Université de technologie de Compiègne

École doctorale « Sciences de l'ingénieur »

Laboratoire COSTECH, EA 2223

Data Protection and Right to Privacy.

Investigating the Contested Notion of "Personal Data"

PhD thesis in information and communication sciences

Defended on July 2nd, 2020 in Compiègne.

Committee:

Serge BOUCHARDON – University Professor at Université de Technologie de Compiègne

Isabelle GARCIN-MARROU – University Professor at Sciences Po Lyon (reviewer)

Gloria GONZÁLEZ FUSTER – Research Professor at Vrije Universteit Brussel

Virginie JULLIARD – University Professor at Sorbonne Université

Valérie SCHAFER – University Professor at the University of Luxembourg (reviewer)

Jérôme VALLUY – Habilitated Associate Professor at Université Paris 1 Panthéon-Sorbonne, research fellow at COSTECH-UTC

Abstract

Internet and digital information and communication technologies in general are often portrayed as a threat to privacy. This gives rise to many debates, both in the media and among decision-makers. The Snowden revelations, in 2013, followed by the adoption in 2016 of the General Data Protection Regulation (GDPR), have moved these discussions under the spotlight of the public sphere.

The research presented in this dissertation was born out of three questions: can we define what "privacy" is? Is there any consensus on its definition? And does this consensus change with the evolution of the technical milieu transforming our ways of communicating, and by doing so, the way in which our privacy can be intruded upon?

By defining "privacy" as the object which is protected by normative texts – laws, court decisions, techno-political standards of the Internet – protecting the right to privacy, it becomes possible to conduct an empirical study of how it evolved and how it has been a topic of contention.

Data protection law emerged in Europe during the 1970's. Its aim was to protect a "privacy" that was perceived as under threat by the advent of computers. Currently, the GDPR, or some documents adopted by standards-settings organisations like the Internet Engineering Task Force (IETF) or the World Wide Web Consortium (W3C), are written with the intention that they protect this privacy through a set of rules and principles referred to as "data protection", that apply to "personal data".

The legal definitions of this notion produced by political institutions and those crafted in standards-settings bodies are identical. Furthermore, the study of the genealogy of data protection reveals that computer scientists have played a pivotal role in the invention of the principles that "data protection" still relies on, for instance in the GDPR.

The analysis of the controversies that took place in the shaping of these rules shows that the notion of "personal data" written down in the normative texts we analysed essentially reflects the beliefs system of a coalition inspired by liberal utilitarian ideals, valuing individual autonomy and granting importance to the respect of one's consent. This framing of "privacy" has become the paradigm on the field. Other theories, such as those defining "privacy" as a space bound by collectively defined borders protecting it from the public eye, or those advocating the recognition of private property rights on personal data, have been less successful in shaping policy outcomes.

The advent and spread of networked computers have not directly determined the evolution of the object that is protected by the right to privacy. It is, rather, the perceptions a group of actors had of computers, that caused such an evolution. Convinced that their liberal conception of privacy is socially valuable, they managed to craft a new legal category during the 1970's in Europe: the right to the protection of personal data. The GDPR, adopted in 2016, just like Web standards aiming at enhancing the protection of privacy, rely those same principles that were invented during these early debates. Therefore, it can be

said that the emergence of computers has indeed, but indirectly, been a triggering factor in the evolution of “privacy” defined as the object protected by the right to privacy.

Keywords : digitisation of communication, privacy, data protection, personal data, communicational theories of Law and public policy

Acknowledgements

I would like to thank my supervisors, Virginie Julliard and Jérôme Valluy, for their guidance, their advice, and for having made this research possible.

I would also like to express my gratitude to Jean-Jacques Lavenue, who supervised my Master’s thesis, and to Clément Fontan, Gloria Origgi and Iván Székely, whose advice has been extremely helpful to improve the quality of the research project I submitted to the Université de technologie de Compiègne in 2015.

I would not have been able to complete this doctorate without the financial and material support of this university and its COSTECH Research Unit, nor that of Université Rennes 2, the University of Szeged, as well as the ANR-ENEID, MSHB-Sensibdata and COMINLABS-PROFILE research projects. I met many great colleagues and friends there, and the many things I learned from them have been at least as valuable, if not more, than the material support I received.

I feel indebted to many other people who helped me along the way. I would like in particular to thank Attila Péterfalvi and Júlia Sziklay and all the former colleagues at the Hungarian National Authority for Data Protection and Freedom of Information, from the French National Commission on Informatics and Liberty, and the Center for High Studies of the Ministry of Interior.

I would like to thank all of those who agreed to help me in my research by agreeing to answer my questions, and all those who gave me access to useful documents and archive materials.

Finally, special thanks go to my family and friends for having not only supported me, but also tolerated my lack of availability as well as my many ramblings on data protection and academia, for five long years.

Table of Contents

Introduction

Many perceive the Internet, and computers in general, as a threat to privacy. More than two French citizens out of three express concerns over this topic (BVA 2018, 3). For many, the Snowden revelations strengthened the impression that they were living in world resembling that of George Orwell's novel *1984* (Orwell 1949). Yet, despite expressing such worries, many still behave in a way that appears to weaken their privacy online, either because they share matters they themselves would deem private, or because they choose to use services that are known to be privacy-intrusive. This has been described in the academic literature as the "privacy paradox" (Acquisti and Gross 2006; Acquisti, Ida, and Rochelandet 2011; Estienne 2011; Martin-Juchat and Pierre 2011; Norberg, Home, and Home 2007).

How does one define "privacy"? And do researchers share the same definition of what "privacy" as people they interview on the topic? If not, can we be sure that what appears as a paradox to a researcher also seems that way in the eyes of research subjects? And do scholars even agree with one another on the definition of privacy? This concept of "privacy" has indeed proven to be rather hard to define in a consensual manner. Some even call it an "essentially contested concept" (Mulligan, Koopman, and Doty 2016).

The "privacy paradox" has already been explained by many different factors (see, i.a., Gerber, Gerber, and Volkamer 2018; Hémont and Gout t.b.p.). But could it also be explained by looking at how different people define and understand "privacy" in different ways?

One possible definition of that word is that it designates the behaviour of a person reacting to a feeling of intrusion (Rey 2012, para. 20). Such feelings, and the ways in which one reacts to it, are culturally and historically situated, even if all societies have been shown to exhibit some form of privacy behaviour (Altman 1977; Ariès and Duby 1988; Moore 2003). If the material infrastructure that surrounds us contributes to the shaping of not only society, but also of the individual self (Bachimont 2010; Steiner 2010) then it can be posited that it has an impact on privacy. For example, the evolution of architecture in Western societies, with the fairly recent invention of the bedroom, has had both material and psychological consequences on the capacity of individuals to build both a place where they can be on their own and their sense of the self (see, i.a., Habermas 1988; Mumford 1938; Prost 1987). The evolution of the telephone offers another example. Whereas, decades ago, a telephone unit used to be shared by a group – at least a family, sometimes a whole village – and offered by limited privacy to its users, the smartphone has arguably turned into a symbol of the secrets of the self that are not even to be shared with one's closest relatives. It would thus appear logical that the emergence of networked computing also had an impact on "privacy", especially considering the many ways in which this technology is used to collect and process data on individuals, often for surveillance purposes. Did this also change social perceptions about "privacy"? Have "private" physical and informational areas of

life shrunk, or increased? Has “privacy” been forsaken as a “lost cause” anyway? Or has it changed its meaning altogether?

One approach to study the social meaning of “privacy” is to define it as the object of the right to privacy (see: Koops et al. 2016). Following this definition, we can observe its evolutions by looking at changes in legislation aimed at implementing this right to privacy. We can therefore look at whether computers and the Internet had an impact on “privacy” by looking at how privacy law evolved as these artefacts were introduced.

The research presented in this summary analysed the debates around the notion of “personal data” and its evolution over time. This controversy is not to be understood as being merely about what the *signification* of this term, but also about the *phrasing* of its written definition. Indeed, the precise wording of the latter has determining effects on the scope of application of data protection law. Data protection law is seen as substantiating both the right to privacy and the right to the protection of personal data, two distinct but related fundamental rights under the European Union’s Charter of Fundamental Rights (Clément-Fontaine 2017; González Fuster 2014a). Given that we just defined “privacy” as the object of the “right to privacy”, that data protection law is at least in part a component of this right, and that its remit depends on the definition of “personal data”, we may safely assume that there is a relation between the evolution of “privacy” and the evolution of “personal data”.

This brings us to the main research question, that we like to call by the rather hard to translate “problématique” in French academia:

> **To what conception(s) of “privacy”, as the object that is protected by normative texts, do the contested definitions of the notion of “personal data” refer to?**

Hypotheses

The hypotheses the reader will find the summary of hereafter are based partly on initial assumptions but are also inspired by observations made on the ground and rephrased into refutable hypotheses. This process therefore mixes elements of both deductive and inductive reasoning.

The first hypothesis is that computer scientists and lawyers differ in their understanding of privacy and data protection. Part of the academic literature supports this hypothesis and suggests, among other things, that this epistemic difference is reflected in the way each group defines “personal data” and/or “personally identifiable information” (see: Mascetti et al. 2013, and also: Meints 2009; Ohm 2010).

The second hypothesis is that is that formulas[1] such as “data protection”, “right to the protection of personal data” and the legal definition of “personal data” emerged as a consequence of *perceptions* of computers being a threat to privacy in particular or fundamental rights in general, but not as a mechanical, teleological or necessary consequence of changes in the technical infrastructure of society.

The third hypothesis is that the right to the protection of personal data and data protection law were invented in order to safeguard the effectiveness of instruments designed to protect an already pre-existing right: the right to privacy. If this is true, then the right to the protection of personal data is a part of the right to privacy, the latter covering a larger area than the former. However, although it is often hard, on the ground, to strictly distinguish discourses on “privacy” from those on “data protection”, the European Court of Justice (ECJ) has ruled that “personal data” and “data relating to the private life” are not to be confused[2].

Finally, and this is the fourth hypothesis, if the right to the protection of personal data and the right to privacy both protect the same thing, we may suppose they share the same genealogy and that the underlying values, ideas and ideological references they are the result of are either the same, or at the very least closely related.

Methodology

Public problems are shaped by social perceptions of reality. They are not direct, necessary and objective consequences of facts. For example, drunk driving has not always been construed as a public problem, that is to say, some thing that is undesirable and that public authorities and/or collective action should address (Gusfield 1994). Sometimes, newly emerging public problems give rise to new categories of collective action and/or public policy. For example, in France, the “politique de la ville” (“city politics”) was born in the 1970’s and 1980’s to address a set of issues plaguing poor neighbourhoods that were then construed as closely related (Tissot 2013). This is one example of the creation of a new “field of public action” (Dubois 2010), “sector of public policy” (Jobert and Müller 1987) or “policy sub-system” (Sabatier 1998; Sabatier and Jenkins-Smith 1993) among many others[3]. Today, such a policy sub-system is dedicated to what is referred to by the formula of “data protection” at the level of the EU (on this topic, see: Karaboga 2018).

Normative definitions of “personal data”, whether contained in legal texts or in technical standards, are an output of this policy sub-system. The latter consists not only of state actors, but also many interest groups and other private organisations, especially in the intersection between data protection policy and Internet Governance. The phrasing of these definitions is debated in different fora, and not only in what is traditionally referred to as the public sphere. This is why, while taking into account the existence of

1 A formula is defined by Alice Krieg-Planque as « a set of formulations that, due to their use at a given moment and in a given public space, cristalise political and social stakes while at the same time contribuing to the shaping of these issues » (Krieg-Planque 2009, 7).

2 ECJ, Judgement of 16 July 2015, ClientEarth and PAN, C-615/13 P, ECLI:EU:C:2015:489, §32

3 The relation between these terms is discussed in the full dissertation in French on page 58.

general debates on privacy and data protection happening elsewhere in the public sphere, my research focused on arenas that were "efficacious[4]" in the productionf of data protection policy instruments[5], but not necessarily easily accessible to the public.

Cognitive approaches to public policy analysis provide tools to study debates within a sector of public policy[6]. Such theoretical frameworks share an emphasis on the role of social representations, discourses and political theory in the production of policy outputs. According to Pierre Müller:

> "Shaping public policy is first of all about […] shaping a representation, an image of the reality one wishes to intervene on. It is as a reference to this cognitive image that agents organise their perceptions of the problem, confront their solutions and define their action proposals: this vision of the world is a public policy's frame of reference [*référentiel*][7]." (Müller 2011, 57)

According to Pierre Müller, each sector of public policy is governed by a *sectorial frame of reference*, meaning a set of values, goals and social imaginary that serves as a common paradigm for all agents in a given sector. In order for a sectorial frame of reference to successfully become or remain the paradigm of a public policy sector, it has to be articulated to a *global frame of reference*, which is "a social image of society as a whole, that is to say a global representation around which sectorial representations are organised and ranked against one another[8]." (Jobert and Müller 1987, 65). This global frame of reference is, today, largely derived from neoliberal ideology and monetarist economic theory (Hall 1986; Jobert 1994). Finally, I define a frame of reference, regardless of whether it is global, sectorial or neither, as any set of beliefs, values and social images that compete within a sector of public policy in order to become the sectorial frame of reference[9]. This framework was used to analyse the actors' discursive strategies on the field.

Paul Sabatier and Hank Jenkins-Smith's (1993) Advocacy Coalition Framework (ACF) emphasises, just like Pierre Müller's theory of the "référentiel", the role of social imaginaries in the shaping of public policy. It was also used in this research. Its analytical emphasis is not on how agents acting within a given sector of public policy manage to articulate their demands and discourses to the global frame of reference, but rather on the ideological rivalry between *advocacy coalitions* within what a single *policy sub-system*. These coalitions are alliances between agents sharing a "belief system" comprised of general values (the *deep core*), policy objectives (the *policy-core*) and concrete measures that are details of the desired policy instruments (called *secundary aspects* in the theory[10]) meant to meet the policy objectives set out in the policy-core. Following this framework, it is possible to map out competing discourses in a field of public policy, even when this controversy happens simultaneously in different fora, even when they cannot be grouped together within a single analytical

4 This term is borrowed from Nancy Fraser (2007) who describes the public sphere as something that, in theory, grants efficacy to the public opinion. Here, "efficacious" fora or arenas are where there is an effective link between a topic of discussion and the product upon which the discussion aims at producing effects.

5 For a definition of "policy instrument", see : Lascoumes 2004; Lascoumes and Le Galès 2005.

6 For a discussion on those approaches in English, see: Hall 2015.

7 Translated from French.

8 Translated from French.

9 These definitions are discussed more in-depth in pages 61 and 62 of the original dissertation.

10 However, these measures are in fact not "secundary" at all, as discussed in page 60 of the original dissertation.

public sphere, and even when part of the said controversy happens behind closed doors. Indeed, once the actors of a policy sub-system are known, it is possible to interrogate them about their beliefs, their goals, the concrete measures they are defending, and their alliances and rivalries.

Description of field work

Before conducting any field work, I started a review of existing discourses and theories available in publicly available literature, such as academic publications, essays, newspapers and magazines. Based on this material, I established an ideal-typical typology of theories on privacy and data protection presented in chapter 2 in the original dissertation, and summarised in the table below:

Name of the theory	Description
The liberal privacy paradigm	
Liberal privacy paradigm	This paradigm is described by Colin Bennett and Charles Raab (2003) and by Christian Fuchs (2011). It is a liberal utilitarian theory that values individual autonomy and self-determination, inspired by ideas similar to those defended by John Stuart Mill (Mill 1989 [1859]). Among others, Alan Westin (1967) had a significant influence on the shaping of this theory, which was later also influenced by elements of liberal constitutional theory, and then by the Foucaldian critique of panoptic social control.
Critiques of the liberal privacy paradigm	
The neoliberal critique	Several monetarist economists of the Chicago School of economics criticised the liberal privacy paradigm mainly because they viewed privacy as an obstacle to market transparency. They argued in favour of the recognition of private property rights on personal information, and against its regulation by statutory instruments and public oversight (see: Posner 1977, 1981; Stigler 1980).
The feminist critique	In short, the feminist critique points out how privacy and the right to privacy, as initially conceptualised by i.a. Samuel Warren and Louis Brandeis (1890), have been used in ways that prevented women from having access to the public space while denying them their autonomy within the domestic sphere. There are different strands within this critique of the liberal privacy paradigm, that are discussed in detail by Judith DeCew (2015).
Marxist and marxian[11] critique	This theory criticises the individual nature of the right to privacy as

11 Marxist critique follows the revolutionary ideals and the political values of Karl Marx. Marxian critics, on the other hand, apply Karl Marx's theories in their analyses without necessarily agreeing with his political objectives.

	defined by its liberal advocates, while at the same time considering the economic dimensions of how personal data is used in a capitalist economy. Examples of such critics are people like Stefano Rodotà (1974), Antonio Casilli (2013, 2015) and Christian Fuchs (2011).
The communautarian critique	Amitai Etzioni published a book called *The Limits of Privacy* in which he argued that liberal "champions of privacy" (Etzioni 1999, 7) gave too much room to individual privacy interests and choice compared to the interests a community may have in being able to process data on its members.
The contextual critique	Helen Nissenbaum is a philosopher proposing a theory of privacy that defines it as respect given to the contextual boundaries wherein personal information is socially expected to circulate (Nissenbaum 1998, 2004, 2010). She is sceptical about the possibility given to individuals by proponents of the privacy paradigm to consent to the processing of personal data. This is not only because she does not believe, in practice, that this consent is being collected in a meaningful way, but also because, for her, privacy is not about individual consent but about the respect of collectively shaped and defended contextual boundaries (Berinato and Nissenbaum 2018).
Political theories on technology that include discourses on privacy and/or the processing of personal data	
The Quantitative Self Movement (QSM)	The QSM advocates the practice of quantitative self-measurement, usually through the use of connected devices (see: Lanzing 2016). It is derived from techno-utopian imaginaries born in the 1970's in the United States (see: Flichy 2001; Turner 2008). It adheres to what José van Dijck calls the "dataist" paradigm (Dijck 2014), according to which the collection of massive amounts of quantitative data bears promises of innovation, growth and well-being, and applies it to the individual. Proponents of this movement do not see the collection and processing of personal data as an alienation of the self, but rather as something that empowers personal autonomy through greater knowledge and control of the self.
Digital sovereignty	Theories on technological sovereignty date back to the 1980's (Grant 1983). Because not all states have control over the increasingly sophisticated technological artefacts their societies rely on, they present contemporary technology as a potential threat to a desirable Westphalian model of national sovereignty. Discourses on digital sovereignty (Bellanger 2014; Nitot and Cercy 2016) apply this reasoning to digital technology and see the adoption of data protection legislation as an instrument promoting their aim with regards to where data on subjects of a sovereign state are being stored and processed (Couture and Toupin 2017).
The environmentalist critique	Arthur Miller, a legal scholar who also influenced the liberal privacy paradigm, started his book called *The Assault on Privacy* (Miller

	1971) by a long quote of Jacques Ellul's criticism of the technological system (Ellul 1954). In the 1980's, André Vitalis (1988) published his doctoral dissertation on "computers and freedom" in a book prefaced by Jacques Ellul. Their reflection on privacy thus began with a more global reflection of the relationship between humankind and its technical milieu, and a criticism of the development of certain artefacts, based on the same philosophical foundations that inspired environmentalist theories such as, for example, the contemporary Degrowth movement (see: Rossi 2016).

While the above table does not pretend to provide a complete list of all political theories formulating discourses on privacy and/or personal data, it provided a broad overview of the kind of ideas that discourses found on the ground may make references to.

While conducting field work, I tried to gather as many discourses as possible on "privacy" and/or "data protection" in general, and on the definition of "personal data" in particular, from a variety of actors, most of whom are or were involved in some capacity in the policy sector of "data protection". This was done by conducting semi-directed interviews with selected actors, by collecting documents (archives, policy papers, amendment proposals, e-mails…) related to the decision-making process, by conducting qualitative document analysis (Bowen 2009) and by attending public events where discourses on "data protection" are produced and arguments exchanged. In most interviews, I asked people about their motivation for being involved in the decision-making process, about what they perceived as the most important concrete measures that should be adopted, what they thought were the most "dangerous" proposals they had heard on the subject matter, how they argued against such "dangerous" proposals and what were the most common arguments they heard from their rivals. In order to test the second hypothesis of this doctoral research, I asked people about their general perceptions of "privacy", "data protection" and computers in general as often as possible given the time they could offer for the interview. In order to test the first hypothesis, I made sure to include people socialised to the law and institutional political as well as people socialised to engineering and computer science.

Each discourse collected on the field was linked to theories on privacy and/or personal data described in chapter 2 of the original dissertation and summarised in the table above. Explicit references to theories that had not already been taken into account in the general overview of theories on privacy and personal data were added to it as the research progressed.

The following table summarises the field work that was conducted to collect empirical data, described in further details in pages 70 to 105 of the original dissertation:

	Aim	**Collected data**
Field 1: exploration	Exploring hypothesis 1 (according to which there is an epistemic difference	10 qualitative semi-structured interviews (5 computer scientists and 5 engineers) + 96

	in lawyers and computer engineers' conceptions of "privacy" and/or "data protection").	answers in an on-line questionnaire.
Field 2 : Council of Europe and Organisation for Economic Co-operation and Development from 1968 to 1981	Studying the agenda-setting process that eventually led to the adoption of the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data and Convention 108 in 1980 and 1981, understanding the genealogy of "data protection", and observing the evolution of early versions of the definition of "personal data". Observing early interactions between lawyers and computer scientists in the shaping of data protection law.	9 semi-structured qualitative interviews (from 30 minutes to several hours) with actors or witnesses of the shaping of early data protection legislation. + Archive documents from OECD and the Council of Europe. + Legal material (bills, early laws, case law…) + Documents referenced in the collected material (essays, press articles, official reports…)
Field 3 : The adoption of the GDPR (2009-2016)	Identifying the advocacy coalitions at play in the EU's data protection policy sub-system, their underlying belief systems, and the main points of contention in the debates surrounding the Commission's proposal to reform EU data protection law. Understanding how these debates relate to discussions on the definition of "personal data."	10 semi-structured interviews with actors, mainly from interest groups, + Ethnographic and sometimes participant exploration of conferences and public events where actors of the policy sub-system socialise and debate, + 534 position papers and official documents retrieved from the Lobbyplag initiative's website and the EU Commission's website, + Various legal documents (draft legislation, legislation, regulatory guidance, case law).
Field 4 : The W3C Privacy Interest Group and Tracking Protection Working Group (2011-2018)	Understanding the functioning of standards-setting fora were techno-policy matters are discussed, and attempting to find differences (if any) between the content of debates and the structure of coalitions (if any) in technical standards-setting fora and in fields 2 and 3, to test hypothesis 1.	10 semi-structured interviews with members of either the W3C Privacy Interest Group (PING) or its Tracking Protection Working Group (TPWG) or both, + About 346 500 emails retrieved from public W3C mailing-lists (analysed with the help of custom Python scripts), + Various Internet and Web standards (and related official documents from standards-setting organisations, mainly IETF and W3C), +

		One day observation of PING's work during its Face-to-Face meeting at the W3C's Technical Plenary and Advisory Committee in Lyon, in October 2018.

It was often necessary to complement the theories and methods I just finished describing on certain fields. For example, the ACF is not really fitted for the study of the emergence of new policy sub-systems, so my work on the invention of data protection law borrowed a lot from the genealogical methodology (Koopman 2013). My work on the debates on privacy in the field of Web standards-setting took into account many elements from Internet Governance Studies (DeNardis 2014; Mueller 2010).

Chapter I: The invention of “Data Protection” in Europe (1968-1981)

Early debates on computers and privacy in the United States in the 1960’s

In the mid-1960’s, a public debate on the potential risks posed by computers to the right to privacy was already much underway. It led to the publication of several essays and reports and to the setup of two parliamentary inquiries into the matter (United States Senate 1967; US House of Representatives 1966). This led to the production of discourses and expertise that were then exported to Europe in the late 1960’s and early 1970’s. This is why studying how “privacy” and the link between computers and privacy was framed in American debates cannot be overlooked when studying the genealogy of European data protection law.

Back in 1890, Louis Brandeis and Samuel Warren published an article in the *Harvard Law Review* defending the recognition of a right to privacy, based on Common law, and defined as a “right to be let alone” (Warren and Brandeis 1890). However, it took until 1965 until the recognition of a coherent right to privacy[12] by the United States Supreme Court, which then ruled that the amendments to the federal constitution contained, *in penumbra*, a recognition of a fundamental right to privacy[13]. This decision is to be understood in a general context where privacy – and, actually, civil rights in general – had become prominent topics in the legal and political agenda of that country.

Indeed, the United States were at the time embroiled in protests against the Vietnam war, against racial discrimination, and were coming out of the McCarthy era. The latter is of a particularly high importance with regards to the debate on privacy. Indeed, many surveillance practices were developed in order to find out who had (real or supposed) sympathies towards the Soviet Union and communist ideas (Goldstein 2006) in the 1950’s, under the leadership of an influent Senator, Joseph McCarthy. These practices were denounced publicly in essays such as Vance Packard’s *Naked Society* (Packard 1965), who drawed a bleak picture of the rapid development of surveillance practices and trade in personal records across the country. Some public statisticians and early computer engineers also worried about what a lack of rules on the processing of digitised personal data could lead to (Atten

12 On the definition of the “coherentist” approach on the right to privacy, see: DeCew 2018. The opposite of the coherentist theory is called “reductionist”. Reductionists argue that the “right to privacy” designates an eclectic set of rights that are already protected under other branches of the law, such as property or personality rights (see: Thomson 1975).

13 See: U.S. Supreme Court 7 June 1965 Griswold v. Connecticut, 318 U.S. 479

2013; Kraus 2013; Ware 1967). Yet computers, at the time, were only one of many other matters of concern for privacy advocates.

One has to remember that, at the time, computers were enormous machines, very much linked in the public imaginary to images of the military-industrial complex (Turner 2008, 12). This view is reflected in this quote by Frank Horton, a representative in the State legislature of New York, who took part in the federal House of Representatives' hearings on computers and privacy in 1966, and in which he drew a parallel between computers and nuclear weapons[14]:

> "I have become convinced that the magnitude of the problem we now confront is akin to the changes wrought in our national life with the dawning of the nuclear age" (US House of Representatives 1966, 6)

Also, according to computer scientist Willis Ware:

> "Great quantities of private information are being accumulated in computer files; and the incentives to penetrate the safeguards to privacy are bound to increase. Existing laws may prove inadequate, or may need more vigorous enforcement." (Ware 1967, 14–15)

Finally, according to Cornelius Gallagher, chairman of the Special Subcommittee on Invasion of Privacy of the Committee on Government Operations in 1966, in what may be the earliest mention of a "right to be forgotten":

> "The possible future storage and regrouping of such personal information also strikes at the core of our Judeo-Christian concept of "forgive and forget," because the computer neither forgives nor forgets." (US House of Representatives 1966, 4)

The invention of Data Protection in Europe

Debates on the potential threat to the right to privacy posed by computers came to Europe in the late 1960's, early 1970's. Work done in the United States on the topic inspired European decision-makers:

> "When we started thinking about that, and discussing it, and trying to react to it, one of the main sources of inspiration of our reflection and of our expectations, was a continuous study on decisions, court decisions, in the United States, that had to do with automation. The Americans themselves had not yet a law. But they offered most of the material, because the automation in their industry […] was by far more developed than in Europe" (Interview with Spiros Simitis)

14 Science-fiction works from the era also tended to cast a rather worrisome light on computers. Besides George Orwell's famous *1984* novel (Orwell, 1949), one can also watch *2001, A Space Oddyssey* (Kubrick, 1968) or *Star Trek, Season 2, episode 26* (Roddenberry, 1968) to see how computers were depicted.

However, whereas Americans never adopted comprehensive data protection laws and favoured reliance on court decisions and market regulation[15], European lawmakers, most of whom were from countries with civil law traditions[16], responded relatively quickly with new legislation. The first law on the protection of personal data calling itself a Data Protection Law is the Hessian *Datenschutzgesetz* from 1970[17]. Sweden followed suit with a national law in 1973, the *Datalag*[18]. In 1974, Rhineland-Palatinate adopted its State Law against the misuse of personal data[19] and in 1978, France did the same with its *Loi informatique et libertés*[20]. Already at the time, these national laws shared many common features. Experts groups at the Council of Europe and the OECD helped coordinate and harmonise these laws, and offered a place where members of what would become a policy community dedicated to privacy would meet and come to a common agreement on what ought to be done[21]. As noted by Colin Bennett:

> "Convergence result[ed] from the interaction within a policy community which [was] bound by a shared expertise and motivation and which operate[d] initially above the fray of national politics." (Bennett 1992, 127)

In 1968, the Parliamentary Assembly of the Council of Europe adopted Recommendation 509 (1968) on Human rights and modern scientific and technological developments, which warned about threats posed by the development of new technologies for the right to privacy:

> "Believing that newly developed techniques such as phone-tapping, eavesdropping, surreptitious observation, the illegitimate use of official statistical and similar surveys to obtain private information, and subliminal advertising and propaganda are a threat to the rights and freedoms of individuals and, in particular, to the right to privacy which is protected by Article 8 of the European Convention on Human Rights" (Council of Europe, Recommendation 509 (1968), art. 3)

In 1971, the Committee on Legal Cooperation advised the Council of Europe to focus its work on the protection of privacy with regards to the registration and use of computerised personal data (Council of Europe, CCJ/Prot.Priv. (71) 6, p. 6). This was followed by the creation of an *ad hoc* expert group called the Committee on the Protection of Privacy vis-à-vis Electronic Data Banks, which held its first meeting on the 16th of June, 1972 (Council of Europe, CCJ/Prot.Priv. (71) 5).

The Organisation for Economic Co-operation and Development (OECD) started working on matters related to the computerised storage and use of personal data around the same time. However, it did not initially approach the matter from a human rights perspective, but rather from an economic and technological perspective. Indeed, as early as 1968, this international organisation expressed concerns

15 The 1974 Privacy Act only applies to federal agencies.

16 The opposition between Common Law and continental or civil law traditions in the framing of the debate on the use of computerised personal data is discussed in more details in section 3.7. of the original dissertation.

17 Hessische Datenschutzgesetz vom 7. Oktober 1970

18 Datalag (1973:289)

19 Landesgesetz gegen mißbräuchliche Datennutzung vom 24. Januar 1974

20 Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

21 To read more about the early stages of European data protection lawmaking and/or the formation of transnational policy community of privacy advocates, see: Bennett 1992; Bennett and Raab 2003; Flaherty 1989; González Fuster 2014; Hondius 1975.

about gaps in computer technology between member states, and started to produce reports on computer networks and flows of electronic information (OECD, DAS/SPR/68.1 and DAS/SPR/68.10). The Computer Utilization Group (CUG), that published a report in 1971 on national legislative developments and its impacts on the flows of data across OECD member states (Niblett 1971), and its successors, had a close relationship with its Council of Europe counterpart. Some experts, such as Louis Joinet, who had a large influence on the French *Loi Informatique et Libertés*, were at some points members of both groups.

In 1980, the OECD adopted its Guidelines on the protection of personal data and transborder flows of personal data[22], and the Council of Europe did the same with Convention 108 in 1981. Both documents contained similar sets of principles.

The Invention of the Data Protection Principles

Both Convention 108 and the OECD Guidelines contain so-called “Data Protection Principles”, that are now also contained in the GDPR. Article 5 of the latter define them as “lawfulness”, “fairness”, “transparency”, “purpose limitation”, “data minimisation”, “accuracy”, “storage limitation”, “integrity” “confidentiality” and “responsibility”. Chapter III contains provisions concerning data subject rights. The OECD Guidelines call them “Collection Limitation”, “Data Quality”, Purpose Specification”, “Use Limitation”, “Security Safeguards”, “Individual Participation” and “Accountability”. Article 5 of Convention 108 does not give them a name, but together with article 7 and 8, they provide for similar principles that are to be abided by data controllers whenever they are processing personal data[23].

A similar set of principles can also be found in Resolution 22 on the protection of privacy of individuals vis-à-vis electronic data banks in the private sector of 1973 and Resolution 29 on the protection of individuals vis-à-vis electronic data banks in the public sector of 1974 of the Council of Europe. A report published under the direction of computer scientist Willis Ware, for the Health, Education and Welfare Department of the United States (the ‘HEW Report’), also proposed applying “Fair Information Principles” to the processing of personal information (Ware 1973).

Contrary to what can often be read, the HEW Report was not the first document making such a proposal. The ideas that have been codified as principles can be found as early as a 1971 report submitted by the British Computer Society (BCS) to the Younger Committee, that had been set up by the British government to make proposals to reinforce the legal protection of the right to privacy. In its contribution, the BCS already talked about the importance of purpose limitation, data minimisation, transparency and the right to access and rectification (this right already existed in the Land of Hesse) (British Computer Society 1971). These ideas were then rephrased as “principles” in the Younger

22 To read more about the development of these guidelines, see: Kirby 2017

23 Except, in the case of OECD guidelines, when “because of the manner in which they are processed, or because of their nature or the context in which they are used”, such processing operations do not “pose a danger to privacy and individual liberties.”
More information can be read on this the topic of Data Protection Principles in section 3.2.5., 3.4.4. and 6.6. as well as appendices 1 and 13 of the original dissertation.

Committee's final report (Younger 1972, 18) and then, G.P. Pratt, one of its members, went to Strasbourg to present them to the Council of Europe's expert group on privacy vis-à-vis electronic databanks to which he had also been appointed (Council of Europe, EXP/Prot.Priv./EDB (72) 5 Rev, pp. 12-16).

This shows that the great principles data protection law still relies on today were not invented only by people socialised to law, but are the result of early interactions between computer scientists, legal scholars and civil servants working together to invent a regulatory framework to protect privacy against the advances of electronic information processing. It therefore contributes to the invalidation of hypothesis 1.

The liberal privacy paradigm and the formation of the privacy community

As mentioned earlier, the existence of experts groups at the Council of Europe and OECD allowed a group of people from different countries, many of them still quite young, and convinced by the need to safeguard human rights, to meet and exchange ideas on how to (in their eyes) improve existing legislation to better protect privacy (and/or, later, also data protection as a separate category of human rights). Many of these people, like Hans Corell, Jan Freese, Peter Hustinx, Louis Joinet, Michael Kirby, Stefano Rodotà or Spiros Simitis, later occupied important decision-making positions either in newly created data protection authorities or in other capacity, and kept in touch to coordinate their activities and political strategies. The role of this community has already been described in the literature (see, i.a., Bennett 1992, 2008; Flaherty 1989; Newman 2008). As Priscilla Regan wrote in 1995:

> "At the time privacy issues were added to the public agenda in the 1960s, a privacy community interested in legislation had not yet formed. By the late 1970's, however, a core policy community interested in general privacy existed along with specialized privacy communities, or advocacy coalitions, concerned with specific aspects privacy, including information privacy, communication privacy and workplace privacy" (Regan 1995, 20–21)

Their influence was instrumental to the adoption of data protection instruments at least from the early 1970's to the mid-1990's (Newman 2008). Charles Raab and Colin Bennett (2003) noted in their book called *The Governance of Privacy* that this policy community was inspired in great part by what they called the liberal privacy paradigm. This belief system emphasises the importance of individual autonomy, and seems inspired by the utilitarian tradition of liberal political philosophy (Mill 1989 [1859]). From this perspective, the right to privacy is defined as necessary to exercise control over's one's life. This shifted the definition of "privacy" from something that is a *collectively* defined area that

should be kept out of the public eye to something that is defined by the *choices* of an *individual*. American authors like Edwards Shils (1966), Alan Westin (1967) and Arthur Miller (1971) were particularly influential in shaping this shared framing of "privacy".

In terms of concrete measures – Paul Sabatier and Hank Jenkins-Smith's "secundary aspects" – this belief system led to a definition of "personal data" that does not require the content of the data to be "private" or "intimate" for data subjects to be able to exercise control over them (each individual data subject makes his or her decision instead of the lawmakers making that decision in their stead), and gradually to a strong emphasis put on consent as a legal basis for processing (already present in French law in 1978, for instance).

"Privacy" was not the only human right this privacy community was concerned with[24]. The balance of power, due process, and the autonomy of the human self towards machines and data controllers were also high on the list of what early privacy advocates defended[25]. According to Peter Hustinx, who was interviewed in the frame of this research, the need for a legal instrument to balance the right to privacy against freedom of expression also contributed to the emergence of the term "data protection law" to designate this new area of law in between all these different rights.

Articulating the liberal privacy belief system with the modernist keynesian global frame of reference

Modernisation through state intervention within a capitalist society was the global frame of reference in Western Europe during the 1970's (Hall 1986; Müller 1984; Rosanvallon 1989). It was largely compatible and/or inspired by Keynesian economic theory (Keynes 1997 [1936]). This belief system acted as a paradigm across and above all public policy sectors until the 1980's turn towards neoliberal ideology. It was favourable to the exploitation of personal data in order to improve the efficiency of state intervention in society. As G.B.F. Niblett reminded his readers in the report he published in 1971 for the OECD:

> "A principal function of the public sector, of government departments and central and local authorities, is the collection, evaluation and transmission of information and the carrying of this function in an efficient and economic manner." (Niblett 1971, 10)

This perspective helps understand the push towards the automation of information processing by state administrations. This is why many countries started using computers to conduct their national censuses (see: Atten 2013; Holvast 2013 for examples in the United States and in the Netherlands). Computers

24 Credit for the mention of the place of preoccupations for due-process rights in the genesis of data protection rights is to be given to René Mahieu, who studies this and has given talks about it. Sadly, his works on this topic are not published yet, but one should keep an eye out and read them as soon as they are.

25 These aspects are discussed in detail in section 2.2., 3.3.1. and 3.6. of the original dissertation.

were perceived by many decision-makers as tools that would help them bring better informed and more rational decisions. As Spiros Simitis recalled in an interview given in the frame of this research:

> "There was an evident opposition. Because the governments, parliaments, were persuaded that you enter a new state in the decision process. And that new state in the decision process would allow you, I would say, the utmost objectivity." (Interview with Spiros Simitis)

The collective response of privacy advocates to this opposition Spiros Simitis referred to in the above quote was to articulate their demands with the global frame of reference by saying that the "data protection" laws they were promoting would guarantee "trust" in computers.

As such, according to the British Computer Society:

> "For any legislation to control data banks to be equitable it must take account of the emotional **distrust**[26] which they arouse, and the constraints on the development of potentially beneficial data banks which this may produce. **Further legislation should both allay public fears**, and permit development by operators in an atmosphere reasonably free of the apprehension these engender." (British Computer Society 1972, 18)

The HEW Report, in the United States, expressed the same discourse:

> "[…] as in the case of campus protests against computerized registration systems, the apprehension and distrust of even a minority of the public can grossly complicate even a safe, straightforward data-gathering and record-keeping operation that may be of undoubted social advantage." (Ware 1973, 29)

Several speakers at a conference organised by the OECD in 1974 on the topic of data protection, attended by many members of the early privacy community, like Spiros Simitis and Alan Westin, expressed a similar need for the "trust" of the public in the development of electronic information processing systems (Blekeli 1974; Svenonius 1974).

The global goals to improve administrative efficiency through the digitisation of data processing were not put into question in those discourses. For example, the explanatory memorandum presenting the draft 1973 Resolution on the protection of privacy of individuals vis-à-vis electronic data banks in the private sector of the Council of Europe states that:

> "[…] in order to avoid any misunderstanding, the preamble reaffirms that the use of computers for purposes of public administration should in general be regarded as a positive development. The purpose of the present Resolution is not to oppose such use, but to reinforce it with certain guarantees." (Council of Europe, EXP/Prot.Priv. (73) 11, p. 6)

This strategy was successful in legitimising the demands for "data protection" in a global policy context where automatic processing of as much data as possible was perceived as a crucial tool to enhance the efficiency of state intervention for the public good.

26 Emphasis added by the author.

Chapter II: The discussions on the European Union's General Data Protection Regulation (2009-2016)

A quick introduction to the GDPR

During the 1970's and the 1980's, the European Commission ignored repeated demands made by the European Parliament to adopt data protection instruments in Community law[27]. It collectively argued that this was a fundamental rights issue that was outside of its remit, and, later, stated that Convention 108 was a sufficient instrument and called on member states to ratify and implement it[28]. However, under the pressure of the network of existing national data protection authorities acting as transgovernmental entrepreneurs (Eberlein and Newman 2006; Newman 2008), the European Economic Community (EEC) finally adopted a Data Protection Directive in 1995 under article 100A on the approximation of national provisions affecting the internal market of the Treaty establishing the European Community[29]. Since that time, data protection law has become part of Community law, and the EU has become one of the main – if not the main – locus of production of data protection norms.

The European Commission started communicating on its intention to reform existing data protection law in 2009, when Jacques Barrot was still Commissioner for Justice, Freedom and Security, right before the final adoption of the directive amending the 2002 e-Privacy directive[30]. The Division on data protection was still under DG Freedom, Justice and Security (DG JLS), which later split into DG JUST – responsible for data protection – and HOME for Home Affairs. Public consultations were held in 2010 and 2011, of which we have collected and analysed the submissions made by a wide variety of actors.

The Commission published the contents of its proposals in January 2012. It included a proposal for a General Data Protection Regulation (now Regulation 2016/679/UE, the GDPR) and an *ad hoc* directive governing the processing of personal data for police and justice in the frame of criminal matters[31]. Both

27 See, i.a., Resolution of 21 February 1975 on the protection of the right of the individual in the face of developing technical progress in the field of automatic data processing. Similar resolutions were adopted in 1976, 1979 and 1982. See the work done by Abraham Newman (2008) on this topic.

28 See: Commission Recommendation 81/679/EEC of 29 July 1981 relating to the Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data.

29 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 on the free movement of such data.

30 Directive 2009/136/EC of 25 November 2009 of the European Parliament and the Council amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws

31 See communications 2012-010 and 2012-011 of the European Commission.

were adopted in April 2016 and they came into application in the EU respectively on May 25th, 2018 and May 6th, 2018[32].

The GDPR follows in the footsteps of the 1995 Directive. Most definitions and principles have remained identical, at least semantically. Changes focused on implementing a compliance approach (Favro 2017) into data protection law, on significantly increasing the maximum amount of administrative fines, and on increasing cooperation between the EU's data protection authorities (see section 4.1.3.).

The discussions on this Regulation were quite heated. An imposing number of amendments were tabled by Members of the European Parliament (MEP's). Based on the topic of these amendments and on what actors on the ground identified as important to their eyes, these were the main points of contention[33]:

- How much sovereignty should be transferred to the EU in general and the European Commission in particular by member states in the field of data protection? Should the GDPR really be a regulation, or would a directive be preferable? Should the Commission be able to adopt delegated acts? (see section 4.3.2.)
- What role should consent have as a legal basis for the processing of personal data, and should it be defined as "explicit"? (see section 4.3.3.)
- How should "personal data" be defined? Should there be a legal definition of "pseudonymous" data, and to what extent should the principles of data protection apply to "pseudonymous" or "pseudonymised" data? (see sections 4.3.4. and 6.4.)
- Although there was rhetoric consensus on the desirability of a "risk-based approach", should it mean that "low-risk" processing operations are to follow more flexible rules than those established under the 1995 Data Protection Directive, or that "high risk" processing operations should be subject to additional requirements? (see section 4.3.5.)
- Should automated decision-making be banned, and/or how should it and profiling be regulated? (see section 4.3.6.)

Identifying the structure of the advocacy coalitions

Most studies implementing the Advocacy Coalition Framework (ACF) have found that the policy sub-system they were studying was structured around a rivalry between two opposing advocacy coalitions[34]. This was no different for the field of EU data protection policy, for which we identified two coalitions:

32 A full chronology is presented in Appendix 3 of the original dissertation.
33 The method used to identify the main points of contention are detailed in section 4.3.1. of the original dissertation.
34 See, for example: Bellon 2019; Bergeron, Surel, and Valluy 1998; Kübler 2002; Mawhinney 1993.

- A coalition of privacy advocates, focused around non-profit and purposive Non-Governmental Organisations (NGO's) such as European Digital Rights (EDRi) or the *Bureau européen des unions de consommateurs* (BEUC) and data protection authorities (DPA's);
- An industrial coalition, mainly structured around industrial interest-groups from the advertisement, financial and technology sectors.

This structure around the conflict between the privacy advocates and the industry was expressed in several interviews. For example, one lobbyist expressed that: "You can't be too much to EDRi, or BEUC, you can't be too much Microsoft and Google, you have to find the right balance." (Euro5 Interview). It is also what can be observed in this graph where each proposed amendment is mapped to an MEP who signed it and to an interest group that had proposed exactly the same text, based on data provided by the Lobbyplag initiative[35]:

This graph, rendered by Gephi, clearly shows European Digital Rights (the big yellow circle on the right) on one side, and a variety of other interest groups having proposed less amendments, such as the

35 Lobbyplag is a website started as a common project by OpenDataCity and Europe v. Facebook. Its aim was to make public a list of amendments that were copy-pasted from proposals made by lobbies. The data they used, which included many position papers, was made available on their Github repository: https://github.com/lobbyplag .

American Chamber of Commerce and Amazon on the other. The collection of amendment proposals (by MEP's and by interest groups) by Lobbyplag was incomplete. It remains a valuable source of information, but it does not provide proof on its own that the policy subsystem is structured along this single line of divide. Still, because this rivalry between two coalitions was also reflected in the narrative of interviewed actors, it is reasonably safe to conclude that there were indeed only two competing advocacy coalitions.

The dialectic opposition between the industrial coalition and the privacy advocates

In their discourses, actors from the industry coalition underlined the importance economic growth had to their eyes as a public interest to which innovative practices requiring the processing of personal data were presented as being instrumental. In the dissertation, this was called the "right balance" argument. It was articulated to the global objectives presented in the EU Commission's H2020 strategy for a "knowledge-based economy". This approach is well expressed in this quote from a position paper written by the Industry Coalition for Data Protection (ICDP), regrouping actors such as the Interactive Advertisement Bureau, DIGITALEUROPE and the Business Software Alliance:

> "We urge the European Commission to **balance** in a sensible manner the protection of individual rights with the functioning of the Single Market. The ability of the **European Information Society** to generate **innovation** and **growth**, as envisaged in the **European Commission's Digital Agenda**, depends on creating the necessary trust, but also on the continued use of all kinds of data that are at **the heart of the digital economy**. Overly strict, static and bureaucratic data protection rules will have a detrimental impact on **Europe's digital economy**. The **Single Market** benefits from open competition. Today and in the future data based business activities are the core instruments to allow any such competition to take place[36]." (Lobbyplag collection, ICDP1[37], 2011, p. 2)

Privacy advocates expressed motivations based on their will to protect human rights. Strategically, they managed to articulate their demands, inspired, as we shall see, by the liberal privacy paradigm, to a neoliberal global frame of reference by insisting on the need for *trust* in data controllers in order for a "knowledge-based society", in alignment with the EU Commission's project for a "Digital Single Market", to be able to flourish. This was expressed, among others, by Anna Walkowiak, of Polish NGO Fundacja Panoptykon, in an interview:

> "Usually we respond by reminding them that when you look at some research about how people feel, they feel that they don't have power, that information about them… they don't know what's going on with information, and **it's a question of** […] **trust**, mainly trust. There should be some safeguards, some rules. […] **And you're trying to build on trust**. […] If you're able

36 Bold added by the author of this dissertation.
37 See: original dissertation, p. 639, for full reference details.

> to create trust, you have a new business model, **you can be competitive that way**." (Interview with Anna Walkowiak, Fundacja Panoptykon)

Joe McNamee, at the time executive director at EDRi, answered the question on how he replied to arguments made by somebody convinced by the arguments of the industrial coalition as follows:

> " I would point this [person] to the NTIA study from June last year, which showed that there is vast damage **to online trust**... NTIA being a government body, used very diplomatic terms to describe its findings. But it found that **45 % of US households are avoiding online transactions** because of fears of privacy invasion. And we in Europe have the possibility to reinforce our data protection to reduce that in Europe, and create a **trustworthy** environment in Europe." (Interview with Joe McNamee, from EDRi)

In the 1970's, the global frame of reference was Keynesian. Privacy advocates initially seemed to be mainly (but far from exclusively) concerned by intrusions into privacy by state actors rather than private companies. They underlined the need for trust in the development of state-run electronic information processing for the sake of efficient and "modern" policy-making. By contrast, while this worry of state surveillance has far from disappeared, as shown by the reactions to the Snowden revelations (Greenwald 2013; Musiani 2015), privacy advocates in the 2010's were dealing with a neoliberal global frame of reference emphasizing deregulation in general as a priority in order to encourage economic growth seen as a public good. Hence a shift of focus to the regulation of private data controllers that had already started in the 1990's during the negotiations on the Data Protection Protection Directive. However, the argument that "trust is needed, and (only) data protection can give you this trust" has remained successful in articulating the liberal privacy paradigm to the global frame of reference.

The stability over time of the liberal privacy paradigm as a sectoral frame of reference

The argument that the "Digital Single Market" needs citizens' "trust" was thus successful. The liberal privacy paradigm has remained a paradigm, or a sectoral frame of reference, in the field of European data protection public policy.

Throughout the debates on the GDPR, "privacy" was defined as "control", and not as a sphere protected by rigid and collectively defined boundaries. Exceptions, such as an attempt made by the Future of Privacy Forum (FPF), a think-tank financed by the industry, to reframe privacy as a matter "contextual integrity" where "consent" becomes less relevant (and therefore should not have to be "explicit") (Lobbyplag collection, document FPF1[38], 2013, p. 4), were rare. Indeed, according to Microsoft:

38 See full reference on page 639 of the original dissertation.

> "As a company committed to user privacy, we believe in being transparent with our customers about our data protection practices and **we work hard to develop innovations that empower our customers to exercise choice and control** over their personal information." (Lobbyplag collection, document MICROSOFT1[39], 2013, p. 1)

Lobbyists argued that requiring "explicit" consent too often would "undermine" the relevance of this consent because of what they referred to as "click fatigue":

> "Systematically requiring explicit consent may lead to practices which are both user unfriendly ('**click fatigue**') while not leading to a higher level of privacy protection for data subjects." (Lobbyplag collection, document TELEFONICA1[40], 2013, p. 8)

The argument was not that requiring consent was *irrelevant* or *undesirable*, but rather that requiring *explicit* consent every time would undermine its relevance. Some also argued that it would be paternalistic:

> "We believe that the review should be guided by a fundamental principal of the EU, namely the notion of the rational and informed consumer. Any over-protective regulation will convey a perception of a consumer who is vulnerable and ultimately unable to navigate through life without the encompassing protection of the government." (Lobbyplag collection, document FEDIL1[41], 2012, p. 3)

Privacy was kept defined as a way for an individual to exercise control:

> "We do not support the changes in the definition of consent as they will make the process too cumbersome and prescriptive. In case of continued business relationships, these requirements are an unnecessary supplementary administrative burden. **This is likely to turn consent into a box-ticking exercise rather than a way for data subjects to control their data**." (Lobbyplag collection, document BUSINESSEUROPE1[42], 2012, p. 5)

While we actively looked for examples of discourses against the right to privacy and/or data protection *as such*, we could not find any in the documents we collected. According to a lobbyist who asked to remain anonymous:

> "I think, you know, in these discussions, it was always coming from the premise that privacy is a fundamental right. So how do you argue ? I mean. We're all for… everybody wants to have the fundamental rights. It is very difficult to sort of deconstruct that argument. And obviously you have to recognise that."

39 See full reference on page 639 of the original dissertation.
40 See full reference on page 639 of the original dissertation.
41 See full reference on page 638 of the original dissertation.
42 See full reference on page 636 of the original dissertation.

Within the privacy community, or, in other words, the advocacy coalition of privacy advocates, there were some who criticised the role given to consent in data protection law and in the informational self-determination doctrine. For example, according to Lionel Maurel of French NGO La Quadrature du Net, “this approach actually relies on a legal fiction that online platforms are already exploiting: the isolated individual, capable of ‘self-determination’, who is therefore erected as the centre of gravity of regulation [on personal data]” (Aufrère and Maurel 2018). Others expressed the idea that to efficiently protect certain collective goods such as a well-functioning democracy, there is a need for a collective minimal level of privacy that individuals should not be able to waive. Finally, there was a lot of criticism directed towards the way that “consent” was collected in practice, often without making sure data subjects were adequately informed about the choices they were about to make, when they have any real practical or actionable choice at all[43].

However, this criticism directed towards the practice of consent collection by data controllers did not result in a turn away from privacy-as-control and informational self-determination, but in the opposite: a consolidation of the definition of “consent” in article 4 of the final version of the GDPR, and the addition of new procedural requirements on how to obtain it in article 7. Many privacy advocates even wanted to eliminate the “legitimate interests” from the legal grounds under which personal data processed, which would have resulted in an increased focus on consent, which they defined as having to be “explicit” (see, i.a., Lobbyplag collection, document EDRI2[44], 2012).

Furthermore, many privacy advocates expressed definitions of “privacy”, “data protection” and explained their commitment to their cause in ways that were all inspired by, or at least compatible with, the liberal privacy paradigm, together with its elements imported from Foucaldian theory on power and control. In an interview, Jens-Henrik Jeppesen of the Center for Democracy and Technology defined the right to privacy as a “right to be left alone” in what was a clear reference to Louis Brandeis and Samuel Warren’s definition (Warren and Brandeis, 1890). Joe McNamee, from EDRi, defined the right to privacy as something related to “autonomy”. Anna Walkowiak, from the Panoptykon foundation, insisted that personal data are “a tool to govern […] and to control” people. Finally, Jan Philipp Albrecht, the Green rapporteur of the GDPR in the European Parliament, perceived as close to the privacy community (if not one of its members) wrote that:

> “Consent should remain a cornerstone of the EU approach to data protection, since this is the best way for individuals to control data processing activities.” (Albrecht, 2013, p. 200)

Although, ultimately, the European Parliament and the Council of the EU adopted a Regulation that did not define consent as being always “explicit”, it did write that it has to be a “freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her” (art. 4 (11) GDPR). It is presented as the preferred ground for the processing of personal data[45].

43 To read more on this topic: Böhme and Köpsell 2010; Hémont and Gout t.b.p. ; Nouwens et al. 2020; Utz et al. 2019.

44 See full reference on page 637 of the original dissertation.

45 See Recital 40: “In order for processing to be lawful, personal data should be processed on the basis of the consent of the data subject concerned or some other legitimate basis […]”.

Furthermore, and as we shall see, personal data is still defined as related an *individual*, just like it was in previous data protection norms.

We may thus conclude that privacy advocates were still inspired by the liberal privacy paradigm in the 2010's, in its version updated with elements derived from Michel Foucault's work on social control. They managed to articulate this frame of reference to the neoliberal global frame of reference, where the latter advocates the use of personal data for the sake of growth defined as a collective interest. They succeeded by arguing that an instrument such as what became the GDPR would permit such use of personal data (and such economic growth) by fostering *trust* in the "digital economy". Finally, the industrial coalition, in the overwhelming majority of examples we found, either did not want to or failed to propose an alternative fundamental to the liberal paradigm's conception of what "privacy" is.

Chapter III: Web standards and “privacy”

Web standards and *Lex Informatica*

There is no unified government of the Internet, and no single government can effectively make decisions affecting the Internet. There is no single point of control. Yet, despite common misconceptions:

> “The Internet is governed” (DeNardis 2014, 222)

In this quote, however, “governed” is not a reference to “government”, but to “governance”. Indeed:

> “The term governance […] gained currency in international relations precisely because it was weaker than government ; it denotes the coordination and regulation of interdependent actors in the absence of an overarching political authority.” (Mueller 2010, 8)

Internet Governance (IG) brings together a multitude of actors of various types, including but not limited to governments. Its functioning does not reflect that of traditional public policy fora. Yet, decisions are made that do produce policy outputs.

These policy outputs involve different types of policy instruments. Laws may apply to online behaviour. But there are other tools to wield political power on the Internet, such the control of certain key elements of the technical infrastructure (Zittrain 2003). Source codes of software making the Internet run are also tools contributing to the governance of the Internet.

According to Lawrence Lessig, “Code is Law” (Lessig 1999). This now famous phrase alludes to the fact that computer source codes can produce regulatory effects on human behaviour. It carries a normative load in ways that he describes as similar to traditional law.

Joël Reidenberg coined the term *Lex Informatica*, which he defined as follows:

> “Technical capabilities and system design choices impose rules on participants. The creation and implementation of information policy are embedded in network designs and standards as well as in system configurations. Even user preferences and technical choices create overarching, local default rules. This Article argues, in essence, that the set of rules for information flows imposed by technology and communication networks form a “Lex Informatica” that policymakers must understand, consciously recognize, and encourage.” (Reidenberg 1997, 554–55)

Design elements are embedded into source codes run by computers on networks that together form the Internet, but they may be described in normative documents called technical standards. Standards edited by the Internet Engineering Task Force (IETF) are called Requests for Comments (RFC[46]) and are defined by this organisation as follows:

> “Standard: As used here, the term describes a specification of a protocol, system behaviour or procedure that has a unique identifier, and where the IETF has agreed that "if you want to do this thing, this is the description of how to do it". It does not imply any attempt by the IETF to mandate its use, or any attempt to police its usage - only that "if you say that you are doing this according to this standard, do it this way". The benefit of a standard to the Internet is in interoperability - that multiple products implementing a standard are able to work together in order to deliver valuable functions to the Internet's users.” (RFC 3935[47])

There is a rough distinction between standards developed by the IETF for the Internet as the underlying networked infrastructure connecting computers together and standards developed by the World Wide Web Consortium (W3C) for one of the Internet’s applications: the World Wide Web (in short: Web). The Web is constituted by documents linked together by hyperlinks. They are stored on computers hosting Web server applications, and accessed by client computers that are equipped with Web browsers. W3C standards are commonly called “recommendations” or, in web standards vernacular, “specs” (short for “specifications”). The procedure leading to the formal adoption of Web standards is described in the W3C Process Document[48].

Standards bear some resemblance to hard law instruments. They are normative, and they rely on performativity[49]. Unlike hard law, however, there is no court and law enforcement system to coerce their public into abiding by the rules they set out. Enforcement of these soft law instruments relies on different mechanisms, such as market adoption. On the other hand, once source codes implement design choices outlined in standards, they will always automatically enforce them.

Some of these standards are techno-political in nature. Techno-policy standards are defined by Deirdre Mulligan and Nick Doty as follows:

> “A small number of W3C working groups have been chartered specifically to consider interlinking technical and policy issues, defining what we might call a “techno-policy standard”.” (Doty and Mulligan 2013, 141)

46 For further reading on the history of RFC’s, see: Bing 2009.
47 The full references to Internet and Web standards are listed between pages 646 and 652 of the original dissertation.
48 See: https://www.w3.org/2019/Process-20190301/
49 For further reading on the performative nature of law, see, i.a.: Austin 1962; Laugier 2004; Reinach 2004.

These are standards that try to address a public policy issue – like privacy or accessibility – through normative descriptions of how the technical design of the Internet should evolve to either enable or disable certain possible uses. The Platform for Privacy Preferences (P3P) was a Candidate Recommendation intended to improve the protection of Web users' privacy once implemented by web browsers and websites[50].

Other standards, such as the W3C's Geolocation API, its Encrypted Media Extension or its Web Payments API, may affect public problems, such as privacy, intellectual property, access to culture or financial regulation, without being designed to address them as such, or with the intention to produce effects in the affected fields of public policy. Sometimes, consequences may not be intentional. For example, researchers have shown how possibilities created by the original Battery Status API could increase *fingerprinting surface* (Olejnik, Englehardt, and Narayanan 2017), a type of attack which uses technical information transferred during a network interaction between a client and a server, allowing the server to single out a device or a user without the latter being aware of such identification taking place.

The World Wide Web Consortium's Privacy Interest Group and Tracking Protection Working Group

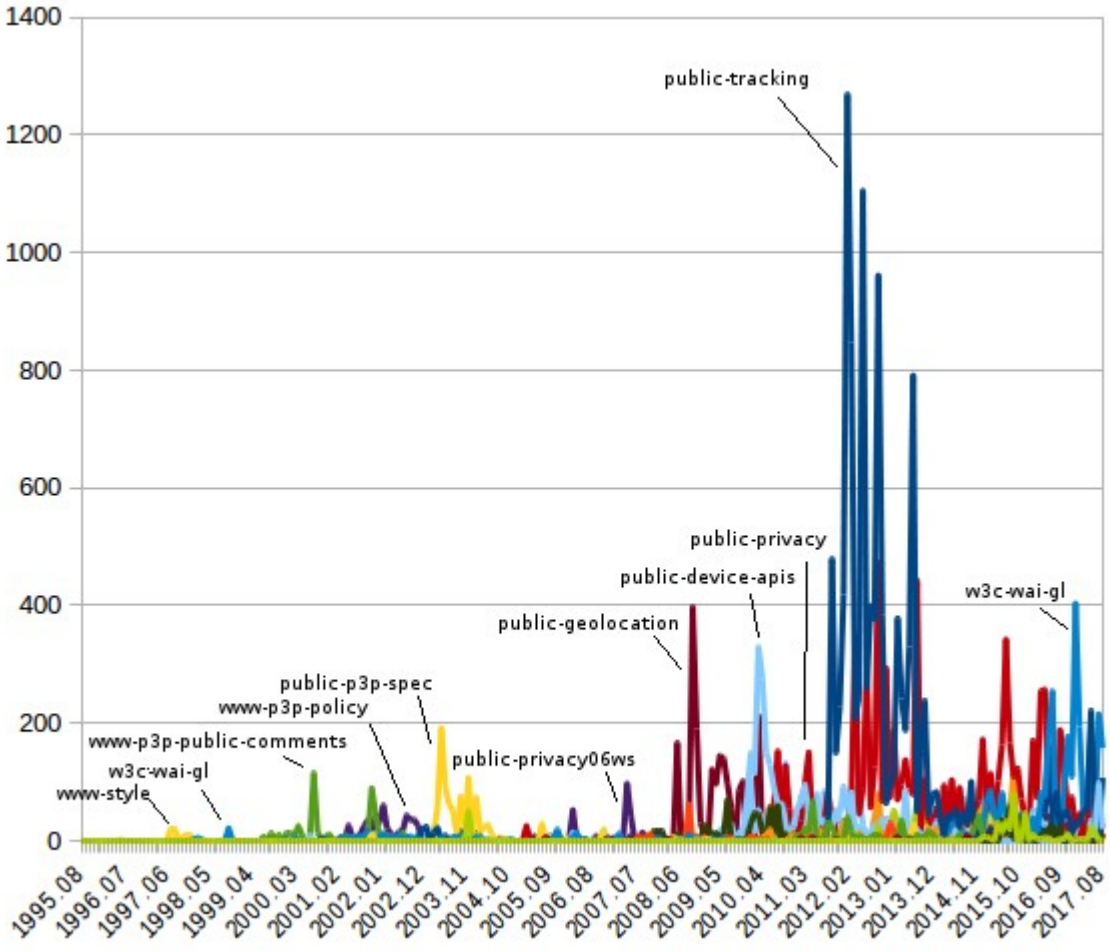
The Privacy Interest Group (PING) was formally set up in 2011 in order to advise the Working Groups of the W3C on how to design the recommendations they work on in a way that protects web users' privacy. Its creation follows a renewed interest in privacy among W3C members, following concerns raised during the discussions on the Geolocation API[51]. This trend is visible in the following graph, which shows the absolute monthly occurrences of the word "privacy" in 56[52] of the W3C's public mailing-lists[53]:

50 More on P3P in section 5.4.2. of the original dissertation. See also, in English: (Doty and Mulligan 2013).

51 More on this topic in section 5.4.3. of the original dissertation.

52 See table 7 in the original dissertation for the full list of these mailing-lists. All the mailing-lists referred to on the homepage of working groups and interest groups active at the time of the study were included, along a few others that were added due to their relevance to the topic of privacy. Community groups were excluded. The reason for limiting the scope was feasability and limited computer capacity.

53 More on how this type of graphics was produced in section 1.2.5.3. of the original dissertation.



Public-privacy is the name of the mailing-list connected to the PING. Public-tracking, in dark blue, also shows a lot of activity around “privacy”, and is the name of the public mailing-list attached to the Tracking Protection Working Group (TPWG).

The TPWG existed formally from 2011 to early 2019. Its members were working on a standard, called Do Not Track, which would have allowed a web user to send the signal that she does not want to be tracked while visiting a website. This would have been done through the settings of her web browser, to which the web server would have responded in a standardised way. Technically, this would have been made possible by adding new fields to HTTP headers and by standardising new Javascript methods to access user tracking preferences. The standard was described in two recommendation projects:

- The Tracking Preference Expression (TPE) document, which specifies how a web browser (or “user agent” in the vocabulary of the W3C) should communicate its user’s preferences with regards to tracking;
- The Tracking Compliance and Scope (TCS) document, which specifies how a website receiving a DNT:1 signal should react to comply with the standard.

Despite active initial support from the Federal Trade Commission (FTC) that contributed to the initial impetus around the project (Vladeck, 2011), Do Not Track failed to be implemented homogeneously by

browser makers, and few websites honoured the wishes of users. In the end, the Working Group was disbanded before the documents it was working on could progress to Recommendation status.

The TPWG and the PING were closely related. Many members of one group are also a member of the other. Their focus was also similar, even though the approach was difference: the TPWG attempted to produce a techno-policy standard protecting privacy, while the PING reviews projects by other groups to provide advice on their privacy impacts and desirable remedies or safeguards. The latter are written into “Privacy Considerations” sections of W3C recommendations.

The focus of the field study on the W3C in this doctoral research was the Privacy Interest Group (PING), because it provides advice on “privacy” in general. Its scope is not restricted to the matter of “tracking”. However, because of how interrelated both groups are, both in membership and in their subject matter, it was not always easy or possible to treat them separately.

Both groups proved relevant to study the way in which the normative debates on privacy defined as the object of the protection granted by the DNT specifications or the privacy considerations promoted by PING members. In contrast to experts groups in the Council of Europe and the OECD and to actors within advocacy coalitions taking part in the discussions on the GDPR, these groups were composed mainly by engineers socialised to computer science. Comparing discourses produced in these different kinds of fora contributed to the test of the first hypothesis, according to which legal experts and computer science experts held epistemically and normatively different views on “privacy” and “data protection”.

Debating the definition of “tracking”, but avoiding having to define “privacy”

The Advocacy Coalition Framework could not be applied as such to the study of the controversies on “privacy” in W3C groups. This was first of all the case because the production of standards does not work like traditional state-centric modes of policy production. It was also the case because identifying conflict was made difficult by the discourse ethics of communicative action (Habermas 1987) most participants adhered to. It was however possible to identify discourses on privacy, and even disagreements and strategic action by certain actors, despite the prevalence of discourse ethics as a social norm.

The adherence of participants in IG fora to discourse ethics has already been well described by Luca Belli, with regards to the Internet Corporation for Assigned Names and Numbers (ICANN) and the Internet Governance Forum (IGF) (Belli 2016). Indeed, in order to be successful, standards have to be implemented. But unlike what is the case with hard law, nobody can coerce actors of the socio-technical ecosystem to which a standard is designed for to obey it. This constraint is perceived within the field of IG standards-setting as an incentive for producing higher-quality documents (Alvestrand and Wium Lie 2009). Authors of standards have to convince implementers that what their documents describe is technically sound and that they have an interest in adopting it, until a point where the

unconvinced minority has no choice but to follow the lead of a convinced majority if they want their products to remain interoperable with the larger ecosystem. Yet nobody will want to implement a standard on their own, unless they are in a position of hegemony, because of the expenses that are involved, which may then end up being for naught if nobody else follows the lead. Any dissension within a group in charge of making progress on a given standard thus postpones the moment when all stakeholders come to a consensus and start implementation. For privacy advocates pushing for the adoption of a privacy-enhancing techno-policy standard, in a way, any standard may still be better than no standard at all. Disagreements on elements that they perceive as non-essential at a given stage in the process are therefore usually muted.

This concerns, among other things, any conceptual discussion on what "privacy" means. All interviewed participants insisted on the need to avoid "unnecessary" and time-consuming theoretical debates postponing technical decisions:

> "Certainly this idea of consensus and the multi-stakeholder process, and all that, which are done differently in different groups, where there are different dominating forces, is definitely an ongoing issue, and is something where it's difficult enough when the questions are fairly crisp for people to agree on what they think ought to be done. So then add to that that we're not really sure, even close, what the right to thing may be to do for asking various questions on things as nebulous as privacy, and it doesn't help the consensus process any, in general, I would say." (Anonymous participant)

> "So it's something that's been discussed in W3C staff and within the Privacy Interest Group, about whether we should have a formal motivating definition of privacy. And I don't think we really do at this point. And I'm not sure there is a strong culture to do so at the moment. […] The concept means different things to different people, and enough of those concepts are related that we can still do productive work in that we don't have exactly the same definition. […] You need to be able to do productive work." (Anonymous participant)

While most participants in the PING and in the TPWG kept their views on what privacy means to themselves, a heated debate on the definition of "tracking" took place between 2011 and 2013[54]. "Tracking", especially in this context, could be described as a partial opposite of "privacy". The debate can be followed on the archives of the public-tracking mailing-list. Relevant e-mails were grouped under a thread identified as "ISSUE-5[55]".

The issue was initially raised by Roy Fielding, co-editor of the TCS recommendation, famous within the standards-setting field for his work on the HTTP protocol. This move was criticised by some of the participants as either a waste of time or, worse, as a strategy to create dissensions on political or philosophical topics that would postpone work on what matters: a technical consensus that can be

54 For a full description of this debate, see section 5.5.4. of the original dissertation.
55 See: https://www.w3.org/2011/tracking-protection/track/issues/5

implemented. This was expressed, for example, by Jonathan Mayer, one of the early proponents of a Do Not Track standard:

> "The working group has now swirled around the "How do we define tracking?" and "How do we define Do Not Track?" drains several times. […] This approach is not productive. […] I would propose that we mark ISSUE-5 as POSTPONED since achieving consensus on it is not necessary to the working group's tasks." (public-tracking, e-mail by Jonathan Mayer, 10 December 2011)

One of the main issues at stake was whether only *third-party* sites should be bound by a DNT:1 signal, which indicates the user's demand not to be "tracked", or whether this should apply to both *first* and *third-parties*. In other words: even if third-party trackers installed on a website, for example on example.com, should not collect data on a user who has turned on the DNT signal, should example.com itself also refrain from tracking? Some, like Chris Pedigo, from the Online Publishers Association, saw the inclusion of first-parties in the scope of the project as a threat to the online media ecosystem[56]. On the other end of the debate, Rigo Wenning, a lawyer working for the W3C on privacy-related projects since the end of the 1990's, expressed during an interview his view that any exemption for first-parties would be a way to allow websites like Facebook to keep collecting data on their own registered users and visitors' behaviour despite them having turned the DNT signal on[57].

This debate was analysed in the research as being in part a discussion, by proxy, on "privacy", on what ought to be forbidden in order to protect that (privacy) which the Do Not Track standard aimed at protecting.

This work on the definition of "tracking" was conducted alongside semi-directed qualitative interviews with members of the PING and of the TPWG, in which they were asked questions about the definition and the value of "privacy". In both cases, the aim was to uncover the argumentative structure of debates on privacy that are often implicit due to the nature of standards-setting organisations as arenas of debate.

User control, user agency and informational self-determination

The image of the archetypical Web user occupies the centre stage in discussions on privacy at the W3C. Both those in favour and against the inclusion of *first-parties* in the scope of Do Not Track argued their position reflected the interests or expectations of users the best, like in the example below:

> "If a strictly-first-party can display an ad based on registration information and geoIP saying, "Welcome back, Julia from the New York Times! It's been 2 hours since you last visited this site. Let me tell you about the bake sale at the elementary school in your neighbourhood,", then I strongly believe user expectations for DNT are going to be violated in a non-trivial way." (*public-tracking*, e-mail by Aleecia McDonald, 12 October 2011)

56 See his e-mail sent on 30 November 2011 on the public-tracking mailing-list.
57 See quote on page 471 of the original dissertation.

Very often, privacy was defined directly or indirectly in documents, e-mails and interviews as “user control”:

> “Let's focus on providing consumers with greater transparency and **control**[58] over online data collection and usage.” (public-tracking, e-mail by J.C. Cannon (Microsoft), 23 October 2011)
>
> “Rather than seeing DNT as a “kill switch”, providing **user control** over a powerful process designed to influence their behavior and decision-making is a business practice that should benefit everyone.” (W3C Tracking Preference Expression, 19 October 2017)
>
> “It is important for users to be able to control access to their data.” (W3C PING Privacy Considerations document)
>
> “So there is a form of definition, […] I think: **user control**. And so there has been a lot of focus on things like: talking about permissions, consent, in the web model, having a user agent... The idea is supposed to be that **you have this piece of software that is working on your behalf, that you have this control over**.” (Anonymous interview)

This notion of “user control” appears very close to what lawyers in Europe would call a right to self-determination of the said user. Defining “privacy” as “user control” means defining it in a way that revolves around the individual and her choices. As such, it fits within the frame of the liberal privacy paradigm.

Yet participants to the PING and the TPWG, both those in favour of strict Do Not Track rules applying to *first-parties* and those promoting less stringent ones, often referred to “contextual integrity”, a concept proposed by Helen Nissenbaum, who is also very critical of the idea of consent and individual control (Nissenbaum 2004)[59].

According to Chris Pedigo, from the Online Publishers Association, it would be legitimate for data on a user visiting a website to circulate within the context of the said website. It is only when data flow out of this *first-party* context that permission should be needed:

> “Online publishers share a direct and trusted relationship with visitors to their websites. In the context of this relationship, OPA members sometimes collect and use information to target and deliver the online advertising that subsidizes production of quality digital content. […] The targeting of a behavioral advertisement by a first-party site is analogous to a sales clerk at a men's clothing store who recognizes a repeat customer and makes wardrobe suggestions based on the customer's past preferences for size, color and designers. The same dynamic is involved when Amazon.com suggests books that a consumer might be interested in reading based on titles that the consumer previously purchased. Given the direct relationship between the consumer and the merchant, the consumer naturally understands that the merchant is in a

58 Emphasis is my own, here and the next few quotes.

59 Her theories are described in section 2.3.5. of the original dissertation. The way in which her theory is referred to by W3C PING and TPWG participants is detailed in section 5.6.2.

> position to recognize and remember its customers' preferences and is not surprised when the merchant uses that information to suggest future purchases. Accordingly, OPA strongly supports an exemption for the collection of data from a consumer with whom the company interacts directly for the purposes of marketing to that consumer and for the general operation and personalization of the site." (public-tracking, e-mail by Chris Pedigo, 30 November 2011)

Kevin Smith, from Adobe, expressed similar views:

> "It does not matter what party the widget is. Under DNXT it cannot cross track. I don't think there would be a ton of concern if google or the weather widget in the examples discussed only tracked you in the context of the site on which they are embedded. For instance, google could remember your zoom level or the coordinates to which you panned, and the weather site may default to the zip code you entered." (public-tracking, e-mail by Kevin Smith, 9 December 2011)

Their argument was ultimately successful. Advocates of more stringent rules relented because opposing proposals to exclude *first-parties* from the scope of DNT would have undermined efforts towards the effective implementation of any Do Not Track standard at all even further. According to the Tracking Compliance and Scope document:

> "With respect to a given user action, a first party to that action which receives a DNT:1 signal MAY collect, retain and use data received from those network interactions."

More surprisingly, privacy advocates like Vincent Toubiana from the French data protection authority, or Joseph Hall, from the Center for Democracy and Technology, also made references to contextual integrity being part of what defines privacy. Because Helen Nissenbaum is critical of the liberal privacy paradigm, and especially of its emphasis on individual control and consent, this could be interpreted as contradictory with observations made before on privacy being defined by PING participants as a form of individual user control. Yet interviewed participants did not portray individual "user control" and "contextual integrity" as opposites, but rather as complementary. Within their frame of reference, user controls are provided by design elements that provide agency to enforce contextual boundaries defined by the user, inside which data related to him or her may flow.

As a conclusion, discourses on "privacy", especially – but not only – those produced by privacy advocates who championed a strict Do Not Track standard, indeed portray "privacy" as a matter of individual control and are either inspired or in line with the liberal privacy paradigm. The presence of computer scientists and engineers, rather than the kind of lawyers and public officials present in the GDPR negotiations or in the OECD and Council of Europe experts groups, did not affect the definition and conception of privacy around which the discussions were structured.

Chapter IV: Defining “personal data”

Why the definition matters

According to article 2 of the GDPR, data protection rules apply “to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.” This makes determining whether a case involves “personal data” the first step in deciding whether such rules apply. As data protection law contains the concrete set of rules that are to ensure the rights to privacy and to the protection of personal data (Clément-Fontaine 2017), understanding the scope of “personal data”, its genealogy and its evolution can contribute to the understanding of what “privacy” is if defined as the object of the right to privacy.

As we shall see, it was decided very early on that “personal data” would mean *any* data, regardless of the sensitivity of its contents with regards to “privacy”, and, in the overwhelming majority of cases, relating to an *individual*, and not a group. This can be interpreted as being in line with the liberal privacy paradigm.

The invention of the legal concept of “personal data” in the early 1970’s

“Personal data” was an expression first used by statisticians who processed data related to persons. According to Spiros Simitis, the pre-existence of this term explains the choice of the term “personal data” (*Datenschutz* in German):

> “[…] when the discussions on automation from, when automation started, they used in those discussions the words "personal data". And the personal data was used because the personal data was seen as an object permitting so to say to develop certain policies, to base certain policies, to explain for whom those policies would be relevant. And because at the time it was already spoken of personal data, in Germany, the word *Datenschutz* was created.” (Interview with Spiros Simitis)

The first data protection act, in Hesse, did not define “personal data”.

Early drafts proposed definitions limiting the scope of “personal data” to data that is related to the privacy, or intimacy, or private life of persons (sometimes both legal and natural persons). For example, the definition in the German federal draft law of 1972[60] was the following:

60 See: Section 2, Referentenentwurf Bundes-Datenschutzgesetz 1972, Council of Europe, EXP/Prot.Priv./EDB (73) 2

> “By “personal data” are meant particulars concerning the personal or material condition of an identified or identifiable natural or juristic person in private law or of an identified or identifiable association of persons (hereinafter termed “the person concerned”). Public undertakings, services or administrative bodies exercising similar functions, which are or belong to public-law corporations, shall be considered equivalent to the persons referred to in sentence 1.”

Further, in section 3 of the same bill, it was stated that:

> “Nothing in this Act shall be construed as protecting personal data which can be directly obtained from generally accessible sources.”

In 1972, Jean-Paul Costa, a French delegate to the experts group on the protection of privacy vis-à-vis electronic databanks of the Council of Europe, proposed that data protection principles should apply to:

> “data […] as relates to the private life or privacy of individuals whom it concerns, and particularly information concerning their race, religion, political opinions, morals, health or past judicial record.” (Council of Europe, EXP/Prot.Priv./EDB (72) 17, p. 14)

Yet the first national data protection law, which is also the first law to ever specify a legal definition of “personal data”, did not restrict its material scope to information related to “privacy” or “intimacy”, but simply and boldly stated that it is: “information relating to a unique individual[61].” Why?

According to Peter Hustinx:

> “ […] in 1950, privacy was: home, mail, correspondence, family life. These concepts […] seemed rather obvious. But they became less evident as we were looking at what privacy is. And especially privacy outside of the home. So the uncertainty on the concept of private when data flow. What does really fall under the notion of privacy[62]?”

Another difficulty was that the power of computers to combine data meant that apparently “harmless” data could one day become very sensitive:

> “Especially with automated data, you may not know at the time that the data is collected that it is or will at some stage in the future become sensitive” (Interview with Michael Kirby, former chair of the OECD experts group that wrote the OECD Guidelines)

This idea was already present in the explanatory report on the preliminary draft resolution relating to the protection of privacy vis-à-vis electronic data banks in the private sector of the Council of Europe, in September 1972:

61 In Swedish: “upplysning som avser enskild person”. Datalag 1973:289.

62 Translated from Dutch: « […] in 1950 was privéleven: huis, brieven, briefwisseling, familieleven. Die begrippen […] hadden een zekere evidentie. Maar naarmate je kijkt naar wat privéleven is, was het onduidelijk. En vooral wat privé buiten het huis plaatsvindt. Dus de onduidelijkheid van het begrip privé als gegevens gaan stromen. Wat valt nou wel en niet onder privéleven? »

> "[…] certain data which are inoffensive when considered separately may be correlated in such a fashion that their availability may become a threat to privacy." (Council of Europe, EXP/Prot.Priv./EDB (72) 14, p. 5)

This difficulty in determining once and for all, *erga omnes*, for everyone, what informational contents would be "private" and which one would be excluded from "data protection" led to the adoption of a broad definition that was agnostic to the content. Any data, whatever its content, would be "personal" if there was link between the said data and a "person".

Legal terminology distinguishes between "natural persons" (living human beings) and "legal persons" (corporations, public entities, associations …). Today, jurisdictions that include data relating to legal persons in their definition of "personal data" have become marginal exceptions[63]. However, back in the early 1970's, this was still an undecided matter.

In 1971, the British Computer Society wrote that:

> "The British Computer Society Privacy Committee submits that legislation should be introduced to define the rights of the person, whether an individual, group or institution, with respect to the privacy of information relating to him, when held by others or handled by them." (British Computer Society, 1971, p. 1)

Including legal persons in the definition was thus conceived as a way to protect "group privacy". Yet in 1973 and 1974, the Council of Europe recommendations excluded legal person data from the scope of data protection, and so did the majority of legal instruments adopted since this early period, despite the fact that Convention 108 gave ratifying states the option. This is how two actors involved in early decision-making on data protection explained the exclusion of legal person data:

> " […] the protection of the personality is purely a constitutional right applicable to the individual persons […]" (Interview with Spiros Simitis)

> "[…] in undertaking its investigation of privacy, the [Australia Law Reform Commission] had pointed out that claims to 'privacy' by legal persons (corporations) raised issues that were distinct and separate from the human rights issues normally addressed in relation to individual claims to privacy." (Kirby 2017, 15)

So since the 1970's, most legal definitions of "personal data" have only covered data where there was a link with an individual natural person who is thereby granted certain control rights over this data. This happens to be in line with the liberal privacy paradigm's definition of "privacy" as individual control.

But what constitutes such a link? How strong should the link be? Where does one draw a line between "personal" and "anonymous" data?

63 It was the case in Liechtenstein until 2018. Now, in Europe, only Switzerland maintains a definition of personal data that includes both natural and legal persons (art. 3. of the Loi fédérale sur la protection des données of 12 June 1992, version of March 1st, 2019).

From a very early stage, it appeared obvious that computers would have the capacity to re-identify seemingly anonymous data with much greater ease than could be done by hand. According to the British Computer Society's 1972 report:

> "The individual identity may be submerged in apparently anonymous statistics, but if it can be extracted then it must be considered to be there." (British Computer Society, 1972, p. 12)

The Swedish definition of 1973 simply stated, as we have seen, that personal data is any data related to a single person. The French definition adopted in 1978 stated that "nominative data" (*donnée nominative*) was any data "directly or indirectly" related to a person. In 1980 and 1981, the OECD Guidelines and Convention 108 referred to an "identified or identifiable" person. The definition of personal data contained in the 1995 Data Protection Directive combined both elements: "identified or identifiable", "directly or indirectly". Therefore, data did not need to contain a precise identifier like a full name to be deemed "personal". Hints that can be used to re-identify an individual to which the information in the data applies is sufficient.

The case law of the European Court of Justice

Several cases brought before the European Court of Justice (ECJ) have involved a discussion on the definition of "personal data".

Quoting a verdict by the European Court of Human Rights[64], the ECJ reaffirmed the fact that the legal definition of "personal data" in Directive 95/46/EC refers to "*any*" data, regardless of its content, as long as it is directly or indirectly linked to an identified or identifiable individual[65]. In 2015, it insisted on the fact that "personal data" should not be confused with "data relating to private life"[66]. In 2017, the Court ruled that:

> "The use of the expression 'any information' in the definition of the concept of 'personal data', within Article 2(a) of Directive 95/46, reflects the aim of the EU legislature to assign a wide scope to that concept, which is not restricted to information that is sensitive or private, but potentially encompasses all kinds of information, not only objective but also subjective, in the form of opinions and assessments, provided that it 'relates' to the data subject." (ECJ 20 December 2017 Peter Nowak v. DPC C-434/16 §34)

There was more debate on what makes data "relate" to an individual. How strong should the link be? According to a relative definition of personal data, one should look at the ability of a given data controller to determine whether data is personal or not *from the perspective of that data controller*, whereas in an absolute definition, only data that can *never* be identified *by anyone* under any circumstance is not personal.

64 ECtHR 16 February 2000 Amman v. Switzerland

65 See: ECJ 6 November 2003 Lindqvist C-101/01 §24 and ECJ 9 November 2010 Volker and Heifert v. Hesse C-92/09 and C-93/09 §52.

66 ECJ 16 July 2015 ClientEarth and PAN v. EFSA C-615/13 P §32.

Case law on this matter is not entirely clear (Zuiderveen Borgesius 2017).

In 2011, the ECJ ruled that IP addresses are personal data, the fact that they are only indirectly identifying being irrelevant[67], but because the case was about an Internet Service Provider, a type of company that controls information able to link such an address with one of its subscribers, the ruling did not give much indication on whether "personal data" should be understood as absolute or relative. Five years later, it indicated that "a dynamic IP address registered by an online media services provider when a person accesses a website that the provider makes accessible to the public constitutes personal data within the meaning of that provision, in relation to that provider, *where the latter has the legal means which enable it to identify the data subject with additional data which the internet service provider has about that person*[68]." (ECJ 19 October 2016 Patrick Breyer v. Germany C-582/14 §49). This would mean that the potential capacity of an unauthorised intruder gaining access to the data to *illegally* correlate a dynamic IP address with subscriber data held by an Internet service provider is irrelevant. Finally, in 2017, the Court maintained that "for information to be treated as 'personal data' within the meaning of Article 2(a) of Directive 95/46, there is no requirement that all the information enabling the identification of the data subject must be in the hands of one person" (ECJ 20 December 2017 Peter Nowak v. DPC C-434/16 §31). But it did not state the criteria that would make it clear that data is not personal. As a consequence, there is still a limited margin of uncertainty in the ECJ's case law regarding what constitutes a link between an individual and data related to that individual.

Debates during the discussions on the GDPR

Although the "risk-based approach" could have been used by the industrial coalition to question the broad definition of "personal data" that includes "any" data, and not only data related to "privacy", I found very few attempts to do that in the positions papers I have read[69]. There were, however, many attempts by that coalition to lower obligations if the link with the data subject was weakened, whereas the privacy advocates lobbied to explicitly anchor an absolute definition of "personal data" into the text of the GDPR. At stake was mainly whether the GDPR would fully apply to online behavioural marketing.

The Commission's initial proposal did not change the fundamental elements of the definition of "personal data", but changed the order in which the concepts of "personal data" and "data subject" were presented by tying the former to the latter:

67 ECJ 24 November 2011 Scarlet v. SABAM C-70/10.

68 Emphasis is my own.

69 One exception would be, for example, a document by the British Digital Marketing Association, that stated that "the definition of personal data in the Directive is possibly too broad in that it sometimes inadvertently captures marginal cases. […] It might be a good idea to introduce a risk of harm criteria to the definition." (2009 EU Commission consultation, document DMA1, 2009, p. 3) (see 634 for full reference)

Definition in the 1995 Data Protection Directive (art. 2)	**Definition in the Commission's initial proposal for a General Data Protection Regulation (COM 2012-011)**
(a) 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;	**(1) 'data subject' means** an identified natural person or **a natural person who can be identified,** directly or indirectly**,** ***by means reasonably likely to be used by the controller or by any other natural or legal person*****,** in particular by reference to an identification number**, location data, online identifier** or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person; **(2)** 'personal data' means any information relating to a data subject;

This inversion raised a lot of opposition[70]. So did the words "by means *reasonably* likely to be used by the controller *or by any other person*", which were removed from the article containing the definitions, but kept in recital 26, showing that the legislator endorsed an absolute concept of "personal data"… while leaving some flexibility for interpretation by leaving in the word "reasonably".

Several interest groups from the industrial coalition lobbied for the inclusion of a definition of a concept of "pseudonymous data" in the GDPR. Such an amendment was presented as the application of a "risk-based approach", as data without any direct identifiers were presented as less-risky than directly identifying data:

> "One possibility to deal with these aspects could be to introduce a harmonised definition of indirect or pseudonymous personal data that could benefit from lighter data protection requirements as the processing of such type of data usually present very low risks to privacy." (Industry Coalition for Data Protection, Lobbyplag collection, document ICDP1, 2011, p. 5)

Yahoo, for example, dedicated a position paper to the issue[71] in which it argued that many information society service providers did not need to know the identity of a data subject to offer their services. The industrial coalition was successful in including a concept of "pseudonymisation" in article 4 of the GDPR, but the coalition of privacy advocates managed to get it to be phrased in a way that ensured that pseudonymous data would explicitly stay contained within the scope of "personal data":

70 See sections 6.4.1. and 6.4.4. of the original dissertation for examples.
71 Document YAHOO1 in the Lobbyplag collection.

> "'pseudonymisation' **means the processing of personal data** in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;" (art. 4 (5) GDPR)

Thus, pseudonymisation in the GDPR is now a useful – and sometimes necessary – extra safeguard, but not something that can be used to be exempted from certain data protection principles or data subject rights. Its inclusion did not move data protection law in the EU away from an absolute definition of "personal data".

Finally, some privacy advocates and NGO's proposed amendments to add the words "single out" or "singling out" to the definition of "personal data"[72].

For example, here is a proposed amendment by Dutch NGO Bits of Freedom:

Original proposal by the EU Commission	**Proposed amendment by Bits of Freedom**
'Data subject' means an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably to be likely to be used by the controller or any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person[73]	'Data subject' means an identified natural person or a natural person who can be identified **or singled out**, directly or indirectly, by means reasonably to be likely to be used by the controller or any other natural or legal person, in particular by reference to an identification number **or a unique identifier**, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person

Reference: Amendment 24, page 12 of document BITSOFFREEDOM1 (Lobbyplag collection[74])

According to Joe McNamee, executive director of EDRi at the time of the GDPR negotiations:

> "I think it was successful as a concept. Why is it important? If you look at the Facebook scandal around the […] elections: there is no value in knowing that Mr. Smith here is from 5 River Street, Minnesota, is called Mr. Smith from 5 River Street. But the matter is the ability to identify him as somebody susceptible to receiving this message, and being manipulable on the basis of not who he is, but what he is. […] Imagine if you could be singled out and manipulated

72 See more on this topic in section 6.4.2. of the original dissertation.

73 Traduction officielle en français : « «personne concernée»: une personne physique identifiée ou une personne physique qui peut être identifiée, directement ou indirectement, par des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par toute autre personne physique ou morale, notamment par référence à un numéro d'identification, à des données de localisation, à un identifiant en ligne ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ; »

74 See page 637 for the precise reference.

without your consent or knowledge, and if this wasn't even a concept that data protection law would cover. How ridiculous would that be?" (Interview with Joe McNamee)

"Singling out" never made it to the final version of the definition[75]. It has, however, been included in recital 26, which states that "[…] to determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly."

To conclude on the discussions on the definition of "personal data" during the writing process of the GDPR, it appears that the new definition, compared to that of Directive 95/46, includes new elements in favour of an absolute interpretation of the notion. While a concept of "pseudonymisation" was included, pseudonymous data was explicitly included in the scope of "personal data" and there was no serious attempt to restrict the application of data protection principles to data that relates to the "private life", "privacy" or "intimacy" of the data subject. There was no attempt either to include legal persons in the definition, nor to change the fact that the definition of "personal data" is based off an individualistic approach.

The hidden influence of the law in techno-policy standards-setting processes

In order to function, the Internet – just like other socio-technical assemblages – relies on decisions on how nodes (computers) in the network should communicate with another in order to be understood. Such decisions are then laid out in documents called standards. Historically, fora where such documents are discussed and written have built themselves in opposition to the state-centered model (Musiani and Schafer 2011; Russell 2006). David Clark, a computer engineer who has been involved in the development of Internet protocols ever since the late 1970's, is famous for having uttered that such institutions and their members "reject kings, president and voting" in favour of "running code and rough consensus" during the 1992 annual IETF conference (Clark 1992). This maxim is still endorsed by the IETF, which includes it in its "Tao", a document meant to explain the role of the organisation to newcomers (ten Oever and Moriarty 2018).

There is often a sense that the "legal" is disconnected from the "technical reality". This view has been expressed on a regular basis by people who took part in the exploratory phase of this doctoral research[76]. Many policy papers written in the frame of the GDPR process included references to such a "technical reality" that decision-makers should pay (better) attention to[77].

75 The final version of the definition states that personal data "means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;"

76 See section 6.6. of the original dissertation.

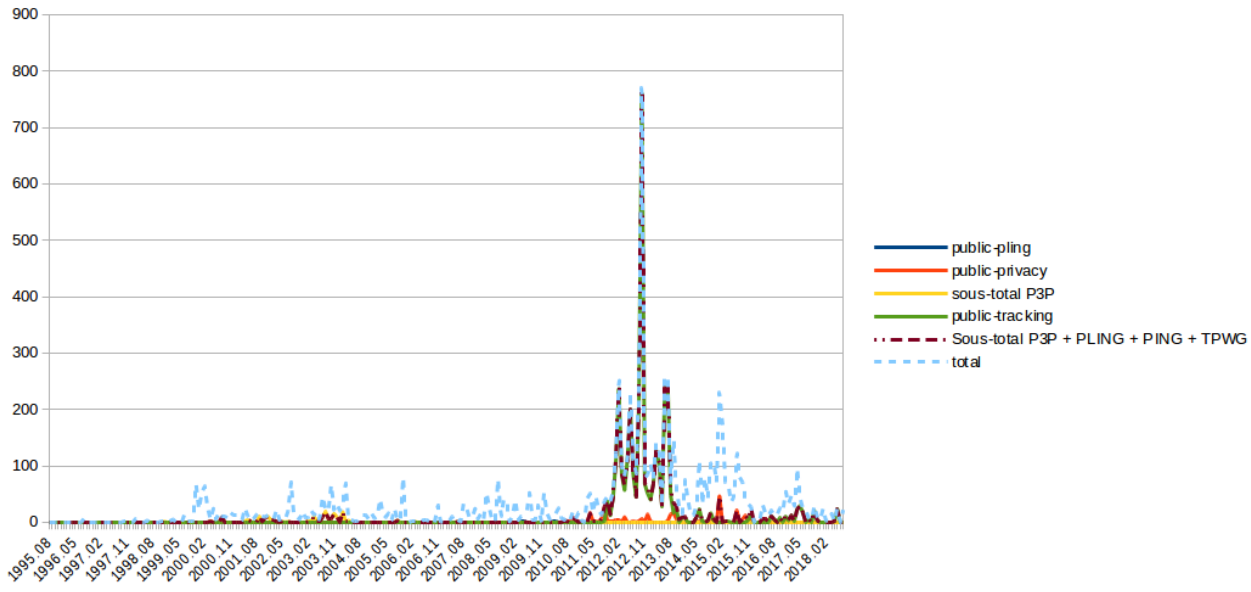
77 Examples include documents DIGITALEUROPE2 and FPF1 of the Lobbyplag collection (see full reference on p. 635 to 640 of the original dissertation).

The development of Internet standards often intersects with domains of public policy, such as privacy. This may even create a sense of competition between state and non-state policy instruments, such as technical standards on the one hand, and the law on the other. At the very least, if standard authors reject “kings, president and voting”, one may assume that they make endeavours at keeping state interference, including the law, at bay.

Standards are global, or at least, they are meant to be. Laws, on the other hand, are not. This is one reason why some participants, when asked, felt that laws were not that relevant to their work at the Privacy Interest Group (PING) and the Tracking Protection Working Group (TPWG) at the W3C. According to one of them: “Regulations differ so much between jurisdictions […]. The goals of W3C are to develop these things that are going to be complemented and used worldwide”.

In practice, however, this does not seem to exactly hold true. State actors have been instrumental in their support of groups dealing with what Deirdre Mulligan and Nick Doty (2013) call “techno-policy standards”. Even though they ultimately failed to produce widely-implemented standards, the Platform for Privacy Preferences (P3P) Working Group and the TPWG oweds their existences in large part to the existence of state actors, and especially to the Federal Trade Commission (FTC) and the European Commission, who pressured actors from the industry into sitting at the same table as privacy advocates. For example, in 2011, David Vladeck of the FTC published a press release in which he threatened to push for legislation unless a multi-stakeholder group managed to agree on a standard to allow individual to turn online tracking off (Vladeck 2011). That regulatory pressure has been an influential factor was clearly identified by some of the interviewed participants.

The discussions that took place around Do Not Track also led to a sharp increase in the number of occurrences of the word “law”, shown here on a graph plotting the evolution of absolute monthly occurrences of the term:



Indeed, despite impressions to the contrary held by some participants, legal arguments *were* made, on a regular basis, by participants trying to defend their views in the debates on the Do Not Track documents. Here is an example of such an exchange, which took place as part of the debate on the definition of "tracking":

> "If you agree on not including first party tracking, you decide to not address in which way soever the requirements of Art. 5 III of the E-Privacy Directive concerning first parties. Lost opportunity." (*public-tracking*, e-mail by Ninja Marnau, 30 November 2011)
>
> "The ePrivacy Directive does not require consent for "legitimate" cookie use to deliver a service and most DPAs I've spoken to have felt this covers 1st party cookie use and that only "3rd party advertising cookies" are the true target of the ePrivacy Directive." (*public-tracking*, e-mail by Shane Wiley, 30 November 2011)

Regardless of the truth value of either statement, we may note that both participants, while in disagreement on the subject matter, agreed on the legitimacy of legal arguments to make their points.

Of course, not *all* laws were mentioned. Legal arguments were predominantly made with references to either U.S. or European law. Furthermore, participants did not rely on legal arguments only. For example, the topic of "trust" was often raised by privacy advocates, just like it has been in various state-centered policy settings since the 1970's[78]. However, the exchange of legal arguments among W3C participants discussing public policy matters shows that the law has become an accepted influence even in settings that were historically wary of state actors and instruments, at least when discussing privacy.

Discussions on what constitutes "anonymous" as opposed to "personal" data drew elements from legal expertise. Rob van Eijk, for an example, made a reference to a study published by Paul Ohm (2010) in the *UCLA Law Review* called "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization" in an e-mail sent on the 5th of September, 2014 on the *public-tracking* mailing list. The *Specification Privacy Assessment* document proposed by Frank Dawson of the PING also contains similar references to legal doctrine.

Over time, European law has become increasingly influential, and this was reflected in documents produced by participants. The first Tracking Protection Expression (TPE) working draft, publihed on the 14th of November, 2011, contained neither "personal data" nor "controller", but it did talk about "personal information". The next version, published on the 13th of March, 2012, introduced the words "data controller", used in European data protection law. "Personal data" replaced "personal information" from the version published on the 2nd of October 2012 onwards. The *Privacy*

78 These arguments are all discussed in further details in section 5.6. of the original dissertation.

Considerations for Web Protocols written by the PING defines “personal data” in the same way as IETF’s RFC 6973, which phrasing is itself a shortened version of the definition found in EU law:

Definition found in Directive 95/46/CE en anglais	“'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;” (art. 2 (a))
RFC 6973	« Personal data: Any information relating to an individual who can be identified, directly or indirectly » (RFC 6973, p. 7)
Privacy Considerations for Web Protocols Unofficial Draft 29 April 2019	« Personal Data: Any information relating to an individual who can be identified, directly or indirectly. » (W3C Privacy Considerations)

RFC 6973 further states that data is only “anonymous” when “an observer *or attacker*[79] cannot identify the individual within a set of other individuals” from that data. This suggests an absolute interpretation of the notion of “personal data” similar to that towards which EU law and case law are leaning. More importantly with regards to the philosophical foundations of privacy and data protection norms, this definition refers to *any* data (whether it is deemed “private” or not) relating to an *individual*.

While it remains true that standards are not hard law documents, and that standards-setting organisations such as the W3C and the IETF operate distinctly from regulatory authorities, they are definitely not impervious to legal influence. This case study on privacy-focused techno-policy Web standards (P3P and Do Not Track) and internal privacy review and consultancy (PING) shows that there is a influence of both the law and legal expertise on the discussions and on the documents that are produced. EU law, in particular, has been a source of inspiration for core definitions such as that of “personal data”.

79 Emphasis added.

Conclusion

The first major conclusion of this work is that no evidence could be found of a divide between legal and computer scientist approaches towards privacy and data protection. There were no significant differences in discussion layouts between legal-oriented and engineering-oriented settings. In both cases, the liberal approach towards privacy prevailed, with an emphasis on individual control rights translated into an individualistic and content-agnostic definition of "personal data". Even "worse", from the point of view of the first hypothesis of this work, is the fact that the fundamental principles of data protection law are a translation into legal wording of proposals that appear to have initially been made by computer scientists in the early 1970's. This suggests that privacy and data protection are not (only) technical issues, but are fundamentally political. Or, in other words, that which is technical is also, at the same time, political. Debates are not so much on *how* to best protect privacy, but rather on *what* it means, *if* it has value and *why*.

As suggested by the second hypothesis, it is the rise of concerns towards a right to privacy seen through the lens of liberal-utilitarian political philosophy and its collision with a distressing social image of computers popularised by science fiction that led to the use of personal data becoming a public problem and, later, in the early 1970's, to the invention of "data protection" as a new right in Europe.

The third and the fourth hypotheses are harder to conclude on, because there is more than one way to answer.

On the one hand, if one defines privacy as an individual control right, then indeed the right to the protection of personal data is a part of the right to privacy, and there is a shared normative narrative supporting both categories of rights. On the other hand, however, one may adopt the view that privacy law should protect the barrier protecting the "private", the "intimate", from the prying eyes of the "public". In that case, data protection law cannot be accounted for on grounds of "privacy", as its remit covers much more than just information that is socially constructed as "personal" or "private" in a given society.

This difficulty in giving a definite answer to the test of the final two hypotheses underlines that the differences between normative conceptions on "privacy" are not merely different ways of saying the same thing. I would therefore argue that the politicisation of computers through the lens of a liberal-utilitarian conception of privacy triggered a series of events that led to a transition from a Privacy of Ancients to a Privacy of Moderns, at least in the realm of the law. In this, I draw a parallel with evolutions described by Benjamin Constant (Constant 1988 [1819]) in his essay on *The Liberty of Ancients Compared with that of Moderns* (see: Rossi 2020).

As pointed out by the feminist criticism of privacy (Decew 2015), for a long time, the right to privacy was not so much a positive right for the individual as much as a negative right preventing the state from

interfering into “private” and/or “domestic” affairs[80]. From a normative perspective, Louis Brandeis and Samuel Warren, credited with the invention of the coherent approach of the right to privacy, believed in the existence of a collective interest in defending the public sphere from the intrusion of lowly private or intimate topics:

> “Even gossip apparently harmless, when widely and persistently circulated, is potent for evil. It both belittles and perverts. It belittles by inverting the relative importance of things, thus dwarfing the thoughts and aspirations of a people. When personal gossip attains the dignity of print, and crowds the space available for matters of real interest to the community, is there any wonder that the ignorant and thoughtless mistake its relative importance?” (Warren and Brandeis 1890)

This is quite foreign to the notions of “informational self-determination” or of “user control” which I encountered on the field. In data protection law, all data is personal as long as it can be traced, even indirectly, to an individual. But this individual is in principle free to share it, as long as conditions for free and informed consent are met, even if the information contained in the data is deemed as “private” or “intimate” by socially constructed cultural norms. Norms such as Convention 108, the GDPR, or the Do Not Track specification documents, do not focus on protecting families and homes from the public eye of either the state or private persons, but on giving *individuals* rights and agency with regards to the processing of data about them.

Even if not *all* social, or even legal norms imposing modesty and protecting the public from the private have disappeared, this, to me, suggests there has been a significant shift over time. The conception of privacy as a collective right for small domestic entities lost ground in favour of of privacy as an individual control right meant to increase autonomy and self-determination.

This may help explain part of what the literature calls the privacy paradox. Indeed, this paradox is predicated on a definition of privacy wherein certain contents, e.g. pictures of raucous parties or displays of nudity, are “private” and should not appear in a public space. Only then is it contradictory for someone to state that privacy is important while he or she shares such content online. Indeed, it is perfectly possible and coherent to state something along the lines of: “I want to be able to post content about myself online *only for purposes that I choose and while keeping a right to control* this content, restrict access to it and maybe even delete the content later on”.

Concluding that there has been such an evolution *in law* is not, however, the same thing as stating that there has been an evolution in social representations and practices with regards to privacy in general and informational privacy in particular. Some elements may hint towards that. For instance, if we take the example of the telephone, then the replacement of landlines where there was at best, in the late 1900’s, one line per home, to a situation where most people are equipped with an individual password-locked individual mobile phone, is a clear evolution from a collective private communicational space

80 In France, this even prevented victims of domestic violence from having their complaints heard by a court. It was not until 1992 that the Cour de Cassation, France’s judicial Supreme Court, told French judges that the right to privacy could not be invoked to prevent a court from accepting to hear a criminal case. See: Cour de cassation, Ch. Crim., 11 June 1992.

(the home, with one line, and one conversation everyone can tap into if there are several phones on the one line) to an individual one. However, at this stage, the idea that society (or at least some societies) as a whole, and not only the law, have embraced a Privacy of Moderns, is no more than a hypothesis which deserves further investigations. Indeed, the study presented in the doctoral dissertation this is a summary of merely looked into the *production* of normative texts that are policy instruments meant to protect “privacy” through that of “personal data”. It does not study the *reception* of these texts, nor how their encounter with local symbolic orders and systems of belief lead to various interpretations and, in turn, material practices.

References

Acquisti, Alessandro, and Ralph Gross. 2006. ‘Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook’. *Proceedings of the 6th International Conference on Privacy Enhancing Technologies*: 36–58.

Acquisti, Alessandro, Michèle Francine MBo’o Ida, and Fabrice Rochelandet. 2011. ‘Les comportements de vie privée face au commerce électronique, Privacy in Electronic Commerce and the Economics of Immediate Gratification’. *Réseaux* (167): 105–30.

Albrecht, Jan-Philipp. 2013 Report on the proposal for a Regulation of the European Parliament and the Council on the Protection of Individuals with Regards to the Processing of Personal Data and on the Free Movement of such Data. Committee on Civil Liberties, Justice and Home Affairs. European Parliament. 21st of November, 2013. Document A7-0402/2013. Available online at: https://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2013-0402+0+DOC+PDF+V0//EN (page accessed on the 20th of August, 2020)

Altman, Irwin. 1977. ‘Privacy Regulation: Culturally Universal or Culturally Specific?’ *Journal of Social Issues* 33(3): 66–84.

Alvestrand, Harald T., and Håkon Wium Lie. 2009. ‘Development of Core Internet Standards: The Work of IETF and W3C’. In *Internet Governance: Infrastructure and Institutions*, Oxford: Oxford University Press, 126–46.

Ariès, Philippe, and Georges Duby. 1988. *Histoire de la vie privée*. Paris: Seuil.

Atten, Michel. 2013. ‘Ce que les bases de données font à la vie privée, What databases do to private life’. *Réseaux* (178–179): 21–53.

Aufrère, Laura, and Lionel Maurel. 2018. ‘Données Personnelles : « Un Enjeu de Dignité Collective, Face Aux Manipulations Des Gafam »’. *Le Monde*. https://www.lemonde.fr/idees/article/2018/05/25/les-donnees-personnelles-un-enjeu-collectif_5304520_3232.html.

Austin, John. 1962. *How to Do Things with Words by J. L. Austin*. Oxford: Oxford University Press.

Bachimont, Bruno. 2010. *Le Sens de La Technique: Le Numérique et Le Calcul*. Paris: Belles lettres.

Bellanger, Pierre. 2014. *La Souveraineté Numérique*. Paris: Stock.

Belli, Luca. 2016. *De la gouvernance à la régulation de l’Internet*. Boulogne-Billancourt: Berger-Levrault.

Bellon, Anne. 2019. ‘Numérisation Des Politiques Culturelles En France’. In *Numérisation de La Société et Enjeux Sociopolitiques. Tome 1. Numérique, Communication et Culture*, Systèmes d’information, Web et société, ed. Éric George. Londres: ISTE, 169–76.

Bennett, Colin J. 1992. *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*. Ithaca, N.Y.: Cornell University Press.

Bennett, Colin J. 2008. *The Privacy Advocates: Resisting the Spread of Surveillance*. Cambridge, MA: MIT Press.

Bennett, Colin J., and Charles D. Raab. 2003. *The Governance of Privacy. Policy Instruments in Global Perspective*. Aldershot: Ashgate.

Bergeron, Henri, Yves Surel, and Jérôme Valluy. 1998. ‘L’Advocacy Coalition Framework. Une contribution au renouvellement des études de politiques publiques ?’ *Politix* 11(41): 195–223.

Berinato, Scott, and Helen Nissenbaum. 2018. ‘Why Data Privacy Based on Consent Is Impossible’. *Harvard Business Reviw*. https://hbr.org/2018/09/stop-thinking-about-consent-it-isnt-possible-and-it-isnt-right.

Bing, Jon. 2009. ‘Building Cyberspace: A Brief History of Internet’. In *Internet Governance: Infrastructure and Institutions*, eds. Lee A. Bygrave and Jon Bing. Oxford ; New York: Oxford University Press, 8–47.

Blekeli, R.D. 1974. ‘Normes à Observer Pour Le Traitement de l’information et Les Procédures de Contrôle’. In *Questions d’ordre Politique Soulevées Par La Protection Des Données et Des Libertés Individuelles, Principes et Perspectives. Compte-Rendu Du Séminaire*, Collection études d’informatique, Paris: Organisation de Coopération et de Développement Economique (OCDE), 75–95.

Böhme, Rainer, and Stefan Köpsell. 2010. ‘Trained to Accept? A Field Experiment on Consent Dialogs’. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI ’10, Atlanta, Georgia, USA: Association for Computing Machinery, 2403–2406. https://doi.org/10.1145/1753326.1753689 (May 14, 2020).

Bowen, Glenn A. 2009. ‘Document Analysis as a Qualitative Research Method’. *Qualitative Research Journal* 9(2): 27–40.

BVA, 2018, *Les Français et les données personnelles*. Observatoire de la vie quotidienne des Français. May 24th. Available online: https://staticswww.bva-group.com/wp-content/uploads/2018/05/PRESSE-REGIONALE-Observatoire-de-la-vie-quotidienne-Mai-2018-Les-donn%C3%A9es-personnelles.pdf (page accessed on 25 August 2020)

British Computer Society. 1971. *Submission of Evidence to the Committee on Privacy*. London, England: British Computer Society.

———. 1972. *Privacy and the Computer--Steps to Practicality: A Review of Recent Work Carried out by the Privacy and Public Welfare Committee of the British Computer Society*. London: British Computer Society.

Casilli, Antonio A. 2013. ‘Contre l’hypothèse de la « fin de la vie privée »’. *Revue française des sciences de l’information et de la communication* (3). https://rfsic.revues.org/630 (July 18, 2017).

Casilli, Antonio A. 2015. ‘Digital Labor : Travail, technologies et conflictualités’. In *Qu’est-ce que le digital labor ?*, Bry-sur-Marne: INA, 8–40.

Clark, David D. 1992. ‘A Cloudy Cristal Ball -- Visions of the Future’. Presented at the IETF 24 Conference, Cambridge, Massuchussets. https://groups.csail.mit.edu/ana/People/DDC/future_ietf_92.pdf.

Clément-Fontaine, Mélanie. 2017. ‘L’union du droit à la protection des données à caractère personnel et du droit à la vie privée’. *LEGICOM* N° 59(2): 61–68.

Constant, Benjamin. 1988. ‘The Liberty of the Ancients Compared with That of the Moderns’. In *Political Writings*, Cambridge: Cambridge University Press, 307–28.

Couture, Stéphane, and Sophie Toupin. 2017. ‘What Does the Concept of “Sovereignty” Mean in Digital, Network and Technological Sovereignty?’ In Genève. https://papers.ssrn.com/abstract=3107272 (July 26, 2019).

DeCew, Judith. 2018. ‘Privacy’. In *The Stanford Encyclopedia of Philosophy*, ed. Edward N. Zalta. Metaphysics Research Lab, Stanford University. https://plato.stanford.edu/archives/spr2018/entries/privacy/.

Decew, Judith Wagner. 2015. ‘The Feminist Critique of Privacy: Past Arguments and New Social Understandings’. In *Social Dimensions of Privacy*, eds. Beate Roessler and Dorota Mokrosinska. Cambridge: Cambridge University Press, 85–103. http://ebooks.cambridge.org/ref/id/CBO9781107280557A018 (July 22, 2017).

DeNardis, Laura. 2014. *The Global War for Internet Governance*. New Haven London: Yale University Press.

Dijck, Jose van. 2014. ‘Datafication, Dataism and Dataveillance: Big Data between Scientific Paradigm and Ideology’. *Surveillance & Society* 12(2): 197–208.

Doty, Nick, and Deirdre K. Mulligan. 2013. ‘Internet Multistakeholder Processes and Techno-Policy Standards.’ *Journal on Telecommunications and High Technology Law* 11: 135–84.

Dubois, Vincent. 2010. ‘Les champs de l’action publique’. https://halshs.archives-ouvertes.fr/halshs-00498020/document (February 20, 2018).

Eberlein, Burkard, and Abraham Newman. 2006. ‘Innovating EU Governance Modes: The Rise of Incorporated Transgovernmental Networks’. In Chicago, Ill. http://councilforeuropeanstudies.org/files/Papers/EberleinNewman.pdf.

Ellul, Jacques. 1954. *La Technique Ou l’enjeu Du Siècle*. Paris: Armand Colin.

Estienne, Yannick. 2011. ‘Un monde de verre : Facebook ou les paradoxes de la vie privée (sur)exposée’. *Terminal. Technologie de l’information, culture & société* (108–109): 65–84.

Etzioni, Amitai. 1999. *The Limits of Privacy*. New York: Basic Books.

Favro, Karine. 2017. ‘La démarche de compliance ou la mise en œuvre d’une approche inversée’. *LEGICOM* N° 59(2): 21–28.

Flaherty, David H. 1989. *Protecting Privacy in Surveillance Societies*. Chapel Hill and London: The University of North Carolina Press.

Flichy, Patrice. 2001. *L’imaginaire d’Internet*. Paris: Découverte.

Fraser, Nancy. 2007. ‘Special Section: Transnational Public Sphere: Transnationalizing the Public Sphere: On the Legitimacy and Efficacy of Public Opinion in a Post-Westphalian World’. *Theory, Culture & Society* 24(4): 7–30.

Fuchs, Christian. 2011. ‘Towards an Alternative Concept of Privacy’. *Journal of Information, Communication and Ethics in Society*. /insight/content/doi/10.1108/14779961111191039/full/html (July 18, 2019).

Gerber, Nina, Paul Gerber, and Melanie Volkamer. 2018. ‘Explaining the Privacy Paradox: A Systematic Review of Literature Investigating Privacy Attitude and Behavior’. *Computers & Security* 77: 226–61.

Goldstein, Robert Justin. 2006. ‘Prelude to McCarthyism: The Making of a Blacklist’. *Prologue* 38(3). http://www.archives.gov/publications/prologue/2006/fall/agloso.html.

González Fuster, Gloria. 2014a. ‘Fighting For Your Right to What Exactly? The Convoluted Case Law of the EU Court of Justice on Privacy and/or Personal Data Protection’. *Birkbeck Law Review* 2(2): 263–78.

———. 2014b. *The Emergence of Personal Data Protection as a Fundamental Right of the EU*. Dordrecht: Springer. //www.springer.com/gp/book/9783319050225 (November 22, 2017).

Grant, Paul. 1983. ‘Technological Sovereignty: Forgotten Factor in the “Hi-Tech” Razzamatazz’. *Prometheus* 1(2): 239–70.

Greenwald, Glenn. 2013. ‘NSA Collecting Phone Records of Millions of Verizon Customers Daily’. *The Guardian*. https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order (June 1, 2019).

Gusfield, Joseph R. 1994. *The Culture of Public Problems: Drinking-Driving and the Symbolic Order*. 4. print. Chicago: Univ. of Chicago Press.

Habermas, Jürgen. 1987. *Théorie de l'agir communicationnel*. Paris: Fayard.

———. 1988. *L'espace public: archéologie de la publicité comme dimension constitutive de la société bourgeoise*. Paris: Payot.

Hall, Peter A. 1986. *Governing the Economy: The Politics of State Intervention in Britain and France*. New York: Oxford University Press.

———. 2015. 'Chapitre 10 / Cognitive Approaches: A French Touch?' In *Une French touch dans l'analyse des politiques publiques ?*, eds. Laurie Boussaguet, Sophie Jacquot, Pauline Ravinet, and Pierre Müller. Paris: Presses de Sciences Po, 237–62. https://www.cairn.info/une-french-touch-dans-l-analyse-des-politiques-pub--9782724616453-page-237.htm (June 23, 2020).

Hémont, Florian, and Marine Gout. à paraître. 'Consentement Résigné : En Finir Avec Le Privacy Paradox'. In *Le Profilage En Ligne : Entre Libéralisme et Régulation*, Paris: Mare et Martin.

Holvast, Jan. 2013. *De volkstelling van 1971: verslag van de eerste brede maatschappelijke discussie over aantasting van privacy*. Zutphen: Paris.

Hondius, Frits Willem. 1975. *Emerging data protection in Europe*. Amsterdam, Pays-Bas, Pays multiples: Elsevier.

Jobert, Bruno. 1994. *Le tournant néo-libéral en Europe: idées et recettes dans les pratiques gouvernementales*. Paris: Harmattan.

Jobert, Bruno, and Pierre Müller. 1987. *L'État en action*. Paris: Presses Universitaires de France - PUF.

Karaboga, Murat. 2018. 'The Emergence and Analysis of European Data Protection Regulation'. In *Managing Democracy in the Digital Age*, , 29–52.

Keynes, John Maynard. 1997. *The General Theory of Employment, Interest, and Money*. Amherst, NY: Prometheus Books.

Kirby, Michael. 2017. 'Privacy Today Something Old, Something New, Something Borrowed, Something Blue'. *Journal of Law, Information & Science* 25. http://www.jlisjournal.org/abstracts/kirby.25.2.html (January 25, 2019).

Koopman, Colin. 2013. *Genealogy as Critique: Foucault and the Problems of Modernity*. Bloomington: Indiana University Press.

Koops, Bert-Jaap et al. 2016. *A Typology of Privacy*. Rochester, NY: Social Science Research Network. SSRN Scholarly Paper. https://papers.ssrn.com/abstract=2754043 (May 10, 2017).

Kraus, Rebecca. 2013. 'Statistical Déjà Vu: The National Data Center Proposal of 1965 and Its Descendants'. *Journal of Privacy and Confidentiality* 5(1). https://journalprivacyconfidentiality.org/index.php/jpc/article/view/624 (November 9, 2018).

Krieg-Planque, Alice. 2009. *La Notion de Formule En Analyse Du Discours: Cadre Théorique et Méthodologique*. Besançon: Presses universitaires de Franche-Comté.

Kübler, Daniel. 2002. ‘Les acteurs associatifs dans l’advocacy coalition framework : application aux politiques publiques de lutte contre la drogue en suisse’. *Pyramides. Revue du Centre d’études et de recherches en administration publique* (6): 83–102.

Kubrick, S. (director), 1968, *2001: A Space Odyssey*, Metro-Goldwyn-Meyer, digital format.

Lanzing, Marjolein. 2016. ‘The Transparent Self’. *Ethics and Information Technology* (volume 18 issue 1): 9–16.

Lascoumes, Pierre. 2004. ‘La Gouvernementalité : de la critique de l’État aux technologies du pouvoir’. *Le Portique* (13–14). https://leportique.revues.org/625 (December 28, 2016).

Lascoumes, Pierre, and Patrick Le Galès. 2005. *Gouverner par les instruments*. Paris: Presses de Sciences Po. http://www.cairn.info/gouverner-par-les-instruments--9782724609492.htm (September 6, 2018).

Laugier, Sandra. 2004. ‘Performativité, normativité et droit’. *Archives de Philosophie* Tome 67(4): 607–27.

Lessig, Lawrence. 1999. *Code and Other Laws of Cyberspace*. New York: Basic Books.

Martin-Juchat, Fabienne, and Julien Pierre. 2011. ‘Facebook et les sites de socialisation : une surveillance consentie’. In *L’homme trace: perspectives anthropologiques des traces contemporaines*, ed. Béatrice Galinon-Mélénec. Paris: CNRS éditions, 105–23.

Mascetti, Sergio, Anna Monreale, Annarita Ricci, and Andrea Gerino. 2013. ‘Anonimity : A Comparison Between the Legal and Computer Science Perspectives’. In *European Data Protection: Coming of Age*, Dordrecht: Springer, 85–115.

Mawhinney, Hanne B. 1993. ‘An Advocacy Coalition Approach to Change in Canadian Education’. In *Policy Change and Learning: An Advocacy Coalition Approach*, Theoretical lenses on public policy, eds. Paul A. Sabatier and Hank C. Jenkins-Smith. Boulder, Colo: Westview Press, 59–82.

Meints, Martin. 2009. ‘The Relationship between Data Protection Legislation and Information Security Related Standards’. In *The Future of Identity in the Information Society*, eds. Vashek Matyáš, Simone Fischer-Hübner, Daniel Cvrček, and Petr Švenda. Berlin: Springer, 254–67.

Mill, John Stuart. 1989. *On Liberty ; with The Subjection of Women ; and Chapters on Socialism*. ed. Stefan Collini. Cambridge [England] ; New York: Cambridge University Press.

Miller, Arthur R. 1971. *The Assault on Privacy: Computers, Data Banks, and Dossiers*. Ann Arbor: University of Michigan Press.

Moore, Adam D. 2003. ‘Privacy: Its Meaning and Value’. *American Philosophical Quarterly* 40(3): 215–27.

Mueller, Milton. 2010. *Networks and States: The Global Politics of Internet Governance*. Cambridge, Mass: MIT Press.

Müller, Pierre. 1984. *Le Technocrate et le Paysan*. Paris: Ouvrière.

———. 2011. *Les politiques publiques*. Paris: Presses universitaires de France.

Mulligan, Deirdre K., Colin Koopman, and Nick Doty. 2016. ‘Privacy Is an Essentially Contested Concept: A Multi-Dimensional Analytic for Mapping Privacy’. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 374(2083): 20160118.

Mumford, Lewis. 1938. *The Culture of Cities*. New York: Harcourt, Brace and Company.

Musiani, Francesca. 2015. ‘Edward Snowden, l’« homme-controverse » de la vie privée sur les réseaux’. *Hermes, La Revue* n° 73(3): 209–15.

Musiani, Francesca, and Valérie Schafer. 2011. ‘Le modèle Internet en question (années 1970-2010)’. *Flux* n° 85-86(3): 62.

Newman, Abraham. 2008. *Protectors of Privacy. Regulating Personal Data in the Global Economy*. Ithaca: Cornell University Press.

Niblett, G.B.F. 1971. *Digital Information and the Privacy Problem*. Paris: OCDE.

Nissenbaum, Helen. 1998. ‘Protecting Privacy in an Information Age: The Problem of Privacy in Public’. *Law and Philosophy* 17(5/6): 559–96.

———. 2004. ‘Privacy as Contextual Integrity’. *Washington Law Review* 79(1): 119–58.

Nissenbaum, Helen Fay. 2010. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, Calif: Stanford Law Books.

Nitot, Tristan, and Nina Cercy. 2016. *Numérique : Reprendre Le Contrôle*. Framabook. https://framabook.org/docs/NRC/Numerique_ReprendreLeControle_CC-By_impress.pdf.

Norberg, Patricia A., Daniel R. Home, and David A. Home. 2007. ‘The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors’. *Journal of Consumer Affairs* (41): 100–126.

Nouwens, Midas et al. 2020. ‘Dark Patterns after the GDPR: Scraping Consent Pop-Ups and Demonstrating Their Influence’. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, CHI ’20, Honolulu, HI, USA: Association for Computing Machinery, 1–13. https://doi.org/10.1145/3313831.3376321 (May 15, 2020).

ten Oever, Niels, and Kathleen Moriarty. 2018. ‘The Tao of IETF A Novice’s Guide to the Internet Engineering Task Force’. https://ietf.org/about/participate/tao/.

Ohm, Paul. 2010. ‘Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization’. *UCLA Law Review* (57): 1701–77.

Olejnik, Lukasz, Steven Englehardt, and Arvind Narayanan. 2017. ‘Battery Status Not Included: Assessing Privacy in Web Standards’. In *3rd International Workshop on Privacy Engineering (IWPE’17). San Jose, United States,*.

Orwell, George. 1949. *Nineteen Eighty-Four (1984)*. London: Secker & Warburg.

Packard, Vance. 1965. *The Naked Society*. New York: Pocket Books Inc.

Posner, Richard A. 1977. ‘The Right of Privacy’. *Georgia Law Review* 12(3): 393–422.

———. 1981. ‘The Economics of Privacy’. *The American Economic Review* 71(2): 405–9.

Prost, Antoine. 1987. ‘Frontières et Espaces Du Privé’. In *Histoire de La Vie Privée. Tome 5 : De La Première Guerre Mondiale à Nos Jours*, eds. Philippe Ariès and Georges Duby. Paris: Seuil, 13–154.

Regan, Priscilla M. 1995. *Legislating Privacy: Technology, Social Values, and Public Policy*. Univ of North Carolina Press.

Reidenberg, Joel. 1997. ‘Lex Informatica: The Formulation of Information Policy Rules through Technology’. *Texas Law Review*: 553–93.

Reinach, Adolphe. 2004. *Les fondements a priori du Droit Civil*. Paris: Librairie Philosophique Vrin.

Rey, Bénédicte. 2012. ‘La privacy à l’ère du numérique’. *Terminal. Technologie de l’information, culture & société* (110): 91–103.

Roddenberry, G. (scriptwriter and producer), 1968, « Assignment: Earth », *Star Trek*, season 2 episode 26, Paramount, digital format.

Rodotà, Stefano. 1974. ‘Protection de La Vie Privée et Contrôle de l’information : Deux Sujets d’inquiétude Croissante Pour l’opinion Publique’. In *Questions d’ordre Politique Soulevées Par La Protection Des Données et Des Libertés Individuelles, Principes et Perspectives. Compte-Rendu Du Séminaire*, Collection études d’informatique, Paris: Organisation de Coopération et de Développement Economique (OCDE), 149–63.

Rosanvallon, Pierre. 1989. ‘The Development of Keynesianism in France’. In *The Political Power of Economic Ideas: Keynesianism across Nations*, ed. Peter A. Hall. Princeton, NJ: Princeton University Press, 171–94.

Rossi, Julien. 2016. ‘Framing the Privacy Debate and Big Data Governmentality in Degrowth Theory’. Presented at the Degrowth Conference Budapest, Budapest - Corvinus Egyetem. http://www.academia.edu/28309106/Framing_the_Privacy_Debate_and_Big_Data_Governmentality_in_Degrowth_Theory.

———. 2020. ‘The Hypothesis of the Privacy of Ancients and Moderns’. In *Digitalization of Society and Socio-Political Issues 1. Digital, Communication and Culture*, Systèmes d’information, Web et société, ed. Éric George. Londres: ISTE, 61–70.

Russell, A. L. 2006. '"Rough Consensus and Running Code" and the Internet-OSI Standards War'. *IEEE Annals of the History of Computing* 28(3): 48–61.

Sabatier, Paul A. 1998. 'The Advocacy Coalition Framework: Revisions and Relevance for Europe'. *Journal of European Public Policy* (5:1): 98–130.

Sabatier, Paul A., and Hank C. Jenkins-Smith, eds. 1993. *Policy Change and Learning: An Advocacy Coalition Approach*. Boulder, Colo: Westview Press.

Shils, Edward. 1966. 'Privacy: Its Constitution and Vicissitudes'. *Law and Contemporary Problems* 31(2): 281.

Steiner, Pierre. 2010. 'Philosophie, technologie et cognition. Etats des lieux et perspectives'. *Intellectica* 53(1): 7–40.

Stigler, George J. 1980. 'An Introduction to Privacy in Economics and Politics'. *The Journal of Legal Studies* 9(4): 623–44.

Svenonius, Per. 1974. 'Déclaration Succincte'. In *Questions d'ordre Politique Soulevées Par La Protection Des Données et Des Libertés Individuelles, Principes et Perspectives. Compte-Rendu Du Séminaire*, Collection études d'informatique, Paris: Organisation de Coopération et de Développement Economique (OCDE), 10–12.

Thomson, Judith Jarvis. 1975. 'The Right to Privacy'. *Philosophy and Public Affairs* 4(4): 295–314.

Tissot, Sylvie. 2013. *L'Etat et les quartiers. Genèse d'une catégorie de l'action publique: Genèse d'une catégorie de l'action publique*. Le Seuil.

Turner, Fred. 2008. *From Counterculture to Cyberculture: Stewart Brand, the Whole Earth Network, and the Rise of Digital Utopianism*. 1. paperback ed. Chicago, Ill.: Univ. of Chicago Pr.

United States Senate. 1967. *Computer Privacy: Hearings Before the United States Senate Committee on the Judiciary, Subcommittee on Administrative Practice and Procedure, Ninetieth Congress, First Session, Ninetieth Congress, Second Session, on Mar. 14-15, 1967, Feb. 6, 1968*. U.S. Government Printing Office.

US House of Representatives. 1966. 'Hearings before a Subcommittee of the Committee on Government Operations. House of Representatives, 89th Congress, Second Session'.

Utz, Christine et al. 2019. '(Un)Informed Consent: Studying GDPR Consent Notices in the Field'. *2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19),*. https://doi.org/10.1145/3319535.3354212.

Vitalis, André. 1988. *Informatique, pouvoir et libertés (2e éd.)*. Paris: Economica.

Vladeck, D., 2011. *A Word from Washington about Behavioral Advertising and Do Not Track*, FTC press release, March 8th. Availlable online: https://www.ftc.gov/sites/default/files/documents/public_statements/word-washington-about-

behavioral-advertising-and-do-not-track/110308forasspeech.pdf (document accessed on Dec. 20Th, 2019)

Ware, Willis H. 1967. *Security and Privacy in Computer Systems.* Santa Monica, Californie: Rand Corporation. Paper. https://www.rand.org/content/dam/rand/pubs/papers/2005/P3544.pdf (November 23, 2016).

———. 1973. *Records, Computers and the Rights of Citizens. Report of the Secretary's Advisory Committee on Automated Personal Data Systems*. U.S. Department of Health, Education and Welfare.

Warren, Samuel D., and Louis D. Brandeis. 1890. 'The Right to Privacy'. *Harvard Law Review* 4(5): 193–220.

Westin, Alan F. 1967. *Privacy and Freedom*. New York: Atheneum.

Younger, Kenneth. 1972. *Report of the Committee on Privacy. Chairman: Kenneth Younger. Presented to Parliament by the Secretary of State for the Home Department, the Lord High Chancellor and the Secretary of State for Scotland by Command of Her Majesty, July 1972.* London: H.M.S.O.

Zittrain, Jonathan. 2003. 'Internet Points of Control'. *Boston College Law Review* 44(2): 653.

Zuiderveen Borgesius, F. 2017. 'The Breyer Case of the Court of Justice of the European Union: IP Addresses and the Personal Data Definition'. *European Data Protection Law Review* 3(1): 130–37.

The full list of documents used in this doctoral research, including those quoted in this summary, is available in the original version of the dissertation, which can be downloaded from www.julienrossi.com/these .