2008." Dutch National Ombudsman, 2008.

De Schutter, Olivier. "Waiver of Rights and State Paternalism under the European Convention on Human Rights." *N. Ir. Legal Q.* 51, no. 3 (2000): 481-508.

Du, Yu, Murphy, Matthew. "Data Protection and Privacy Issues in China." In *HG.org: Worldwide Legal Directories*, 2008.

Dunoff, Jeffrey L., Trachtman, Joel P. "A Functional Approach to International Constitutionalization." In *Ruling the World? Constitutionalism, International Law, and Global Governance*, edited by Jeffrey L. Dunoff, Trachtman, Joel P., 3-37: Cambrigde University Press, 2009.

ENISA. "Cloud Computing: Benefits,Risks and Recommendations for Information Security." edited by Daniele Catteddu, Hogben, Giles European Network and Information Security Agency, 2009.

EPIC. *Privacy & Human Rights: An International Survey of Privacy Laws and Developments*: EPIC, 2006.

Epstein, Richard A. "A Clear View of the Cathedral: The Dominance of Property Rules." *Yale L.J.* 106, (1997): 2091.

———. "Privacy, Publication, and the First Amendment: The Dangers of First Amendment Exceptionalizm." *Stan. L. R.* 52, (2000): 1003.

Etzioni, Amitai. *The Limits of Privacy*. 1 ed: Basic Books, 2000.

Europe, Digital Civil Rights in. "Final Agreements between EU and USA on Pnr and Swift."

Fader, Wendy W. Moe and Peter S. "Capturing Evolving Visit Behavior in Clickstream Data." *Journal of Interactive Marketing* May, (2003).

Fairfield, Joshua. "Virtual Property." *Boston University Law Review* 85, (2005).

Fenrich, William J. "Common Law Protection of Individuals' Rights in Personal Information." *Fordham L. Rev.* 65, (1996): 951.

Ferrera, Maurizio; Rhodes, Martin "Recasting European Welfare States: An Introduction." *West European Politics* 23, no. 2 (2000): 1-10.

Garland, David. *The Culture of Control: Crime and Social Order in Contemporary Society*: The University of Chicago Press, 2001.

Garner, Bryan A., ed. *Black's Law Dictionary*. 9th ed: West, 2009.

Garret, Paul Michael. "Social Work's 'Electronic Turn': Notes on the Deployment of Information and Communication Technologies in Social Work with Children and Families." *Critical Social Policy* 25, no. 4 (2005): 529-53.

Gellman, Robert. "Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing." The World Privacy Forum, 2009.

Giddens, Anthony. *The Nation-State and Violence*. Berkeley: University of California Press, 1985.

Girot, Clarrisse. "The Development of the Protection of Weak Parties in Comparative Law." In *User Protection in IT Contracts*, 19-53, 2000.

Gordley, James. *Foundations of Private Law : Property, Tort, Contract, Unjust Enrichment*. Oxford [etc.]: Oxford University Press, 2006.

Gormley, Ken. "One Hundred Years of Privacy." *Wis. L. Rev.* (1992): 1335.

Grant, Hazel. "Data Protection 1998-2008." *Computer Law & Security Report* 25, (2009): 44-50.

Gray, Kevin. "Property in Thin Air." *Cambridge Law Journal* 50, no. 2 (1991): 252-307.

Gruening, G. "Origin and Theoretical Basis of New Public Management." *International Public Management Journal* 4, (2001): 1-25.

Gutwirth, Serge, de Hert, Paul. "Regulating Profiling in a Democratic Constitutional State." In *Profiling the European Citizen: Cross-Disciplinary Perspectives*, edited by Mireille Hildebrandt, Gutwirth, Serge. Dordrecht: Springer, 2008.

Harris, D.J, O'Boyle, M.O., Bates, E.P., Buckley, C.M. *Harris, O'boyle & Warbrick Law of the European Convention on Human Rights*. 2nd ed: Oxford University Press, 2009.

Harris, J.W. *Property and Justice*. Oxford [etc.]: Clarendon Press, 1996.

Harris, Mark Townsend and Paul. "Security Role for Traffic Cameras." *The Observer* (2003).

Haythornthwaite, Caroline. "Social Networks and Internet Connectivity Effects." *Information, Communication, and Society* 8, no. 2 (2005): 125-47.

"Health Checks from Your Doctor Could Be Replaced by Visits to the Bathroom, Thanks to a Smart Toilet Developed by a Japanese Company.". *CNN.com*,no. June 28 (2005), http://www.cnn.com/2005/TECH/06/28/spark.toilet/index.html.

Heisenberg, Dorothee. *Negotiating Privacy: The European Union, the United States, and Personal Data Protection*. London: Lynne Rienner Publishers, 2005.

de Hert, Paul. "A Right to Identity to Face the Internet of Things?".

de Hert, Paul, Gutwirth, Serge. "Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalization in Action." In *Reinventing Data Protection?*, edited by Serge Gutwirth, et al., 3-45. Berlin: Springer, 2009.

de Hert, Paul, Gutwirth, Serge "Making Sense of Privacy and Data Protection: A Prospective Overview in the Light of the Future of Identity, Location-Based Services and Virtual Residence in the Institute for Prospective Technological Studies: Report Eur 20823 En." *Security and Privacy for the citizen in the post-September 11 digital age: a Prospective overview* (2003).

de Hert, Paul, Gutwirth, Serge, Moscibroda, Anna, Fuster, Gloria Gonzalez, Wright, David. "Legal Safeguards for Privacy and Data Protection in Ambient Intelligence." *Personal and ubiquitous computing* 13, no. 6 (2009): 435-44.

Hildebrandt, Mireille. "Defining Profiling: A New Type of Knowledge?" In *Profiling the European Citizen: Cross-Disciplinary Perspectives*, edited by Mireille Hildebrandt, Gutwirth, Serge, 18. Dordrecht: Springer, 2008.

Hildebrandt, Mireille, Gutwirth, Serge, ed. *Profiling the European Citizen: Cross-Disciplinary Perspectives*. Dordrecht: Springer, 2008.

Hill, Kashmir. "Justice Scalia Responds to Fordham Privacy Invasion!" *Above the Law: A Legal Tabloid*,no. Wednesday, April 29 (2009), http://abovethelaw.com/2009/04/justice_scalia_responds_to_for.php.

Hirsch, Dennis D. "The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?" *ExpressO* (2010), http://works.bepress.com/dennis_hirsch/1

Hoeren, Thomas, Rodenhausen, Anselm. "Constitutional Rights and New Technologies in Germany." In *Constitutional Rights and New Technologies: A Comparative Study*, edited by Ronald Leenes, Koops, Bert-Jaap, De Hert, Paul, 137-59. The Hague: Asser Press, 2008.

Kaczorowska, Alina. *European Union Law*. London and New York: Routledge-Cavendish, 2009.

Kane, Daniel. "Digital Dandelions: The Flowering of Network Research." *USCD News Center* no. August, 31 (2007).

Kang, Jerry. "Information Privacy in Cyberspace Transactions." *Stan. L. R.* 50, (1998): 1193.

Kang, Jerry, Buchner, Benedikt. "Privacy in Atlantis." *Harvard Journal of Law and Technology* 18, no. 1 (2004): 229.

Kee, Tameka. "Survey: More Employers Use Facebook to Vet New Hires Than Linkedin." *paidContent.Org: The Economics of Content*,no. 19 August 2009 (2009), http://paidcontent.org/article/419-more-employers-scanning-facebook-for-new-hires-than-linkedin/.

Keeton, W. Page, Prosser, William Lloyd. *Prosser and Keeton on the Law of Torts*. 5th student ed. ed, Hornbook Series: West Publishing co, 1984.

Komuves, Flavio L. "We've Got Your Number: An Overview of Legislation and Decisions to Control the Use of Social Security Numbers as Personal Identifiers." *J. MARSHALL J. COMPUTER & INFO. L.* no. 16 (1998): 529.

Koops, Bert-Jaap. "Conclusions and Recommendations." In *Constitutional Rights and New Technologies: A Comparative Study*, edited by Ronald Leenes, Koops, Bert-Jaap, De Hert, Paul, 265-87. The Hague: Asser Press, 2008.

———. "Law, Technology, and Shifting Power Relations." *TILT Law and Technology Working Paper Series* September, (2009).

Koops, Bert-Jaap, Groothuis, Magda. "Constitutional Rights and New Technologies in the Netherlands." In *Constitutional Rights and New Technologies: A Comparative Study*, edited by Ronald Leenes, Koops, Bert-Jaap, De Hert, Paul, 159-99. The Hague: Asser Press, 2008.

Korff, D. "EC Study on the Implementation of the Data Protection Directive - Comparative Summary of National Laws."

Kuner, Christopher. "An International Legal Framework for Data Protection: Issues and Prospects." *Computer Law & Security Review* 25, no. 4 (2009): 307-17.

———. *European Data Protection Law: Corporate Compliance and Regulation*. 2nd ed. New York: Oxford University Press, 2007.

Lagemaat, A.C., Boonk, M.L., Briet, M. "Vermogensrechtelijke Aspecten." In *Recht in Een Virtuele Wereld: Juridische Aspecten van Massive Multiplayer Online Role Playing Games.*, 21-40: Elsevier, 2007.

Lamb, Charles W., Hair, Joseph F. Jr., McDaniel, Carl *Marketing*. 10 ed: South Western Educational Publishing, 2008.

Lawson, F.H., Rudden, B. *The Law of Property*. 3rd ed, Clarendon Law Series: Oxford University Press, 2002.

Leenes, Ronald. "Do You Know Me? Decomposing Identifiability." *TILT Law & Technology Working Paper Series* no. 006/2008 (2008).

Leenes, Ronald, Koops, Bert-Jaap. "'Code': Privacy's Death or Saviour?" *International Review of Law, Computers, and Technology* 19, no. 3 (2005): 329-40.

Lenaerts, K., Vanvoorden, K. "The Right to Property in the Case Law of the Court of Justice of the European Communities." In *Property and Human Rights*, edited by H. Vandenberghe, 195-241: Bruylant, 2006.

Lessig, Lawrence. *Code 2.0*. New York: Basic Books, 2006.

———. *Code and Other Laws of Cyberspace*. New York: Basic Books, 1999.

———. "Privacy as Property." *Social Research: An International Quarterly of Social Sciences* 69, no. 1 (2002): 247 - 69

———. "The Law of the Horse: What Cyberlaw Might Teach." *Harvard Law Review* 113, (1999): 501.

Lievens, Eva, et al. "Constitutional Rights and New Technologies in Belgium." In *Constitutional Rights and New Technologies: A Comparative Study*, edited by Ronald Leenes, Koops, Bert-Jaap, De Hert, Paul, 11-57. The Hague: Asser Press, 2008.

Litman, Jessica. "Information Privacy / Information Property." *Stan. L. R.* 52, (2000): 1283.

Llewellyn, Karl. *The Common Law Tradition*. Boston: Little, Brown, 1960.

Lowery, David. *Interest Groups*.

Martin, Richard, J., Hoover, Nicholas. "Guide to Cloud Computing." In *Information Week: the business value of technology*, 2008.

Mayer-Schőnberger, Viktor. "Data Protection in Europe." In *Technology and Privacy: The New Landscape*, edited by P.E. Agre, Rotenberg, Marc, 219-43: The MIT Press, 1997.

Michaels, Ralf. "American Law (United States)." In *Elgar Encyclopedia of Comparative Law*, edited by Jan M. Smith, 66-78. Cheltenham and Northampton: Edward Elgar, 2006.

Migdal, Joel. *Strong Societies and Weak States. State-Society Relations and State Capabilities in the Third World*. Princeton, NJ: Princeton University Press, 1988.

Milo, Michael J. "Property and Real Rights." In *Elgar Encyclopedia of Comparative Law*, edited by Jan M. Smith, 587-602: Edward Elgar, 2006.

Moerel, Lokke. "The Long Arm of EU Data Protection Law: Does the Data Protection Directive Apply to Processing of Personal Data of EU Citizens by Websites Worldwide?" *International Data Privacy Law* no. November (2010): 1-19.

Moringiello, Juliet. "Towards a System of Estates in Virtual Property " *Int. J. Private Law* 1, no. 1-2 (2008).

Murphy, Richard S. "Property Rights in Personal Information: An Economic Defence of Privacy." *Geo. L.J.* 83, (1996): 2381.

Nabeth, Thierry. "Reply: Further Implications?" In *Profiling the European Citizen: Cross-Disciplinary Perspectives*, edited by Mireille Hildebrandt, Gutwirth, Serge. Dordrecht: Springer, 2008.

Neil Robinson, Hans Graux, Maarten Botterman, Lorenzo Valeri. "Review of the European Data Protection Directive: Technical Report Prepared for the Information Commissioner's Office." Santa Monica: RAND, 2009.

Nimmer, Melville. "The Right of Publicity." *Law & Contemp. Probs.* 19, (1954): 203.

Nwabueze, Remigius N. *Biotechnology and the Challenge of Property*. Edited by Sheila McLean, Medical Law and Ethics. Aldershot - Burlington: Ashgate, 2007.

Otjacques, Benoit, Hitzelberger, Patrik, Feltz, Ferdant. "Interoperability of E-Government Information Systems: Issues of Identification and Data Sharing." *Journal of Management Information Systems* 23, no. 4 (2007): 29-51.

Otter, Thomas. "Data Protection Law: The Cinderella of the Software Industry?" *Computer Law & Security Review* 23, (2007): 67-72.

Penner, J.E. *The Idea of Property in Law*: Clarendon Press, 1997.

Posner, Richard A. *Economic Analysis of Law*. 5th ed. New York: Aspen Publishers, 1998.

———. *The Economics of Justice*1981.

Poullet, Yves. "Data Protection Legislation: What Is at Stake for Our Society and Democracy?" *Computer Law & Security Report* 25, (2009): 211-26.

———. "The Directive 95/46/EC: Ten Years After." *Computer Law & Security Report* 22, (2006): 206-17.

Prechal, Sacha. *Directives in EC Law* Oxford European Union Law Library: Oxford University Press, 2005.

Prins, J.E.J. "Burgers En Hun Privacy: Over Verhouding En Houding Tot Een Ongemakkelijke Bezit." In *16 Miljoen Bn'ers? Bescherming van Persoonsgegevens in Het Digitale Tijdperk*, 3-15: NJCM, 2009.

———. "E-Overheid: Evolutie of Revolutie?" *Nederlands Juristenblad* 76, no. 11 (2001): 515-20.

———. "Name, Shame and Everlasting Blame." *NJB* 84, no. 3 (2009).

———. "Property and Privacy: European Perspectives and the Commodification of Our Identity." In *The Future of the Public Domain, Identifying the Commons in Information Law*, 223-57: Kluwer Law International, 2006.

Prins, J.E.J., Van der Hof, Simone. "Personalization and Its Influences on Identities, Behaviour and Social Values." In *Profiling the European Citizen: Cross-Disciplinary Perspectives*, edited by Mireille Hildebrandt, Gutwirth, Serge. Dordrecht: Springer, 2008.

"Privacy International Case Report." London: Privacy International.

PrivacyRightsClearinghouse. "The Privacy Implications of Cloud Computing ".

Proeller, Kuno Schedler and Isabella. "The New Public Management: A Perspective from Mainland Europe." In *New Public Management: Current Trends and Future Prospects*, edited by Stephen P Osborne Kathleen McLaughlin, and Ewan Ferlie: Routledge, 2001.

Prosser, William. "Privacy." *Cal. L. Rev.* 48, (1960): 383.

Purtova, Nadezhda. "Property in Personal Data: Second Life of an Old Idea in the Age of Cloud Computing, Chain Informatization, and Ambient Intelligence." In *Privacy and Data Protection. An Element of Choice.*, edited by Paul de Hert, Gutwirth, Serge, Poullet, Yves: Springer, 2011-forthcoming.

———. "Property Rights in Personal Data: Learning from the American Discourse." *Computer Law & Security Report* 25, no. 6 (2009): 507-21.

Raab, Charles D., Koops, Bert-Jaap. "Privacy Actors, Performances, and the Future of Privacy Protection." In *Reinventing Data Protection?*, edited by Serge Gutwirth, Poullet, Yves, de Hert, Paul, 207-25: Springer, 2009.

Radin, Margaret Jane. "Property and Personhood." *Stanford Law Review* 34, no. 5 (1982): 957-1015.

Reding, Viviane. "Towards a True Single Market of Data Protection Given at the Meeting of the Article 29 Working Party "Review of the Data Protection Legal Framework" Brussels, 14 July 2010." *Speeches of the Vice-President of the European Commission responsible for Justice, Fundamental Rights and Citizenship available on-line at* *http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/386&format=HTML&aged=0&language=EN&guiLanguage=en* 14 July, no. SPEECH/10/386 (2010): 1-4.

Regan, Priscilla. *Legislating Privacy: Technology, Social Values, and Public Policy*: The University of North Carolina Press, 1995.

Reich, Charles A. "The New Property." *Yale L.J.* 73, (1964).

Reid, Karen. *A Practitioner's Guide to the European Convention on Human Rights*. 3rd ed: Thomson, Sweet & Maxwell, 2008.

Reidenberg, Joel R. "Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?" *Fed. Comm. L. J.* 44, (1992): 195.

Reimann, Mathias. *The Oxford Handbook of Comparative Law*. Reinhard Zimmermann ed: Oxford University Press, 2006.

Rights, United States. Congress. Senate. Committee on the Judiciary. Subcommittee on Constitutional. *Federal Data Banks and Constitutional Rights*: U.S. Govt. Print. Off., 1974.

Robins, Kevin, Webster, Frank. "History of the Inforation Revolution." In *The Information Society Reader*, edited by Raimo Blom Frank Webster, Erkki karvonen, Harri Melin, Kaarle Nordenstreng, Ensio Puoskari, 62-80. London and New York: Routledge, 2004.

Robinson, Neil, Graux, Hans, Botterman, Maarten, Valeri, Lorenzo. "Review of the European Data Protection Directive: Technical Report Prepared for the Information Commissioner's Office." Santa Monica: RAND, 2009.

Rotenberg, Marc. "Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)." *Stan. Tech. L. Rev.* 1, (2001).

———. "The Privacy Act and the Data Protection Granted to Non US Citizens." In *Public Seminar on PNR/SWIFT/Safe Harbour: Are Transatlantic Data Protected?* Brussels, 2007.

Rouvroy, Antoinette, Poullet, Yves. "The Right to Information Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy." In *Reinventing Data Protection?*, edited by Serge Gutwirth, et al., 45-77. Berlin: Springer, 2009.

Rule, James. *Privacy in Peril: How We Are Sacrificing a Fundamental Right in Exchange for Security and Convenience*: Oxford University Press, 2007.

Rule, James, Hunter, Lawrence. "Towards Property Rights in Personal Data." In *Visions of Privacy: Policy Choices for the Digital Age*, edited by Colin J. Bennett, Grant, Rebecca, 168-81. Toronto, 1999.

Samuelson, Pamela. "Privacy as Intellectual Property?" *Stan. L. R.* 52, (2000): 1125.

Schatz Byford, Katrin. "Privacy in Cyberspace: Constructing a Model of Privacy for the Electronic Communications Environment." *Rutgers Computer & Tech. L.J.* 1, no. 24 (1998).

Schermer, B. and Wagemans, T. *Onze Digitale Schaduw. Een Verkennend Onderzoek Naar Het Aantal Databases Waarin De Gemiddelde Nederlander Geregistreerd Staat*. Amsterdam: Considerati, 2009.

Schrage, E.J.H. "Property from Bartolus to the New Dutch Civil Code of 1992." In *Property Law on the Threshold of the 21st Century*, edited by G.E. van Maanen, van der Walt, A.J., 35-69. Antwerpen-Apeldoorn: MAKLU Uitgevers, 1996.

Schwartz, Paul M. "Privacy and Participation: Personal Information and Public Sector Regulation in the United States." *Iowa L. Rev.* 80, (1995): 553.

———. "Property, Privacy, and Personal Data." *Harv. L. Rev.* 117, no. 7 (2004): 2055-128.

Schwartz, Paul M., Reidenberg, Joel R. *Data Privacy Law: A Study of United States Data Protection*. Charlottesville, Virginia: MICHIE Law Publishers, 1996.

Seligman, Edwin R.A. *Principles of Economics*1905.

Sjaak Nouwt, Berend R. de Vries, Corien Prins, ed. *Reasonable Expectations of Privacy?: Eleven Country Reports on Camera Surveillance and Workplace Privacy* Information Technology and Law: Asser Press, 2005.

Solove, Daniel J. "A Taxonomy of Privacy." *U. Pa. L. Rev.* 154, (2006): 477.

———. "Conceptualizing Privacy." *Cal. L. Rev.* 90, (2002): 1087.

———. "Privacy and Power: Computer Databases and Metaphors for Information Privacy." *Stan. L. R.* 53, (2001): 1393.

———. "The Darkest Domain: Deference, Judicial Review, and the Bill of Rights." *Iowa L. Rev.* 84, (1999).

Solove, Daniel J., Rotenberg, Marc; Schwartz, Paul M. . *Information Privacy Law*. New York: Aspen Publishers, 2006.

Steiner, Josephine, Woods, Lorna. *EU Law*. Oxford, New York: Oxford University Press, 2009.

Swadling, W.J. "Property: General Principles." In *English Private Law*, edited by P. Birks. Oxford: Oxford University Press, 2000.

———. "Property: General Principles." In *English Private Law*, edited by P. Birks. Oxford: Oxford University Press, 2007.

Taylor, Martic. *International Competition Law. A New Dimension for the WTO?* Cambridge: Cambridge University Press, 2006.

Tibben, Aad. "Genetic Discrimination in Huntington's Disease." *BMJ* 338, (2009).

Till, Hamilton &. "Property." *Ency. Soc. Sci.* no. 12 (1933).

Tilly, Charles. *Coercion, Capital, and European States, Ad 990-1990.* Oxford: Blackwell Publishers, 1998.

TransLinksSystemsB.V. "De Ov-Chipkaart and Uw Persoonsgegevens."

Treitel, Guenter. "Contract: In General." In *English Private Law*, edited by Andrew Burrows: Oxford University Press, 2007.

Tribe, Laurence *American Constitutional Law* 2nd ed1988.

Van der Meulen, Nicole. *Fertile Grounds: The Facilitation of Financial Identity Theft in the United States and the Netherlands*: Wolf Legal Publishers, 2010.

Van Dijk, Niels. "Intellectual Rights as Obstacles for Transparency in Data Protection." In *Mobile Marketing in the Perspective of Identity, Privacy and Transparency, Future of Identity in the Information Society (Fidis), D.11.12.*, edited by A. Deuker, 2009.

———. "Property, Privacy and Personhood in a World of Ambient Intelligence." *Ethics Inf Technol* 12, (2009): 57-69.

Van Erp, Sjef. "European and National Property Law: Osmosis or Growing Antagonism?" In *Walter van Gerven Lectures*: Europe Law Publishing, 2006.

———. "From 'Classical' to Modern European Property Law?" In *Essays in Honours of Konstantinos D. Kerameus/Festschrift Für Konstantinos D. Kerameus*, 1517-33. Athens/Brussels: Ant. N. Sakkoulas/Bruylant, 2009.

———. "From "Classical" To Modern European Property Law?" *Maastricht University Faculty of Law Working Papers* (2009).

———. "Security Interests: A Secure Start for the Development of European Property Law." In *Sicherungsrechte an Immobilien in Europa*, edited by Hinteregger M. and Boric T., 3-39. Vienna/Berlin: Lit Verlag, 2009.

———. "Security Interests: A Secure Start for the Development of European Property Law." *Maastricht University Faculty of Law Working Papers* (2008).

Viergever, Lieneke. "Privacy in De Cloud." *Tijdschift voor internet recht* 2010, no. 3 Junie (2010): 78-86.

Vogt, Roy. *Whose Property? The Deepening Conflict between Private Property and Democracy in Canada*. Toronto: University of Toronto Press, 1999.

Warren, Samuel, Louis Brandeis. "The Right to Privacy." *Harvard Law Review* 4, (1890).

Weber, H. Rolf. "Internet of Things - New Security and Privacy Challenges." *Computer Law & Security Report* 26, no. 1 (2010): 23-30.

Weinrib, Arnold S. "Information and Property." *University of Toronto Law Journal* 38, (1988).

Westin, Alan F. *Privacy and Freedom*. London, Sydney, Toronto: the Bodley Head, 1967.

White, G. Edward. *Tort Law in America : An Intellectual History*. Expanded ed ed. New York Oxford University Press, 2003.

Whitman, James Q. "The Two Western Cultures of Privacy: Dignity Versus Liberty." *Yale L.J.* 113, no. (2004): 1151.

Wieneke, Dave. "Is Linkedin for Sale? Does That Mean Your Personal Information Is, Too?" *UsefulArts.us: Online Law Blog: How trademark, copyright, privacy and politics shape the Web.* (2008), http://usefularts.us/2008/06/18/is-linkedin-for-sale-does-that-mean-your-personal-inforamtion-is-too/.

Wong, Rebecca. "Social Networking: Anybody Is a Data Controller?" *Social Science Research Network* (2008).

Wood, Stacy L., Moreau, C. Page. "From Fear to Loathing? How Emotion Influences the Evaluation and Early Use of Innovations." *Journal of Marketing* 70, no. 3 (2006): 44-57.

Wright, David, Gutwirth, Serge, Friedewald, Michael, de Hert, Paul, Langheinrich, Marc, Moscibroda, Anna. "Privacy, Trust and Policy-Making: Challenges and Responses." *Computer Law and Security Review* 25, (2009): 69-83.

Zarsky, Tal Z. "Desparately Seeking Solutions: Using Implementation-Based Solutions for the Troubles of Information Privacy in the Age of Data Mining and the Internet Society." *Maine Law Review* 56, no. 1 (2004).

Zweigert, Konrad, Kötz, Hein, Weir, Tony. *Introduction to Comparative Law*. Oxford [etc.]: Clarendon Press, 1998.