Faculty of Social Sciences
University of Helsinki

THE POLITICS OF DATAFICATION

THE INFLUENCE OF LOBBYISTS ON THE EU'S DATA PROTECTION REFORM AND ITS CONSEQUENCES FOR THE LEGITIMACY OF THE GENERAL DATA PROTECTION REGULATION.

Jockum Hildén

DOCTORAL DISSERTATION

To be presented for public discussion with the permission of the Faculty of Social Sciences of the University of Helsinki, room 302, Athena, on the 8th of November 2019 at 12 o'clock.
Helsinki 2019

Publications of the Faculty of Social Sciences 2019: 127
Media and Communication Studies

ISSN 2343-273X (print)
ISSN 2343-2748 (web)
ISBN: 978-951-51-3409-7 (pbk)
ISBN: 978-951-51-3410-3 (pdf)
Unigrafia
Helsinki 2019

ABSTRACT

This study explores how one of the most talked about regulations in the internet policy domain was drafted. The General Data Protection Regulation (GDPR) has been widely regarded as one of the most lobbied pieces of legislation in the history of the European Union (EU). This raises two questions: What policy alternatives were put forth by the EU institutions in the course of the GDPR's legislative process, and how did they correspond to the ideas, issues and frames promoted by interest representatives? What does the influence of organized interests and stakeholders in GDPR decision-making reveal about the democratic legitimacy of the process?

Drawing on new institutionalism, this research traces the evolution of the GDPR, comparing the different EU institutions' iterations of the new law with the positions of interest representatives, and simultaneously situating the GDPR in the history of data protection policy. The results reveal that business groups dominated the public consultations prior to the Commission's draft proposal, but the Commission's approach was more closely aligned with the positions of civil society. Members of the European Parliament were, on the contrary, highly susceptible to the influence of business interests, until public salience of information privacy increased owing to Edward Snowden's revelations of governmental mass surveillance by the National Security Agency. These revelations made it possible for policy entrepreneurs to push for stronger rules on data protection.

However, public salience would not have a significant impact on the Council, which was mostly aligned with the interests of businesses and concerned with maintaining public interest exceptions. The final GDPR was more reminiscent of the Council's position than the Parliament's first reading, demonstrating that in many instances, business interests prevailed. This result should not be understood as mere resistance to policy change, but rather that a big data paradigm, which encourages the collection, processing and exchange of personal data in the name of progress, security and innovation, structured and constrained the available policy options. Therefore, the answer to the second question is that the institutionalized inclusion of stakeholders in the early stages of the process did not negatively impact its legitimacy, but the opaqueness and overall tendency to support business interests in the Council critically challenge the democratic legitimacy of the GDPR's legislative process.

ACKNOWLEDGEMENTS

This dissertation could not have been written without the help of my colleagues, who have helped me significantly throughout the years. First and foremost, I am immensely grateful for the support given by my two supervisors, Hannu Nieminen and Johanna Jääsaari, without whom I would never have embarked on an academic career to begin with. Already as a master's student, Hannu motivated me to delve deeper into the intricacies of internet policy regulation, and ultimately encouraged me to narrow my focus on the General Data Protection Regulation's legislative process. Johanna has on her part spent the past five years gradually shaping me into a political scientist, assisting me in finding ways to navigate research and theory on political processes and helping me sharpen my focus, which has tended to flounder.

During my time as a doctoral candidate I have had the pleasure of collaborating with the Helsinki Media Policy Research Group, which alongside my two supervisors includes Kari Karppinen, Anette Alén-Savikko, Katja Lehtisaari, and Minna Horowitz. I am very grateful for their insightful comments and encouraging words. Working with them has been and continues to be a pleasure. I would also like to thank Marko Ala-Fossi and Juha Herkman for their assistance with my various other academic endeavours, and my two external reviewers, Sandra Braman and Alison Harcourt, for urging me to think harder and hone my arguments.

I also want to extend my thanks to my colleagues at the Department of Media and Communication Studies at Södertörn University, my home away from home, for their valuable input on various parts of this manuscript, and the engaging discussions that we have had. Specifically, I want to thank Jonas Andersson Schwarz and Peter Jakobsson for taking the time to thoroughly review my drafts.

Lastly, I would like to thank my friends and family for enduring and supporting me during the past five years. To quote American poet Cody Chesnutt: 'all this caffeine in me, is the reason I've been so mean'.

CONTENTS

Tables

Figures

LIST OF ABBREVIATIONS

ACCIS	Association of Consumer Credit Information Suppliers
ACRO	Association of Clinical Research Organizations
ACT	Association of Commercial Television
AFME	Association for Financial Markets in Europe
ALDE	Alliance of Liberals and Democrats for Europe
BBA	British Bankers' Association
BCR	Binding Corporate Rules
BEUC	The European Consumer Organisation
BSA	Business Software Alliance
CBI	Confederation of British Industry
CEA	Comité Européen des Assurances
CIPL	Centre for Information Policy Leadership
CIA	Central Intelligence Agency
CJEU	Court of Justice of the European Union
CNIL	Commission nationale de l'informatique et des libertés
DG	Directorate-General
DG	INFSO Directorate-General Information Society
DPA	Data Protection Authority
DPD	Data Protection Directive
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DSCI	Data Security Council of India
EADP	European Association of Directory and Database Publishers
EBF	European Banking Federation
EBU	European Broadcasting Union
ECJ	European Court of Justice
ECHR	European Convention of Human Rights
ECR	European Conservatives and Reformists
EDPS	European Data Protection Supervisor
EDRI	European Digital Rights Initiative
EFTA	European Free Trade Association
EGDF	European Games Developer Foundation
ENPA	European Newspaper Publishers Association
EPOF	European Privacy Officers Forum
EPP	European's People's Party
ETNO	European Telecommunications Network Operators' Association

ETUC	European Trade Union Confederation
EULA	End-User License Agreement
EUROFINAS	European Federation of Finance House Associations
FAEP	European Federation of Magazine Publishers
FBI	Federal Bureau of Investigation
FIAD	International Federation of Film Distributors Associations
FIAPF	International Federation of Film Producers Associations
FTC	Federal Trade Commission
GCHQ	Government Communications Headquarters
GDPR	General Data Protection Regulation
GIS	Geographic Information Systems
Greens/EFA	Greens-European Free Alliance
GUE-NGL	European United Left–Nordic Green Left
IAB	Interactive Advertising Bureau's
IATA	International Air Transport Association
ICO	Information Commissioner's Office
ICT	Information and Communication Technology
IFPI	International Federation of the Phonographic Industry
IP	Internet Protocol
IPR	Intellectual Property Rights
ISP	Internet Service Provider
ITRE	Committee on Industry Research and Energy
IVF	International Video Federation
JURI	Committee on Legal Affairs
LIBE	Committee on Civil Liberties, Justice and Home Affairs
MEP	Member of European Parliament
MPA	Motion Picture Association
NGO	Nongovernmental Organization
NIGB	National Information Governance Board for Health and Social Care
NSA	National Security Agency
OECD	Organization for Economic Cooperation and Development
PPD	Presidential Policy Directive
S&D	Progressive Alliance of Socialists and Democrats
THL	Finnish national welfare authority
WFA	World Federation of Advertisers
WP29	Article 29 Working Party
WPPJ	Working Party on Police and Justice

1 INTRODUCTION

The use of data processing in all areas of life has exploded in the 21st century owing to the advances in both computing and networking. The increased processing power of computers and the introduction of social networking sites, cloud computing and the internet of things has contributed to an ever-increasing pile of data ready to be processed, in real time. The use of so-called big data promises efficiency and predictability, providing businesses, states and citizens the tools to technological innovation, new businesses, and solutions to climate change, urban planning, and medicine.

Barocas and Nissenbaum (2014, p. 46) identify big data not as a particular technology, but as a new paradigm for decision-making and knowledge production. It is connected to the quantification or datafication of all aspects of society (Mayer-Schönberger & Cukier, 2013) and used to inform both public and private bureaucracies in their daily operation. In contrast, the expanding databases of personal information have raised significant concerns, prompting legislators to create new rules regulating the use of personal data. Critical examinations of the online advertising economy and vendors of personal information encouraged the European Commission to initiate reform of the European Union's (EU's) data protection legislation. The goal of this dissertation is to explore the events that led up to the General Data Protection Regulation (2016/679) (GDPR), the EU's new data protection law that entered into force on May 25, 2018.

The notable presence of lobbyists during the GDPR's legislative process has been thoroughly documented,[1] and non-governmental organisations (NGOs) have demonstrated that many Members of the European Parliament (MEPs) were highly susceptible to the suggestions made by lobbyists (Lobbyplag, 2013, 2016). The question of whether these lobbyists were ultimately successful in shaping the final regulation has not yet been conclusively answered by earlier research.

The GDPR's legislative process is an ideal case for analysing the legitimacy of EU policy and regulations for a number of reasons. First, many policy insiders have claimed that the lobbying surrounding the GDPR was extremely aggressive (Fontanella-Khan, 2013). What is less certain, however, is how the legislative process as a whole was affected by interest representatives. Previous

[1] German broadcaster ARD even aired a documentary about the legislative process called Democracy – Im Rausch der Daten (Democracy-film, 2018).

research on the GDPR has mostly focused on the impact of the Snowden revelations on the process (Rossi, 2018; Laurer & Seidl, *forthcoming*; Kalyanpur & Newman, 2019), but notably less scholarly attention has been devoted to examining to what extent interest representatives were influential.

Second, the GDPR is the latest regulation in a series of legal instruments aimed at regulating different aspects of the datafication of society. Therefore, its legislative process is instrumental in examining whether historical trajectories and path dependence have made data protection policy sufficiently rigid to withstand both political conflict and exogenous pressure caused by the rise of social media, the National Security Agency (NSA) revelations, and the overall ubiquity of online tracking and surveillance.

Third, the GDPR has already had an outsized impact on a wide variety of industries, forcing actors to oversee their data-handling practices to avoid sanctions associated with non-compliance. Furthermore, many countries have been inspired by the EU's approach and adopted or plan to adopt similar legislation, partly in order to enable unhindered data transfers from the EU.[2] The extraterritorial application of the GDPR also means that it has generated a lot of interest outside the borders of the EU. Thus, it is a suitable case study for examining the role foreign influence can have on the EU's legislative processes, which has not received much attention in interest group research.

In sum, this dissertation aims to find out whether interest representatives were able to influence the contents of the different versions of the GDPR as presented by the EU institutions. The study will focus on the extent to which the interests of stakeholders are represented in the different versions of the GDPR, dating back to the first Commission Communication (2010a) on the protection of personal data. Whose voices were heard in the process, and how did the Commission, the Council, and the Parliament take conflicting interests into account in the drafting of the GDPR? How was the right to privacy operationalised, and which information privacy applications that stakeholders suggested ended up in the different draft Regulations? Can the legislative process be perceived as legitimate, given the extensive lobbying involved?

Thanks to a determined effort to increase the transparency of the EU's legislative process, alongside the position papers submitted to the public consultations, lobby position papers submitted to MEPs were made available during the legislative process (Lobbyplag, 2013). These papers and the EU institution's respective draft regulations will serve as the main sources on which this study is based. Thus, the position papers will serve as a valuable source depicting how stakeholders advocate for different policy applications,

[2] See CNIL (2019) for a comprehensive list of national data protection laws.

and show how data protection regulation affects different spheres of activity. Therefore, their value is not simply connected to this particular legislative process, but to normative questions of privacy and data protection in general.

1.1 BACKGROUND

The GDPR is unquestionably one of the most influential information and communication technology (ICT) laws that have been drafted because it aims to govern not only European companies, institutions and organisations but also actors from other continents that offer services to Europeans. Moreover, the GDPR introduced fines for violating privacy provisions up to four percent of the annual turnover of the violating party. Such severe sanctions have previously only been found in the sphere of competition law. For these reasons (and others) national public authorities, NGOs, trade associations, companies and private individuals have tried to influence legislators via official consultative procedures and more targeted lobbying.

The big data paradigm is inherently connected to discourses of competitiveness, productivity, and the future. In technology, there is a dominant narrative that openness and sharing of data will foster economic growth and provide new means of producing value to the greater good of society. Regardless, the big data paradigm is often critically at odds with fundamental rights such as the right to privacy. New technologies have always challenged not only existing regulation but also existing social norms of privacy, on which laws are based (Tene & Polonetsky, 2013), but the challenges associated with the big data paradigm are manifold. First, digital technologies produce, as a rule, a trace. Whereas the imperfection of memories and human record-keeping enabled privacy rights in practice, digital records are designed to persist over time. Moreover, the nature of data is highly different. Social networking sites, fitness apps and smart smoke alarms lack historical equivalents because the data they provide is significantly richer and more frequently updated. What happen when information that used to be intimate is stored on the servers of private companies? Who 'owns' the information, and how may it be used? Is the automatic mining of keywords on an instant messaging app comparable to someone reading a private conversation? Do intellectual property rights trump privacy rights? Is online tracking comparable with tracing someone in person? This is sometimes referred to as the 'variety' of data that constitutes a defining element of big data. In sum, it is not only the sheer volume but also the richness of data that has changed.

Second, the velocity of data is amplified – not only in speed of the collection of data from a variety of sources but also in terms of actual transfers of databases. Data changes hands and crosses borders at an intensifying pace. This makes it increasingly difficult to trace where the information is going and for what purposes. Therefore, a central problem is the lack of transparency surrounding the use of personal data. A report on U.S. data brokers by the Federal Trade Commission (2014) noted that nine data brokers collectively register data on hundreds of millions of users worldwide and add billions of new records each month. While this problem is endemic to the U.S. where no federal law on privacy protections exists for consumer relationships, many of the companies also operate in Europe. Importantly, there is still little oversight of how personal data is transferred and merged into different databases. As Pasquale (2015, p. 21) points out, we do not know 'how data from one sphere feeds into another … [but] [w]e do know that it does'. With social networks, smartphones and countless smart devices there are now more data sources on citizens than ever before, and the number of connected devices will only increase.

To some extent, our privacy has in practice become something to barter with: we agree to access a service by sacrificing privacy (van Dijck, 2013, pp. 170-1). People readily accept the terms that service providers present as a condition to access their services, but it is unclear to what extent consent is given consciously. It is this balance of data utility and protection that legislation tries to strike, but finding the appropriate level of protection without undermining legitimate uses of data is challenging (Ohm, 2010, pp. 1704-1705). On a societal level, this might mean that better services, medicine or products are made available, and it is often difficult to see when the sacrifice is proportionate to the gains – the sacrifice might be invisible to people, and the consequences might not materialise until several years after the data has been collected. The Cambridge Analytica scandal is a case in point. The users of the Facebook app 'This is Your Digital Life' could hardly imagine that their and their friends' data would be used for micro-targeting in the U.S. presidential election in 2016 and lead to a massive privacy scandal (Hern & Cadwalladr, 2018) forcing Facebook CEO Mark Zuckerberg to testify in front of the U.S. Congress[3] and answer the European Parliament's questions.

Internet services in the 21st century have one defining characteristic: they are often connected to central databases, i.e. 'the cloud', that not only store data on their users but also provide their owners with an ample supply of data

[3] Some questions were answered in two documents submitted almost two months after the hearings (Facebook, 2018a, 2018b).

which can be mined for intelligence. The 21st century information society is based on collecting and processing data to acquire *actionable intelligence* (Gandy, 2012). Although this process seldom includes the physical monitoring of people, it is nonetheless a form of surveillance. While surveillance triggers negative connotations, its etymological origins are neutral: to watch over.[4] It is perhaps for this reason that several terms have been used to designate different forms of surveillance: consumer monitoring, intelligence gathering, spying, supervising, observing, auditing and tracking, depending on the context – sometimes different terminology implies different legal obligations. The one who surveils might have the best of intentions, but the constant tracking of the movements and communications of people opens for abuse and risks.

Legal loopholes and unanswered questions are abundant. Law is slow and code is fast, which means that regulation always lags technological development. Legal reforms take years to process, especially in the EU, whereas new software can be deployed instantaneously with a disrupting impact. For this reason, laws are often either too far-reaching or simply ineffective (Ohm, 2010, p. 1736). However, laws should still reflect social perceptions of privacy and not the technological development of surveillant instruments. The availability of sensitive personal information, such as sexual preferences through dating apps, should not lead to the conclusion that this data can be exploited without considering individuals' sense of privacy. The expansion of big data analytics and behavioural marketing should not lead to an apologetic privacy regime that fails to offer Internet users a reasonable level of data protection.

Legislators strive to regulate the use of data through various data protection instruments. European governments have valued information privacy long before big data was a concept, whereas the U.S. approach has been marked by laissez-faire and self-regulatory instruments. The governments of France, Germany, and the UK already adopted rigorous data protection rules in the 1970s (Newman, 2008a), concurrently pressuring the European Community to adopt its first Data Protection Directive (95/46/EC) that eventually entered into force two decades later. The above-mentioned developments have, however, forced the EU to reassess its data protection legislation.

---

[4] The historical origins of the English use of the word are, however, less neutral: the word came to English from the Terror in France where 'surveillance committees' were formed in 1793 to monitor suspected persons and dissidents (Online Etymology Dictionary, 2014).

The GDPR aims to not only clarify data protection rules and address loopholes in the law but also advance the single market. By harmonising the data protection rules across the Union, the EU institutions hope to achieve a better level of protection for citizens and clearer and consistent rules for businesses that operate in the region. On the one hand, the right to privacy of citizens is a primary concern. On the other hand, the new legislation affects both private and public use of big data and challenges business models and surveillance schemes on a wider scale. Regulation which advances the interests of citizens might be unfavourable for marketing companies or research institutions.

1.2 AIMS AND RESEARCH QUESTIONS

Data protection legislation is inherently complex, and it can be difficult to balance privacy, security, property rights, and business interests. Stricter data protection rules do not always favour citizens because they might outlaw useful applications. Bearing this in mind, it is important to examine not only if the views expressed by interest groups are reflected in the policy output of the EU institutions but also if the structural imbalances of participation among different interest representatives during the process have an impact on the outcome. Given the big data paradigm encouraging the collection and processing of personal data, how susceptible are the EU institutions to the influence of actors involved in these activities, and what effect does the inclusion of stakeholders in the legislative process have on the outcome? Thus, the main, overarching focus of this study can be divided into the following research questions:

1. What policy alternatives were put forth by the EU institutions in the course of the GDPR's legislative process, and how did they correspond to the ideas, issues and frames promoted by interest representatives?

2. What does the influence of organised interests and stakeholders in GDPR decision-making reveal about the democratic legitimacy of the process?

The first question relates to how problems associated with the data protection domain are defined by interest representatives and what solutions the EU institutions propose to remedy the identified issues. To quote Campbell (2004, p. 107), 'how do ideas affect institutional change?' To answer the question, I need to look outside the legislative process of the GDPR. I will not only focus

on specific events but also on discourses on surveillance and privacy. I use Pinizza and Miorelli's (2013, p. 303) post-structuralist conceptualisation of the term: 'discourses involve political struggles to inscribe and partially fix the meaning of a term within a certain discursive chain to the exclusion of others'.

To provide the necessary context for the evolution of data protection policy, I draw on both surveillance studies and socio-legal theories of privacy to explain the development of data protection regulation. Surveillance studies are a decidedly broad and multidisciplinary field composed of political economy scholarship, sociological and historical accounts, as well as more philosophical work. Common to most of these approaches is a broader perspective on the structures that enable surveillance in society. Therefore, they are more apt at describing where ideas come from than the policy studies literature.

In contrast, socio-legal theories of privacy are much more focused on the individual and often draw on psychological studies. While this dissertation does not seek to present a theory of privacy, I will demonstrate how the perceptions of privacy have guided information privacy regulation. At this point, it is also worth noting that public disclosures of private information are generally outside the scope of this dissertation, and the dichotomy between freedom of expression and the right to privacy will only be touched upon in connection to information privacy legislation. The right to private life is not the focus of this study but information privacy and the legal concept of data protection are.

The second question is focused on the role of institutions. It is theoretically grounded in the field of EU interest group studies and focuses on the democratic aspects of the GDPR's legislative process. First, this study aims to examine how different concepts of legitimacy can be used to evaluate the process. Here I draw mainly on Scharpf's (1999) input–output legitimacy model focusing on the input by citizens on the one hand and the output of the EU institutions on the other and Schmidt's (2013) concept of throughput legitimacy, which mainly looks at the process.

A question which undoubtedly arises is whether the legislative process must include a deliberative element (Habermas, 1999) or whether other procedural elements can be used to overcome the democratic deficit of EU policy-making. I also aim to address the question of influence, drawing on both new institutionalism as well as interest group studies in the EU to inform my methodological choices and support my analysis (cf. Peters, 2012; Zahariadis, 2008; Coen & Richardson, 2009). The primary method applied in this study is *process tracing*, which entails analysing evidence of the different stages of policy to infer causal relations (Collier, 2011). My aim is to demonstrate

influence by studying the different iterations of the GDPR and comparing them to the regulatory applications promoted by interest groups and other advocates.

While process tracing is often associated with historical institutionalism, there are notable connections to discursive institutionalism where policy discourses and ideas have a central role (cf. Peters, 2012, p. 112; Schmidt, 2008; Schmidt, 2010). Historical institutionalism is useful for understanding how institutions maintain the policy equilibrium, whereas discursive institutionalism is more apt at explaining policy change by looking at the agency of policy actors and the role of ideas and discourses (Schmidt, 2006; Schmidt, 2008). In the case of data protection policy, both approaches are valuable. The aim is to provide a contextually rich study that not only focuses on the internal aspects of the legislative process but also emphasises how broader societal structures impact concrete policy applications.

Finally, it is worth reflecting on how data protection regulation sits in the broader framework of media and communication policy. Media and communication policy studies in the European context have traditionally focused almost exclusively on either the broadcasting or telecommunications policy (cf. Donders, Pauwels, & Loisen, 2014; Simpson, Puppis, & Van den Bulck, 2016; Freedman, 2008; Michalis, 2007; Harcourt, 2005; McQuail & Siune, 1998) while leaving questions of information privacy regulation to legal scholars. Therefore, the purpose of this dissertation is to introduce information privacy into the field of media and communication policy studies. The digitisation of both the media and communication means that the very provision of such services is dependent on processing vast quantities of personal data.

The major impact of social networking sites and the rise of behavioural advertising as the dominant model of revenue accumulation for media industries mean that data protection is no longer a peripheral question of media and communication policy but at its very core. From a critical political economy perspective, the role of data has already been detailed by scholarship focused on so-called datafication (van Dijck, 2014, 2018, p. 33). The term originates from the book by Mayer-Schönberger and Cukier (2013, p. 77) on big data and signified transforming qualitative elements into quantitative data points, but other scholars, such as van Dijck (2014, p. 198), have used the term in a narrower sense as 'the transformation of social action into online quantified data, which allows for real-time tracking and predictive analysis' (see also Hintz, Dencik, & Wahl-Jorgensen, 2018; Lupton & Williamson, 2017; Couldry & Hepp, 2018). To not confuse the concepts, I will refer to the big data paradigm when addressing the general societal trend to quantify, record, log,

and use large datasets to inform decision-making and refer to datafication when discussing the quantification of social action. Therefore, datafication is a key component of the broader big data paradigm and also inherently connected to data protection. Datafication has been conceptually addressed within the field of media and communication studies, but these studies have generally been limited to political economy approaches and not looked at how the big data paradigm informs and impacts policy. It is this critical connection that this study aims to explore.

1.3 STRUCTURE AND SCOPE

Examining the GDPR's legislative process in isolation of the development of the Internet and surveillance technologies would clearly not result in an adequate answer to the research questions stated above. Because the first research question relates to the influence of interest groups and other advocates, it is also necessary to address the societal power that data industries wield. At this stage, it is important to note that almost all industries are, on some level, data-intensive. Therefore, the approach here is to refrain from the temptation of focusing on some of the key players in the online economy and instead discuss the wider framework of surveillance. The theoretical underpinnings of the second chapter are mainly drawn from the work of surveillance scholarship that can be traced back to two schools of thought: (neo)Foucauldian accounts focusing on societal control and critical political economy theories of communication. As demonstrated below, a combination of the two is better suited at providing an explanation of the material and ideational building blocks that have contributed to the big data paradigm.

The third chapter is focused on the evolution of data protection policy in the EU. The order of chapters two and three is not a coincidence. All important developments in the field of privacy law were preceded by significant technological changes. The law of privacy would likely not have been codified unless new technologies and their implementation had radically challenged pre-existing normative conceptions of publicity and privacy. The position here is that data protection cannot be seen as a separate legal domain that is only related to the broader concept of privacy but rather a more operational concept that is on a lower level of abstraction than privacy. Moreover, I discuss the role of path dependence and policy entrepreneurs to historically contextualise policy equilibrium and change in the EU and what role both played in the development of European data protection policy and regulation.

After addressing the societal shifts that serve as the context in which the GDPR was drafted, I will address the question of legitimacy of EU policy and specifically the inclusion of stakeholders in the legislative process. To this end, it is imperative to provide an overview of the influence of interest groups in the EU in general to shed some light on the particularities of drafting legislation in the data protection policy domain. Chapter four outlines the policy environment in the EU and focuses on providing both the theoretical rationales for the inclusion of third parties in the legislative process and more empirical accounts on what lobbying in the EU looks like. My approach is influenced by EU policy studies on the three levels of democracy legitimacy: *input*, *output*, and *throughput legitimacy*. Each of these concepts will be further explored and connected to the context of data protection legislation below.

The methodological approach heavily draws on empirical policy studies on lobbying and is further outlined in chapter five. While it might be tempting to revert to either a deep reading of some of the proposals using discourse analysis or a quantitative content analysis of all the documents, the method applied here, process tracing, uses mainly qualitative document analysis to draw causal inferences from documentary sources. There are two main reasons for taking this approach. First, a more in-depth approach would clearly result in a more detailed reading of some of the aspects of information privacy, but a more limited sample would mean missing important details that contribute to the larger narrative that is the goal of process tracing. Moreover, as position papers can be quite limited in scope and are mostly focused on advancing specific interests, they are not as suitable for discourse analysis as other, more strategic policy documents. Second, although quantitative content analysis would enable a full analysis of the entire material provided in the legislative process, there are some issues that undermine the utility of this approach. The position papers do not represent all lobbying positions, meaning that even the results from a study of all position papers submitted could not necessarily be representative of all possible industry interests. Moreover, it would be difficult to address more normative issues without looking at the position papers' complete line of argumentation. Therefore, there are no apparent benefits to using an exclusively quantitative approach, but some quantitative elements have been incorporated to provide additional context to the qualitative analysis.

The results are presented in chapters six and seven, focusing on examining the GDPR's legislative process from a legitimacy perspective and outlining the discursive ideas that shaped the EU institutions' proposals. The questions are answered through a chronological review of the different steps of the

legislative process, expanding on the background provided above and filling in details on how the legislative documents evolved over time. The findings can be categorised on three different levels. On the first level, I provide a detailed description of the different parties to the legislative process and their respective agendas. On the second level, I outline how the interests and agendas are represented in the EU institutions' proposals. On the third level, I discuss the differences between the EU institutions' proposals and what the finalised GDPR means for citizens, businesses, and the public sector.

Finally, I will conclude by assessing to what extent the GDPR was shaped by interest representatives, and what this means for the legitimacy of the process. After summarising the results of the study, I will discuss how the GDPR's legislative process relates to the general societal development of datafication. What will be the consequences of the GDPR in the short-term, and will it be able to challenge the current trend of data maximisation on a wider scale?

2 CONCEPTUALISING THE BIG DATA PARADIGM

> *Ultimately, it's important to remember that data protection is about power. Anyone who has ever tried to access their data quickly recognizes the profound informational asymmetries that characterize today's data economies.*
>
> *Frederike Kaltheuner, Privacy International (Kaltheuner, 2018).*

The policy initiative to amend the EU's data protection legislation cannot be understood simply in terms of a regulatory void created by technological advances. Rather, it is a reaction to a wider paradigm shift that relates to surveillance and how decision-making is rationalised. According to Campbell (2004, p. 94), 'paradigms are cognitive background assumptions that constrain decision making and institutional change by limiting the range of alternatives that decision-making elites are likely to perceive as useful and worth considering'. Following Campbell (2004) and Schmidt (2008, p. 307), data protection policy has elements of both cognitive ideas that aim for concrete policy solutions and normative ideas that 'attach values to political action and serve to legitimate the policies'. These ideas form part of what can be determined as the big data paradigm.

A few societal trends are decisive in understanding both the cognitive and normative ideas that shape data protection policy. The first change is the increased bureaucratisation of society that builds on progressively granular record-keeping. Uses of personal information are not only limited to the bureaucratisation of the nation state but also increasingly serve commercial bureaucracies. Data matching and sorting technologies traditionally used for public services and administration may be repurposed for security policy and practice if there is political will to do so (Webster, 2012, p. 317). Moreover, commercial data brokers often have public authorities among their clients, resulting in data being transferred between private and public bureaucracies. This, in turn, means that the data collected on individuals is increasingly granular and used for a wide variety of purposes (van Dijck, 2014). The second change is that the purpose of surveillance has evolved from discipline to discipline *and* prediction. The third change is connected to the first two developments: big data has become the epistemic standard of knowledge production. Policy, action, and decision-making are increasingly reliant on the analysis of massive datasets (Barocas & Nissenbaum, 2014, p. 46). As boyd

and Crawford (2012, p. 14) suggest, '[t]here is a deep government and industrial drive toward gathering and extracting maximal value from data, be it information that will lead to more targeted advertising, product design, traffic planning, or criminal policing'. A natural consequence of this is the commodification of personal data, resulting in the creation of a market for personal information that is most pronounced in the field of advertising but serves other uses as well.

The following chapter will outline three constitutive elements of the big data paradigm: the bureaucratisation of society, datafication of social action, and market for personal information. Data protection regulation cannot be addressed merely from a perspective of privacy but must consider the contexts where personal information is used. Therefore, this chapter aims to provide a theoretical framework for understanding privacy as a legally recognised exception to data-driven bureaucratisation. The very purpose is therefore to explore the limits of this relative fundamental right before turning to how it has been operationalised in chapter three.

2.1 BUREAUCRATIC CONTROL, DISCIPLINE AND PREDICTION

The history of surveillance traces two curves – the development of the modern nation state and the development of record-keeping in various forms. As the two are inherently intertwined, significant technological advances have both marked a shift in society at large and surveillance at the same time. Tracing the prehistory of surveillance, Lyon (1994) highlights census records in ancient Egypt as one of the earliest examples of state surveillance. For Lyon, drawing on the work of Innis (1951), a prerequisite for surveillant administration was the development of writing and thus record-keeping. Much later, the invention of the printing press would speed up the development of modern governance. Similarly, Mayer-Schönberger and Cukier (2013, p. 78) define datafication as 'humankind's ancient quest to measure, record and analyse the world'.

The 19th century scholars such as Karl Marx, Frederick Taylor, and Max Weber have already established the link between bureaucratic efficiency and surveillance. During this time, the bureaucratisation of nation states intensified and included personal documentation (Lyon, 1994, p. 31). For Weber, the efficiency of management and thus bureaucracies was dependent on surveillance that stems from both record-keeping and direct supervision (Dandeker, 1994). In Weber's view, the nature of bureaucracies was both

productive and destructive at the same time – enabling the efficient management of people but trapping individuals in an iron cage of bureaucracy that renders them into cogs in a soulless machine (Weber, 1978).

For French philosopher and historian Michel Foucault, the development of the modern bureaucracy is connected to when surveillance superseded violence as the primary disciplinary tool in the 18th century. In his landmark work *Discipline and punish: the birth of the prison*, Foucault (1977) outlined how the modern nation state stopped using corporal punishments and started incarcerating and monitoring its subjects instead. One of Foucault's key theoretical contributions is the concept of *panoptic surveillance*. The term refers to 18th century philosopher Jeremy Bentham's model prison, the *Panopticon*. Bentham's Panopticon was a prison which is built like a circle with cells facing the inner prison yard. A guard tower occupies the heart of the yard, allowing the guards to see into each cell in the prison. The prisoners are always in the guards' line of sight, yet they are never certain of when they are being surveilled. The prisoners simply must assume that they are being watched, and this assumption guides their behaviour. Surveillance is thus used to *discipline* populations. This is not to say that the importance of violence had receded. The threat of violence was (and is) of course a constitutive element of the disciplinary nature of surveillance. According to Foucault, the panoptic model was eventually applied in principle in society at large, although Bentham's architectural vision was not widely employed. This transition is what constitutes the *panoptic diagram*, a society organised by discipline through surveillance. Although most subsequent scholarly accounts on surveillance have focused on this aspect of Foucault's work, Foucault himself also stressed that the purpose behind surveillance was often to increase the productivity of the subjects of surveillance, be it students in schools, soldiers in the military or patients in the hospital. In other words, Foucault's panoptic diagram is highly inspired by Weber's vision of societal bureaucratisation.

Although Foucault's panoptic diagram serves as a starting point in understanding the function of surveillance in society, modern day surveillance has evolved (Lyon, 1994, p. 78). The fragmented yet continuous collection of data from a multitude of sources has been termed *panspectric surveillance* (De Landa, 1991, p. 180). [5] For example, commercial surveillance has traditionally used four 'surveillance streams': customer records from

[5] While panspectric surveillance refers mainly to signals being transmitted on the electromagnetic spectrum, most contemporary surveillance is focused on digital streams of data, and the technical delivery – a network cable or radio frequency – is of secondary importance compared with what platform was used to intercept the data.

companies, direct marketing companies, credit bureaus, and government (Schneier, 2015, pp. 51-2). Internet surveillance is a fifth stream that partly includes all of the above. The collected data is subsequently filtered and analysed by computers to produce *actionable intelligence* that can be used to guide decision-making (Gandy, 2012, p. 125).

Whether one calls it ubiquitous surveillance, post-panoptic surveillance or the panspectric diagram, it differs from the panoptic diagram in that the purpose of surveillance is not to influence the behaviour of the surveilled but to collect as much information as possible to identify security threats (Brown & Korff, 2009, p. 124), recognise customer patterns (Pridmore & Zwick, 2011, p. 272) and predict future behaviour (Zwick & Knott, 2009, p. 234; Hildebrandt, 2006, p. 548). In most cases, present day surveillance is, in other words, less about discipline and more about omnipresent record-keeping and prediction (Gandy, 1989, p. 63). This applies equally to both public and private bureaucratisation (Dandeker, 1994, p. 61; Gandy, 1993, p. 47). To mark this shift, surveillance scholars have used concepts such as *dataveillance* (Clarke, 1988), *ubiquitous surveillance* (Andrejevic, 2012, p. 92), *the panoptic sort* (Gandy, 1993), *superpanopticon* (Poster, 1990), *panspectron* (Braman, 2006, p. 315) or *panspectric diagram* (Palmås, 2011, p. 350). A defining feature of contemporary surveillance is that individuals are monitored on numerous levels by several actors and data collected in one context is frequently used in another, a practice which has been labelled *function creep* (Lyon, 1994), *surveillance creep* (Bogard, 2012) or *mission creep* (Christl, 2017). The collection of data is usually rendered permissible in one policy domain and subsequently moves into other areas.

The shift from Foucault's terminology signifies that the primary objective of surveillance is not the threat of watchful eyes but the promise of preventing undesirable individuals from acting or predicting the life choices of individuals (Gandy, 1989, p. 64). In a perfect post-panoptic state, discipline is not necessary because predictive technologies prevent all forms of crime from ever occurring. However, the quintessential democratic problem with such surveillance is that it is fundamentally opposed to the principles of the *Rechtsstaat*, such as transparency of decisions, due process, and non-discrimination.

Video monitoring equipment is, of course, still used extensively for the very purposes Foucault envisioned, suggesting that the shift from discipline to prediction is not complete. However, it must be underlined that modern surveillance is more about the information surveillance provides than about the behaviour it shapes. New developments in machine learning and, especially, facial recognition technology mean that video surveillance will

become an integrated part of the predictive surveillance apparatus, focusing less on the disciplinary effects of being watched and more on the data that can be drawn out of the images. In China, the disciplinary and predictive elements of surveillance have now merged with the launch of China's 'social credit system'. Presently, the social credit system logs the offences, awards, and volunteer work that can directly affect people's ability to travel within the country and obtain a mortgage (Mistreanu, 2018). The social credit plummets only for breaking the law, but it is easy to see how the system can be abused in a country where fundamental freedoms are frequently trumped in the name of social order. Although the exact parameters of the final social credit system are not yet known, the system has been envisioned to not only include criminal offences but also evaluate networks of friends, consumer data, and social media activity similar to the Alibaba-affiliated social credit system *Sesame Credit* (Botsman, 2017).[6]

A key point raised by Gandy (1989, p. 64) is that surveillance, while often automatic, is usually triggered by the data subject[7] themselves – either by accessing a website, using a credit card, or signing up for a loyalty programme or life insurance. These actions are superficially consensual because individuals trade their privacy for goods and services. According to Gandy (1989, p. 66), organisations also collect more information on people than is 'socially optimal'. Moreover, because each isolated piece of information might seem trivial and come with a small privacy cost and keeping track of the big picture is nigh impossible, 'individuals are incapable of acting in their own interests'. Cohen (2016) has coined this as 'the participatory turn of surveillance'. This is not to say that this action would be an expression of free will – it is precisely the type of disciplinary system that Foucault envisioned would make us obedient subjects or, in many cases, consumers. The freedom of choice is heavily influenced by two factors: the lack of meaningful choice and the penalisations (either social or economic) involved in refusing surveillance. Sometimes the loss is highly tangible, such as in the case of

[6] A prerequisite for the Sesame credit system is that data collection is highly centralised in China, where WeChat, the everything app, reaches 850 million citizens. The data collection practices involved in creating the social credit system are unquestionably pervasive, but it remains to be seen if the consequences are more severe than what is already achieved through regular credit rating systems that also draw from a variety of data sources.

[7] Data subject is a legal term which refers to the individual whose personal data is being processed. It should not be conflated with 'user' or 'consumer' because data subject status is not contingent on having a customer relationship with the entity that processes the data. It should also not be equated with 'citizen' because citizen status is frequently irrelevant for jurisdictional purposes and mere residence or even current location may be enough.

various retail loyalty programmes where members shop at a discount, whereas sometimes the loss is more intangible, such as missing invitations to parties because one does not have a Facebook profile. It is this unequal relationship in combination with the 'spread of the computerisation throughout the bureaucratic infrastructure' that strengthens the bureaucratic enterprise's power over the individual (Gandy, 1989, p. 65). Therefore, information inequality between data subjects and data collectors is best explained through the inability of the individual to have a say – the power of the bureaucratic organisation is congealed by its institutional structures rather than pure hierarchical relationships between individuals (Gandy, 1989, p. 62). Take, for example, the Cambridge Analytica scandal – Mark Zuckerberg's profile data was found among the information that was shared with the notorious data broker. Not even the CEO, founder, and biggest share-holder could shield himself from bureaucratic control of his own creation.

Innovations during the past 150 years have radically improved the surveillant assemblage or in Rule's (1974) terminology, the surveillance capacity of nation states and private bureaucracies. The mid-to-late 19th century and the 20th century innovations such as the electric telegraph, photographic film, telephone, radio, personal computer (PC), satellite communications, and Internet have not only radically sped up communications but also impacted how private communications can be intercepted and populations can be monitored. These technological changes have also triggered regulatory change.

As communications have become digitised, the data has become richer as well. Datafication relies on the availability of behavioural data, which is inherently connected to how technologies of communication have evolved. In the end of the 1980s, Gandy (1989, p. 67) wrote that the spread of PCs in the workplace represented 'temporary loss of … surveillance potential' because the data was handled locally but predicted that the use of local area networks would remedy this in the future. Gandy's prophecy was right, but he failed to realise the scale. According to Cisco (2018), one of the world's largest networking equipment providers, 94% of all workloads will be processed in the cloud by 2021. From the perspective of surveillance, this means that data which were previously accessible locally are now frequently stored externally in data centres across the world. From a jurisdictional perspective, it means that data previously contained within one jurisdiction now crosses borders and might leave the owners of the database without necessary legal safeguards. I will now illustrate how this availability of communicative and behavioural data contributes to the creation of profiles.

2.2 DATAFICATION AND THE DATA SUBJECT

The first parts of this chapter dealt with the evolution of the present surveillance society and connected the technological developments with a greater societal trend to track, analyse, and predict people's behaviour. I will now turn to how datafication produces *data subjects* and how it relates to the big data paradigm.

The underlying logic of surveillance has not changed radically from the 90s, but the scale of data collection and the availability of data have reached a different scale, which lead to the widespread usage of the term *big data* since the early 00s. The definition of big data tends to vary, but the definitions tend to include the following characteristics: there are large quantities of data, it is collected in real-time and changes quickly, and the data is high in complexity owing to an extensive range of data types and sources (see e.g. Kitchin, 2014; Laney, 2001; Franks, 2015, p. 4, 24).[8] The meaning of big data has somewhat expanded from referring to what the datasets contain to including also the inferences and analysis of said data. This definition can be compared with Rule's (1974, pp. 37-40) four factors explaining the growth of 'surveillance capacity': (1) the size of files, (2) the degree of centralisation, (3) the speed of information flow, and (4) the number of contacts between administrative systems and subject populations.

A key aspect of the big data paradigm is that everything is logged in the odd event that the data might at some point be useful (Schneier, 2015, p. 19). Big data thrives in an environment of data maximisation because present day data collection cannot predict future correlations. As Pasquale (2015, p. 32) explains, causal relationships do not have to be established because 'correlation is enough to drive action'. According to Athique (2018, p. 65), big data is nothing but numerology,[9] as the lack of interest in causality constitutes an explicit departure from the epistemology of science. Kitchin (2014) makes the important point that while a paradigmatic shift is underway, it is worth distinguishing between big data analysis in the form of completely inductive empiricism and data-driven science which is more firmly rooted in the scientific tradition of deductive reasoning. While the second category of science is certainly more epistemologically sound, it is at the same time influenced by the data maximisation paradigm. Although data maximisation

[8] The industry usually refers to the three to five V's of big data: volume, velocity, variety, variability and value. An oft-quoted simplified definition is 'data too big for an excel spreadsheet'.

[9] The Oxford English Dictionary defines numerology as 'the branch of knowledge that deals with the occult significance of numbers'.

is unproblematic for non-personal data, it becomes controversial when applied to personal data. As Athique (2018, p. 62) points out, 'For the purposes of the computational process alone, it is fundamentally irrelevant whether this information being unitised is about people or brightly coloured rocks'. For the people whose lives are impacted by the decisions influenced by statistical inferences, the lack of established causality is more problematic. The idea that anything can be solved with sufficient data is further facilitated by the lowered costs of retaining data. The cost of computing power and storage have decreased immensely in the previous decade and essentially removed any economic incentive to delete data that previously limited data collection and surveillant practices (Schneier, 2015, p. 24). Therefore, such incentives must be created with the help of regulation.

Corporate actors log billions of transactions worldwide to create consumer profiles for various purposes. Insurance companies create risk profiles to determine appropriate premiums (Bouk, 2018), and credit rating agencies rate individuals' creditworthiness based on past transactions (Lauer, 2017). Online advertising networks generate detailed profiles based on online behaviour, and data brokers aggregate data from all of these sources (Schneier, 2015; Christl, 2017). Security agencies like the U.S. NSA or the British Government Communications Headquarters (GCHQ) gather information to create security profiles (Greenwald, 2014). Although these profiles have been critiqued with terms such as *dividual* (Deleuze, 1992) or *data double* (Haggerty & Ericson, 2000, p. 606), the critique often focuses on different tools of surveillance but ignores how these profiles are constructed in practice.

What is important to note is that *objective data points*, such as age, sex, income, births, and deaths, have always been part of the modern bureaucratic state (see above and, for example, Giddens, 1985). The difference is that behavioural data points, such as what people like to read, what people are searching for online, whose social media profiles they look for, and other interests, are significantly easier to map than before (cf. Bolin, 2012; Bolin & Andersson Schwarz, 2015; van Dijck, 2014, p. 201).

While these events produce objective data points, they are used to infer *subjective elements* such as interests, psychographics, affective states, and behaviour. More than that, the subject is 'reproduced' in advance (Bogard, 2012, p. 35). The consequence is that a clear distinction between objective data points and subjective elements is no longer possible.

From a profiler's perspective, the challenge does not lie in tracking people – these technologies are already quite advanced. The challenge lies in applying the appropriate weights to a wide variety of indicators to make the right assessments of people's traits. Some tend to disregard demographic data

altogether and trust the inferences instead – why keep track of a person's sexual orientation or marital status if it can be inferred from their behaviour, networks of friends or browsing habits? In 2002, Canadian Tire executive J.P. Martin came up with the idea to not only use past credit payment behaviour to predict whether a person was likely to pay their debt but also incorporate purchasing data in the predictive model. His analysis showed that people who bought felt pads for their furniture, carbon monoxide detectors for their home or branded motor oil were less likely to default on their loans (Duhigg, 2009).

A psychological study by Kosinski, Stillwell and Graepel (2013) demonstrated that Facebook likes could be used to accurately predict a range of personal attributes such as 'sexual orientation, ethnicity, religious and political views, personality traits, intelligence, happiness, use of addictive substances, parental separation, age, and gender'. Sensitive data is often not needed to make sensitive inferences (for a wide range of practical examples, see O'Neil, 2016). Facebook does not, for example, offer targeting based on race, religion, disability or sexual orientation (despite asking many of these things when signing up) but does offer 'multicultural affinity segments' for people whose activities on Facebook 'suggest they may be interested in content related to the African American, Asian American, or Hispanic American communities' (Facebook, 2018a, p. 2). Another trend in profiling is the use of sentiment analysis to infer affective states. One of the more prominent examples is Spotify's 'mood data' that it infers from its users' listening behaviours and preferences. Since 2016, Spotify has shared this data with the WPP's Data Alliance, which means that a broad range of advertisers have access to the data (WPP, 2016). Spotify users may themselves suggest moods, indicating that Spotify is partly informed by users' own, active choices.

From a commercial perspective, the main goal is to define and find the most attractive customers, usually in the top 20% (Turow, 2006, p. 95). Advertising networks argue that through extensive profiling, people will be shown the ads most relevant to their needs. The truth is a bit more sinister because the most valued customers are the ones that buy the most. Discrimination is not an unwanted by-product, it *is* the product. Gandy (2009) has demonstrated how the uses of data are often discriminatory by nature. He underlines how geographical data can be used as proxies for racial data and thus be used to discriminate against populations without explicit collection of ethnographic data (Gandy, 2009, p. 80). By combining census data and clustering models, U.S. ZIP codes could be turned into lifestyle clusters that could then be exploited in marketing systems. These geographic information systems (GIS) can of course be used for other purposes as well, such as for demonstrating how environmental hazards tend to be concentrated in areas

inhabited by minority groups or differences in access to healthy foods. One of the key points Gandy (2009, p. 81) makes is that automated decisions often have a racial effect without necessarily having a racist intent. Even though automatic systems are said to eliminate human prejudice, the ways in which data are collected and interpreted may produce equally strong biases. While the provider of an advertising platform may not have a racist intent, advertisers can use these platforms for racist purposes, such as when Facebook allowed discriminatory housing ads (Facebook, 2018a, p. 3). Even though this discrimination was not made based on race but based on 'multicultural affinity segments', the result is the same.

Popular writing on surveillance often presupposes that the information gathered is correct; in fact, it contains a significant amount of errors owing to the statistical error rates associated with making inferences. Although the collection of data is extensive, it does not always translate into accurate predictions (Pasquale 2015: 22). The statistical origins of how profiles are constructed mean that the accuracy of a profile is subject to a margin of error. Probabilities are never 1, and with datasets with millions of entries, even minor erroneous predictions may have devastating effects. For Haggerty and Ericson (2000: 632), profiles "transcend a purely representational idiom", and as such the accuracy of the profiles is secondary to their pragmatic value of "allowing institutions to make discriminations among populations." In other words, the profiles do not need to be a mirror of reality to serve their purpose as long as the error rate is within a tolerable range. In some cases, however, wrong predictions have devastating effects. Risks for false positives are also higher in some sectors than others. For example, finding evidence of money laundering and terrorism financing by looking at transactions is difficult because they differ little from legitimate transactions (Canhoto 2013: 98).

Although the data collection is extensive, it does not always translate into accurate predictions (Pasquale, 2015, p. 22). The statistical origins of how profiles are constructed mean that the accuracy of a profile is subject to a margin of error. Probabilities are never 1, and with datasets having millions of entries, even minor erroneous predictions may have devastating effects. For Haggerty and Ericson (2000, p. 632), profiles 'transcend a purely representational idiom' and as such, the accuracy of the profiles is secondary to their pragmatic value of 'allowing institutions to make discriminations among populations'. In other words, the profiles do not need to be a mirror of reality to serve their purpose as long as the error rate is within a tolerable range. In some cases, however, wrong predictions have devastating effects. Risks for false positives are also higher in some sectors than others. For example, finding evidence of money laundering and terrorism financing by

looking at transactions is difficult because they differ little from legitimate transactions (Canhoto, 2013, p. 98).

It is important to address one important conceptual distinction between the (post)panoptic diagram and the big data paradigm. They overlap to a high degree and it is often neither feasible nor necessary to distinguish between the two when the data concerned is personal information. However, there is one difference that I would like to underline at this point. While the origins of surveillance are also rooted in the regimes of disciplinary, bureaucratic control, the big data paradigm is less concerned with the psychological effects of being monitored. It is epistemically closer to the natural sciences than social psychology. Surveillance is naturally an important element of this type of societal optimisation, but the big data paradigm moves beyond managing populations and focuses on managing resources, human or otherwise. Therefore, it is important to also address how personal information may be regarded as a resource and, by extension, a commodity.

2.3 THE MARKET FOR PERSONAL INFORMATION

To understand why data protection policy cuts across sectors and societal actors, it is necessary to look at the structures that enable the transmission of personal data. Most major companies accumulate data on their users and customers to create consumer profiles and have been doing so for decades (Hildebrandt & Gutwirth, 2008; Christl, 2017, p. 13). While state surveillance has received most of the media attention, most surveillance is in fact corporate (Schneier, 2015, p. 47; Zuboff, 2018). As already touched upon in the previous section, data change hands at an accelerating pace. Retailers and creditors sell their customer records to data brokers. Data brokers sell personal data to customers who wish to verify credit history, target potential customers or even security agencies that want to identify security threats. Social networking sites use these profiles to match advertisers' content to potential customers, whereas online retailers use them to suggest new products to their customers. Banks and credit card companies track transactions to offer new services, detect fraud, and sell aggregated data to data brokers. Insurers gather data to make personalised risk assessments. Owing to the globalised nature of today's multinational corporations, data flows are increasingly international.

Nevertheless, it is worth noting that different countries offer different levels of protection of healthcare, financial, and credit data. In the EU, credit bureaus are usually subject to quite strict regulations and may in most countries not provide their services to others than creditors and for other

purposes than credit assessment, but there are a few exceptions (Ferretti, 2015, p. 16). In Sweden, Finland, the United Kingdom (UK), and Germany, credit bureaus may provide their services for other purposes and to others than creditors. But those sharing restrictions do not apply to customer lists that are shared within the same corporation. Gandy (1989, p. 73) proposes that this is the reason behind conglomerates seeking to provide banking and financial services, credit cards, travel, insurance, and consumer retail service records at the same time. This is already happening in some sectors, with especially airlines and retailers providing their own credit cards that are directly connected to their loyalty programmes.

The use of analytics systems has become especially ubiquitous in marketing. Automated, personalised behavioural marketing requires vast amounts of data that are fed into analytics systems that can sometimes provide counter-intuitive suggestions on how to proceed in a specific market. Central to the success of these systems is the collection of data from all possible sources. Thus, it is no coincidence that Facebook and Google together dominate the online advertising market and are increasing their share of worldwide advertising revenue year by year (Reuters, 2017). The two behemoths are sitting on the most advanced databases of human behaviour in the history of marketing – Facebook's data on social relationships and networks of two billion accounts and Google's near-monopoly search engine provide the two with extensive capabilities to infer people's interests.

A significant contribution of the critical political economy studies of communication is the so-called audience commodity thesis, famously introduced by Dallas Smythe (1977). The central contribution of Smythe's landmark paper was to focus on how audiences were being bought and sold, which had previously been a blind spot for political economists who tended to focus more on the production of media content. Smythe's subject of study was the television industry in the U.S. and the use of audience segments to sell advertising spots, but the underlying logic that Smythe identified applies to not only the media industry but the wider sale of personal data. The audience commodity thesis has subsequently been developed by scholars such as Fuchs (2012, 2013), Mosco (2009), Andrejevic (2002), Napoli (2010, 2016), Hesmondhalgh (2012), Jin and Feenberg (2015), Bolin (2012), Bermejo (2007), and Meehan (2002, 2005), to name a few. Common to most accounts would be a close connection to Marx's (1867/1984) commodity thesis as presented in *Capital*.

Some problems with applying the Marxist approach to personal information need to be addressed. First, as Gandy (2011, p. 442) notes, information does not require labour to be reproduced. By definition, data is

both non-rivalrous and virtually costless to reproduce, which means that its value is largely determined by the extent to which the proprietors of data can control (and monetise) access to the database. Thus, it is inherently related to how privacy rights are conceptualised, as we will see in the following chapter.

Second, the value of personal information does not reside in each variable but in adjunct with other information in the aggregate (Gandy, 2011, p. 444). This also explains why it would be difficult to create a system where people would sell access to their own personal data to the highest bidder. Third, the value of raw data is trivial compared with the value of that which is *inferred* from the data (cf. Athique, 2018, p. 64). These inferences are not the product of human labour but that of algorithms. While the initial setup requires labour and the systems might be tweaked over time, the inferences themselves are made by machines. As soon as the systems are in place, the cost of each acquired data point and each inference is miniscule (Gandy, 1989, p. 66), allowing established data brokers and online advertising giants to reap the benefits. Thus, the database is greater than the sum of its parts, and its creation is not the result of processes that can clearly be associated with some sort of labour.

Whether one sees audiences as the product of labour, product of consumption or dispossession is a broad theoretical discussion that is not the primary purpose of this study; the focus here lies in explaining how the big data paradigm relates to policy change. Regardless of how one conceptualises the audience, it is clear that personal information can be regarded as a commodity at least in aggregate form. Different industries tend to value different data points, as shown by Turow's (2006, p. 98) presentation of data broker Acxiom: the auto insurance package is sold with 33 elements, health care with 40, travel and entertainment with 36, and financial services industries with 12, to name a few. For the biggest U.S.-based data brokers, the three biggest sources of revenue are marketing, risk mitigation, and people search, corresponding to US$196 million, US$178 million, and US$53 million, respectively, in 2012 (Federal Trade Commission, 2014, p. 23). Facebook has partnered with several data brokers in the U.S., such as Epsilon, DLX, Experian, and Acxiom (Andreou et al., 2018, p. 5); however, owing to the massive critique surrounding the Cambridge Analytica scandal, it limited its partners' access to data. This, of course, does not stop Facebook from buying data sets to develop the company's own targeting portfolio. Google and Facebook have previously sought to incorporate all of their data within the same corporate structure, although Facebook wowed not to do so when it acquired WhatsApp. Now both Google and Facebook are trying to launch their payment services on a wider scale to further cement their targeting power. It

is not too unlikely that Google and Facebook will start providing credit ratings of their own.

For present purposes, it is not necessary to provide a detailed description of how audiences have been sold over time, but it is important to provide a brief overview of how the evolution of distribution technologies has changed the fundamental dynamics of the marketing industry (see Table 2.1). From a process-tracing perspective, the critical event that needs to be pinpointed is the moment where the commodification of audiences evolved into the commodification of individual audience profiles, thus triggering questions of data protection.

The history of audience commodities can be divided into three distinct eras that have each been decisively connected to how media products are distributed.[10] For newspapers, the product that was sold to advertisers was reach – the ability to reach certain groups of people, either the subscribers or the people who bought single copies (Turow, 1997, p. 22). The readership of the newspaper would be sold partly as an entity in terms of total reach (total circulation) and partly, as the advertisement industry evolved, as a way to reach certain demographics. With broadcasting, the dynamics changed. The key metric under broadcast television is exposure to content and thus advertising. The potential audiences were largely unknown until the rating industries evolved in the 1930s and started to keep track of audiences and the content they consumed (Napoli, 2010, p. 37). The first audience researchers largely distributed paper diaries to keep track of what people were consuming. While the use of targeted marketing goes back to before the 1950s, it was not until the late 1970s that targeted marketing was deployed on a wider scale (Turow, 1997, p. 19). In the 1970s, ratings companies handed out set-top meters to keep track of what audiences were watching (Napoli, 2010, p. 40). At this time, the focus shifted from households to individuals. The audiences for different television shows could then be packaged and sold as segments.

The first Internet ads in the mid-90s were so-called banner ads on websites, closely emulating newspaper ads in both their presentation and how they were sold. It is worth noting that Internet cookies were not addressed in the Data Protection Directive – when the Directive was drafted, cookies were not used for online advertising purposes.

[10] While it is worth noting that the evolution of audiences traces slightly different curves in Europe and the U.S., I will focus only on the starting points for paradigmatic shifts in marketing rather than detail their actual implementation worldwide. Many of the developments outlined below thus describe the U.S. context.

Table 2.1 A brief history of Internet ads.

1994: The first banner ads see the light of day
1995: Internet explorer accepts cookies by default
1996: DoubleClick is founded. Ad networks emerge
2000: Google starts selling keyword ads (Auletta, 2009, pp. 61-63)
2007: The rise of ad exchanges; DoubleClick is acquired by Google for $3.1 billion
2008: Facebook introduces 'Facebook Ads' analytics for advertisers
2009: Real-time bidding (RTB) is invented
2011: RTB becomes commonplace along with demand-side platforms

Napoli (2010, p. 88) stresses that new sources of data on media audiences challenge the traditional exposure metric. With the introduction of browser cookies, it was possible for ad-serving companies to start tracking users over time. This allowed for a new metric to materialise – that of *engagement*. Napoli (2010, p. 96) underlines that while the concept of engagement has become the 'dominant buzzword of the measurement industry', the actual definition of engagement is elusive and varies across contexts. Whereas some choose to define engagement according to a combination of exposure metrics, others tend to value appreciation and emotional responses, recall of brands and attitudes, or behavioural responses (Napoli, 2010, pp. 100-13).[11]

Nevertheless, central to the definition of engagement is that the behaviour of the target audience is recorded and analysed. Therefore, the promise of online advertising is not only that it offers detailed data on the interests of audiences but also that it is possible to track their actual behaviour post advertisement exposure. Thus, it is possible to disregard demographic data as proxies for possible future behaviour and look directly at purchases. This is also what drives the data broker industry – data on purchases are combined with records of advertisement exposure to 'onboard' offline behaviour to online marketing platforms (Napoli, 2010, p. 110, Christl, 2017).

Marketers gather a variety of demographic data, location data, activities, social networks, online behaviour, and offline purchases to target individuals (Turow, 2011, p. 89). Nevertheless, connecting advertising exposure or engagement to purchases is only part of the equation. It is equally important to use this data to create predictive models of user behaviour that can then be used to personalise both content and ads (see Pridmore & Zwick, 2011). Online behavioural advertising can be defined as 'the practice of monitoring people's

[11] While many of these definitions of engagement are used in market research, audiences are sold relative to exposure and behavioural metrics by referring to either impressions (CPM) or clicks (CTR).

online behaviour and using the collected information to show people individually targeted advertisements; (Boerman, Kruikemeier, & Borgesius, 2017). Access to profiles is sold programmatically in milliseconds without human involvement using real-time bidding. Personal data are sent with each programmatic bid, which occurs several hundred billion times per day (Ryan, 2019).

Because advertisers frequently employ several different databases and it is often difficult to know whether an advertiser uses exclusively online data, I choose to use the broader term *behavioural targeting*. Behavioural targeting entails three stages: the collection of data (tracking), the search for and inference of patterns (mining), and the association of the patterns with an individual (profiling) (Castelluccia, 2012). While the collection of data, data mergers, and inferences made are the foundational building blocks on which targeting relies, an important aspect of behavioural targeting is the ability to reach individuals. Drawing on the work of Turow (1997), Hildebrandt (2006), and Pasquale (2015), I define behavioural targeting as *the dissemination of content to select recipients based on the contextual information and inferred attributes and interests of those recipients and their proxies*.

To further elucidate this dynamic, I denominate access to audiences and control over behavioural databases *targeting power*. An important aspect that I have ignored until now is the centralisation of targeting power. In the early days of media advertising, targeting power was mainly divided between audience research companies, data brokers, and media outlets, with the two former providing data on the audience and the latter a way to reach those audiences. This division of power lied in the interest of media buyers who could rely on third party data which made it possible to compare the performance of the media outlets (Bermejo, 2009, p. 139). As pointed out elsewhere in this chapter, especially Google and Facebook have acquired dominant positions in the realm of online marketing. Their dominance lies in their unparalleled targeting power – the combination of access to audiences and control over behavioural data. The company that provides both access and behavioural analysis is one and the same. Media companies that provide the context for the ads are increasingly becoming replaceable middlemen – as long as it is possible to reach the same demographic, what difference does the publication make?

An important development that helps explain Google's current position was the rise of ad networks in the early 2000s to mid-2000s. Instead of media sites offering banner ads for sale directly to advertisers, the ad networks sell access to profiles and serve ads across different sites (Bermejo, 2007, p. 136; Webster, 2014, p. 71). DoubleClick, one of the largest ad networks at the time,

was acquired by Google for US$3.1 billion in 2007 despite the antitrust claims made by the online advertising industry and most notably by Microsoft (Teinowitz, 2007). Both the Federal Trade Commission (FTC) and the European Commission agreed to the acquisition. With DoubleClick, Google could move from selling keyword ads to using the detailed profiles that DoubleClick had crafted (Turow, 2011, p. 81). DoubleClick's profiles were based on tracking cookies placed on the sites that adhered to the ad network. Previously, the company had combined this data with a database on purchases that the company had obtained through its acquisition of the data firm Abacus but backed away from this practice after widespread critique (Turow, 2006, p. 82). Although DoubleClick eventually gave up onboarding, the practice is still commonplace and used by many marketers and data brokers.

The EU updated the ePrivacy Directive (2002/58/EC) in 2009 to reflect the changes in the online advertising economy. The updated ePrivacy Directive (2009/136/EC) entered into force in May 2011 and included a new rule requiring that online advertising should be based on consent. In practice, the consequence of this provision was that many websites added a pop-up claiming that by using this site you agree to our deployment of tracking cookies. The provision did little to stop online tracking and has largely been regarded as a dead letter owing to how the ePrivacy Directive was practically implemented.

The online advertising ecosystem has become increasingly complex since 2009.[12] Whereas early day tracking was based strictly on cookies and Internet Protocol (IP) addresses, single-sign on, device IDs and various device fingerprinting techniques are currently used to tie people to online behaviour across different devices (Narayanan & Reisman, 2017; Englehardt, Han, & Narayanan, 2018). Escaping surveillance is virtually impossible because even opting out from most tracking and refraining from using the services of Google and Facebook will not erase the tracks that emanate from other users and data

[12] Ad exchanges have also become increasingly sophisticated. Their predecessors, ad networks, lacked coordination and media buyers had to bid on many different networks at the same time. Ad exchanges were developed to gather the sale of access to publishers in one place. Websites (publishers) provide their advertisement slots via supply-side platforms to ad exchanges (such as DoubleClick, Microsoft Ad Exchange, or AppNexus), while advertisers can bid on access to profiles using demand-side platforms (such as the DoubleClick Bid Manager, Adobe Media Optimizer, or AppNexus). Advertisers (or more frequently, media agencies) define their target group, budget and track the performance of bought ads via the demand-side platform. Although there are a few different supply-side platforms, ad exchanges, and demand-side platforms, the biggest companies tend to offer both the marketplace for ads and the platforms for buying ads and keeping track of ad performance. Google has thus steadily been acquiring companies to be able to control the entire online advertising supply chain.

controllers. Facebook, for example, actively encourages advertisers to upload their own consumer databases to be able to target look-a-like audiences and previously bought databases on purchasing behaviour to hone their own database.

Whether the ineffectiveness of the ePrivacy Directive is attributable to the lack of meaningful sanctions or unclear definitions of what consent entails is a matter of debate. The shortcomings of the ePrivacy Directive and the Data Protection Directive would have a clear impact on the policy applications put forth by the Commission's draft General Data Protection Regulation. The need to update the laws demonstrates that the old principles in a pre-online surveillance era had not aged well. While the ePrivacy Directive managed to introduce compulsory cookie notices, it is doubtful whether these notices were effective in influencing corporate practice.

2.4 THE INFLUENCE OF PARADIGMS

At the beginning of this chapter, I have highlighted how paradigms and ideas shape political decision-making. Thus, the purpose of this chapter is to demonstrate how a big data paradigm has evolved, tracing its origins to three elements: that data on individuals and their performance generate greater efficiency and control, that social action can be accurately quantified and individual behaviour predicted, and that this enables a market for personal information. A significant part of this market is the online advertising ecosystem. This part of the market has come to be dominated by a few key players, most notably Google and Facebook.

Paradigms structure and constrain institutional change (Campbell, 2004, p. 108). Therefore, the regulatory initiatives that aim to limit the uses of personal data face powerful and influential discourses of surveillance as security and data as an important driver of economic progress and innovation. Moreover, strong economic forces resist and lobby against regulation on data use. However, this does not mean that the big data paradigm is completely uncontained because many of the developments presented above have also been met with resistance from the fundamental rights discourse.

As will be demonstrated in subsequent chapters, the GDPR was partly a response to the evolution of online behavioural advertising, which the previous Data Protection Directive and the ePrivacy Directive had failed to curtail – mainly because of unclear definitions but also because they lacked meaningful sanctions. It is consequently time to take a closer look at how

privacy relates to data protection and how data protection regulation is used to not only contain but also enable the big data paradigm.

3 THE PATH TO DATA PROTECTION

The previous chapter outlined how the big data paradigm has evolved and the economic incentives crucial for understanding exactly why the vast collection of personal information has become so central in bureaucratic societies. The big data paradigm is highly connected to the innovation discourse, and proponents of the big data paradigm often state that the regulation that limits data collection and processing also ultimately hinders innovation (Cohen, 2016). The relationship between the big data paradigm and regulation is complicated. On the one hand, regulation can be (and has been) used to intensify the surveillance capacity of states in particular. On the other hand, privacy regulation can and has limited commercial surveillant practices (Goldfarb & Tucker, 2010). All this indicates, quite naturally, that there are strong incentives for both public and private actors to influence legislators whenever data protection laws are being drafted.

The data protection policy domain is somewhat abnormal in the EU policy context because it cannot be easily connected to the media policy paradigms, information society initiatives, or competition policy. While the origins of data protection policy cannot be readily attributed to these three policy domains, data protection issues are moving from the periphery to the centre of each of them. The evolution of data protection policy and regulation can be traced back to national rights-based activism that frequently involved the intervention of legal professionals. According to Venturelli (2002), the EU's approach to privacy legislation is characterised both by the Member States' focus on public service regulation that, to some extent, prioritises citizen rights over contractual freedoms yet maintains a wide margin of appreciation for the solutions that can be seen as privacy infringing but somehow advance collective interests within the domains of welfare, law enforcement, and national security. It may be noted that a significant part of this chapter is devoted to demonstrating the differences between the EU and U.S. approaches to information privacy. This comparative approach is motivated by the importance of showing how ideas motivate policies (Schmidt, 2008). U.S.-based companies participated in the GDPR's legislative process to a very high degree, as will be demonstrated in chapter six; therefore, it is important to be aware of the regulatory background that has, at least on some level, ideationally guided their submissions and lobbying activities in the policy process. Moreover, the originators of European data protection legislation were also inspired by U.S. scholarship on information privacy (Simitis 2010).

The GDPR is largely based on its predecessor, the Data Protection Directive (95/46/EC), which was in many respects a more radical regulatory intervention than its successor. According to Peters (2012, p. 76), one of the most decisive questions for historical institutionalist research is defining the moment of creation. In the case of the GDPR, does one start with the Data Protection Directive, the first regional data protection law in the state of Hesse in Germany, the UN Declaration of Human Rights of 1948, or even earlier? While it is possible to argue for each of these starting points, I will focus on the events leading up to the Data Protection Directive but also provide an overview of the history of privacy legislation. Drawing on new institutionalism and Mahoney's definition of path dependence[13] (2000, p. 509), I consider the GDPR's legislative process as a sequence that can be traced back to the events that unfolded in Europe in the 1970s and 1980s. Following Pierson (2000), the objects of study are the 'critical junctures' that set political institutions on a specific path. Crucially, early events are considered more important than later events, but this does not preclude that different mechanisms of change can provide a deviation from the path (Mahoney, 2000, p. 517; Pierson, 2000, p. 263). These mechanisms of change can be associated with changing political or economic realities, the introduction of new technology, or the Importantly, the mechanisms of change can constitute the policy windows that open for the possibility of enacting new policies (Kingdon, 2013, p. 166; Zahariadis, 2008). In Kingdon's multiple streams approach, political issues are significantly more likely to draw the attention of decision-makers if three streams are coupled: problems, policies, and politics. At any given time, there are a number of solutions and ideas available: in Kingdon's terminology, a 'primeval soup' of ideas. However, their realisation is dependent on not only whether the policies may be seen as acceptable or feasible in the policy community but also if the time is right. Policy windows open because of changes in the political stream (such as a change of administration or shift in national mood) or because a new problem captures the attention of decision-makers (Kingdon, 2013, p. 168). According to Kingdon, policy windows 'present themselves and stay open for only short periods'. When the window is open, policy entrepreneurs can push for and introduce specific policies. Kingdon's model is based on the political process in the U.S., and it excludes actual decision-making and focuses on the agenda-setting stage (Zahariadis, 1995, p. 33).

However, in Zahariadis view (1995, p. 34), it can be revised to also include the decision-making stage to explain why certain policies are not only set on

[13] For more comprehensive lists of the studies that have used path dependence as an analytical approach, see Greener (2005) and Bennett and Elman (2006).

the agenda but also ultimately chosen. Furthermore, Zahariadis is critical of the notion of 'public mood' because it is difficult to pinpoint and instead chooses to interpret the political stream as 'the ideology and strategy of governing parties'. In the EU context, Zahariadis (2008, p. 518) sees the politics stream as 'the balance of Council member national and partisan affiliation, the ideological balance of parties in Parliament, and the European mood', seemingly forgetting his initial critique of the vagueness of a concept such as national mood. Noting the difficulties in defining a national mood, let alone a European mood, I choose to define the European mood not as an existing public discourse but rather as a discourse that is perceived as dominant among decision-makers.

The policy windows approach explains why issues are reframed and why change happens. Nevertheless, there are other factors in place that also explain policy equilibrium and more incremental change. Drawing on the economic theory by Arthur (1994) and North (1990), Pierson (2000) proposes that policies are resistant to change owing to the increasing returns processes, where positive feedback loops lead to equilibrium. Therefore, changes to current policies may be resisted by the legislators, those subject to the new policies, and those enforcing them. While acknowledging that this may be the case in the early stages of path-dependent systems, Greener (2005, p. 69) nevertheless argues that Pierson's static approach to change simply does not hold owing to the pressure applied from both endogenous and exogenous forces for change. Thelen (2009, p. 475) points out that sometimes significant change can take place not only by an abrupt exogenous shock but also 'through a cumulation of seemingly small adjustments'. Peters, Pierre, and King (2005) also highlight that historical institutionalism approaches are ill-adapted to handling the political conflict which occurs not only in the formative moments of a policy but also at later, path-dependent stages.

In the case of information privacy, notable events include the computerisation of databases in the 1950s, industry sharing of personal data in Europe in the 1970s, subsequent regulatory initiatives in Europe, evolution of ad-tracking technology from the early 2000s onwards, proliferation of social networking sites from 2006 onwards, NSA leaks of 2013, and Facebook/Cambridge Analytica scandal of 2018. Few of these events would constitute policy windows in a strict sense owing to their prolonged nature but were in many cases strategically used by policy entrepreneurs to put forth information privacy regulation in the EU. The Data Protection Directive was, for example, not a result of a window of opportunity occurring, but it was a product of national authorities forcibly prying a window open. There are similar examples of policy entrepreneurs creating windows of opportunity in

education (Corbett, 2005) and telecommunications (Cram, 1997), although the extortive nature of the data protection authorities' (DPAs') actions was quite extraordinary.[14] Before turning to the evolution of data protection policy, I will present an overview of the history of the right to privacy.

3.1 THE RIGHT TO PRIVACY AND ITS ORIGINS

The history of privacy legislation is concomitant with the development of media and communication technologies. Newspapers, pocket cameras, covert listening devices, video cameras, and social networking sites have changed how people relate to the private sphere, blurred the distinction between what is private and what is public, and at times, created an urgent need for more legislation (Tene & Polonetsky, 2013).

While the criminalisation of libel and slander can be traced back to the code of Hammurabi, it can be argued that the foundations of privacy as a fundamental right originate from the U.S. Bill of Rights from 1791 and the French Constitution of the same year, both heavily influenced by the Enlightenment philosophy.

Although the ten Amendments to the U.S. Constitution do not explicitly mention privacy, the Fourth Amendment expresses the following:

> *The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.*

Reflective of the U.S. Constitution, the Fourth Amendment provides protection of the individual from the interference of the state – it is, in other words, a negative right.

[14] DPAs are independent regulatory bodies focused on enforcing data protection regulation. Their powers are mainly investigatory, but the GDPR has granted supervisory authorities the power to issue sanctions, which was previously possible on a national level but not explicitly recognised in the Data Protection Directive. Sometimes the DPAs are called Information Commissioners, and sometimes they are part of other regulators. For reasons of clarity, the term 'data protection authority' will be used consistently in this study.

The French Constitution established protections for freedom of the press, but those freedoms were also restricted in Article 17, which extends protections against insults relative to the '*vie privée*' (cf. Whitman, 2004, p. 1172).[15] In Europe, the development of the right to privacy through later court practice and statutory law was mostly related to dignity (Whitman, 2004, p. 1174). According to Simitis (2010: 1993), this is a rather blunt assessment, and in his view, privacy was grounded in both dignity and liberty in Europe. While accounts may differ on this particular aspect of the origins of privacy legislation, present day privacy regulation in Europe can at least be traced to both notions.

The rise of new technology as well as journalistic institutions has had a profound impact on privacy legislation. The press' use of photographs extended the honour of private life to a right to one's image in France in the mid- to late 19th century (Whitman, 2004, p. 1176). Similarly, in the U.S., the early privacy laws were torts that permitted individuals to seek compensation if the media had violated their privacy (Ohm, 2010, p. 1733).

Inspired by continental legal developments, Warren and Brandeis (1890, p. 206) defined privacy as a right which 'protect[s] the privacy of the individual from invasion either by the too enterprising press, the photographer, or the possessor of any other modern device for rewording or reproducing scenes or sounds'. Thus, this definition of privacy was closely related to capturing a moment and making that moment available in the public sphere. Warren and Brandeis' significant contribution was that they suggested that the right to privacy must be separated from libel and slander and be construed as the broader right to be let alone. While clearly inspired by the European notion of reputation, the right to be let alone was slightly broader. Reputation protects individuals from false and hurtful information, while the broader right to privacy contains also factually correct information that is not harmful (Neuvonen, 2014, p. 13). Warren and Brandeis' suggestion did not result in new privacy laws as such, but their article influenced practice in the U.S., effectually carving out a new right to privacy.

It was not until after the Second World War that the right to privacy evolved to its present form. Most constitutions base their wording of the right to privacy on Article 12 of the UN Declaration of Human Rights from 1948, which was inspired by the French and U.S. approaches to privacy. The article combines both elements of privacy: the integrity of a person and their communications as well as dignity.

---

[15] Chapter V, Article 17, third paragraph: 'Les calomnies et injures contre quelques personnes que ce soit relatives aux actions de leur vie privée, seront punies sur leur poursuite'.

> *No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.*

While the Declaration is an important landmark for the evolution of human rights, it does not bind nations other than morally. It has, nonetheless, been the inspiration to both international treaties and national laws on privacy. These laws often provide a more extensive list of exceptions than the original declaration. While privacy rights are recognised in national law, there are clearly many other issues of public interest that mandate exceptions to those very rights. Fundamentally, the human rights law rests on the idea of 'contextual balancing', where it is possible to invoke a counter-right for every right, and each right is accompanied by exceptions (Koskenniemi, 2004, p. 208). For privacy, the counter-rights most frequently invoked are either security or freedom of expression. Moreover, civic freedoms and rights have always been partially relinquished in exchange for security and access to valuable infrastructure in the modern bureaucratic state (Giddens, 1985).

Privacy laws as such do not make room for business interests as a permissible exception, as Article 4(1) of the International Covenant on Civil and Political Rights clearly states that derogations are necessary only '[i]n time of public emergency which threatens the life of the nation and the existence of which is officially proclaimed'. However, the European Convention of Human Rights (ECHR), ratified by all EU member states, does contain a reference to the macroeconomics of a state in Article 8(2):

> *There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*

The exceptions in the ECHR outline some of the collective interests that can be invoked to limit the right to privacy. This is usually the case when law enforcement is involved, for example, when police are granted permission to use wiretaps to prevent crime. In these cases, there can be a direct, foreseeable outcome – the surveillance activity is directly connected to the crime being committed. In other areas, the outcome may be less predictable, such as in the area of mass surveillance. Similar uses of mass processing of personal data could be applied to infer public health risks. This requires that highly sensitive medical records are shared between as many research institutions as possible,

but the collective gains from sharing medical information might surpass individuals' privacy claims.

Whether one accepts these measures is usually dependent on whether the end goal is regarded as achievable and proportional in relation to the limits it imposes on the right to privacy. The characteristics of the EU's information society policy include the 'persistence of the European social model and political tradition of public service regulation as reflected in higher levels of protection for individual citizens in cyberspace' and a legal tradition that privileges public interest over proprietary rights and contractual freedoms (Venturelli, 2002, p. 80). However, this public interest may also correspond with significant exceptions to privacy rights in matters of national security and law enforcement. This is a significant difference vis-à-vis the U.S., where privacy rights have been used to limit the powers of the federal government rather than private actors, whereas the EU has favoured the opposite approach.

It important to stress that the derogations to the right to privacy are connected to the interest of the nation, which is usually equated with public interest. Industry requests to limit the right to privacy that fail to become universally regarded as the public interest are not compatible with the right to privacy. However, if a corporation's wish to limit the right to privacy can be argued to serve the public interest, derogations could be justifiable. Therefore, corporations choose to participate in policy processes. Corporations wish to define their activities as within the public interest rather than as a single business' private interest. It is no coincidence that many position papers start by expressing the size of the industry in which they operate.

As its history demonstrates, the right to privacy has not remained static over time. The different aspects of privacy can be defined as conceptual subdomains of the right to privacy. These include the physical integrity of a person, the integrity of personal communications, the integrity of one's home, information privacy, and the right to one's reputation. Therefore, each subdomain will be subjected to a different set of exceptions that are legitimised in different ways. As the focus here is on information privacy, I will not address the other subdomains – importantly, I will not address the question of reputation because data protection policy does not directly discuss the reputational damage information disclosures cause – although it is implied.

Conceptually, I consider data protection a policy instrument used to enable information privacy. In this dissertation, data protection is defined as the operationalisation of information privacy which is itself a subdomain of the right to privacy. The two are not to be seen as synonymous, and especially in the European context, data protection is considered separate from privacy.

Instead, I argue that data protection operates on a lower, operational level than privacy and information privacy, which are more conceptual in nature.

The boundaries of information privacy have always been difficult to pinpoint owing to technological change and people's different perceptions of what privacy entails (see Nissenbaum, 2011; Cohen, 2012; Papacharissi, 2010, p. 46). For example, citizens from the different EU member states value different information quite contrarily; whereas most EU citizens regard financial information as personal data, most Polish and Romanian citizens disagree (European Commission, 2011b, p. 13). Earlier research has also shown that German citizens are concerned with surveillance and telecommunications data retention (Bug, 2013). These changes in attitudes make EU regulation especially difficult because normative ideas of privacy differ quite substantially.

In the EU, the particular challenge of what people regard as private has been circumvented by abstaining from limiting the definition of personal data to certain categories of data, but whether data can be reasonably linked to an individual. Therefore, the question of whether something is regarded as *personal* is irrelevant. However, as techniques of re-identification are refined, this may lead to a situation where all data becomes personal, 'like an ideal gas to fit the shape of its container' (Ohm, 2010, p. 1741). Nevertheless, in the EU, it is believed that refraining from limiting the scope of the law awards the greatest protection of information privacy. This solution has been called the 'omnibus' or 'principle-based' approach to personal data. In the U.S., both academics and policy-makers argue that an all-encompassing definition is too vague to be efficiently enforced. They favour the 'sectoral approach', where different standards of protection are granted to different types of data (see Nissenbaum, 2010; Ohm, 2010; Schwartz, 2013). The separation between the two approaches is less clear-cut in practice, because European lawmakers use the omnibus approach for defining general principles, but specific legislation to regulate uses of data in different domains (Simitis 2010). The European approach has nevertheless been more influential globally, as many other countries have opted for the omnibus approach to data protection (Bennett & Raab, 1997, p. 244; Schwartz, 2013; Newman, 2008a, p. 104; Bradford, 2012; Fischer-Hübner, 1998).

The costs and benefits of the collection, processing, and trade of personal information come at potential benefits for businesses and costs to individuals, which would argue for an interpretation of privacy law that prioritises the individual (Nissenbaum, 2010, p. 111). In information privacy law, this balance is no longer as clearly tilted in favour of citizens. Information privacy is fundamentally different from the negative right to privacy that requires the

state to refrain from being intrusive. Data protection is a positive right, which happens to recognise practices that both protect the rights of individuals and limit those same rights at the same time. As noted at the beginning of this chapter, human rights law is fundamentally based on conflicts of rights (Koskenniemi, 2004), such as whether one should give precedence to the freedom of expression or the right to privacy. The abnormal trait of data protection is that it seeks to advance two opposing goals at the same time: to secure the free movement of data and protect the privacy of individuals. Schwartz (2013, p. 1971) argues that the international debate on information privacy has always been about both human rights and data trade. However, data trade does not advance the right to privacy, which generates an inherent tension in information privacy law.

To understand the origins of this purpose paradox, it is worth revisiting the origins of data protection regulation. When national legislators set to create the first data protection rules in Europe in the 1970s, public authorities were already processing personal data and analysing it with the help of computers. When databases were digitised, they also became easier to transfer, which shifted the focus of privacy law from control over publication to control over data flows. Activists and legal professionals were concerned that state-run computerised databases on citizens could be abused and required that safeguards be instated. The first countries to introduce data protection legislation in the 1970s were Sweden, Denmark, Norway, Germany, Austria, France, and the UK (Schwartz, 2013; Newman, 2008b). In other words, data protection regulation was, as with previous privacy laws, a reaction to technological change. Furthermore, owing to the perceived benefits of computerising the databases of personal information, it would be unrealistic to outlaw the practice simply because of the privacy risks their use might entail.

The first global document on data protection was the Organization for Economic Co-operation and Development (OECD) (1980) guidelines on the protection of privacy and transborder flows of personal data, which can be regarded as the common baseline for all data protection regulation. . The first legally binding international instrument on data protection, Convention 108, opened for signature a few months later in 1981. Five states had ratified the Convention by 1985, and 51 states have currently acceded (Council of Europe, 2018). Whereas the OECD principles were more focused on establishing a common, general framework for what could be described as decent data processing, the Convention introduced some more detailed provisions. However, because the Convention is an international treaty, it produces no direct effects for citizens – a breach under the Convention is therefore

meaningless if national law does not recognise it. Under the Convention, it is also possible to come up with a wide range of exceptions as long as those are explicitly stated in the law.

The global data flows raised significant concerns among privacy advocates. DPAs in European countries with stringent data protection laws were concerned that multinational corporations were relocating their data processing activities to Belgium and Spain, which lacked data protection laws altogether – although both were signatories of Convention 108. The concern of these DPAs would ultimately trigger data protection reform at the community level.

3.2 THE PURPOSE PARADOX

Research on the politics surrounding the inception of the Data Protection Directive conducted by Simitis [16] (1995), Bennett and Raab (1997), and Newman (2008a, 2008b) has revealed three important features of the Directive's legislative process. First, it was initially the Parliament that from 1979 onwards was concerned with questions of data protection, while the Commission was reluctant to initiate legislation for a decade (Simitis, 1995, p. 446). Second, lobbyists from data-intensive industries, such as the European Banking Federation (EBF) and the European Direct Marketing Association, were significantly involved in lobbying the first 1990 draft and were eventually successful in introducing the reference to the 'free movement of such data' in the title of the second draft in 1992 (Bennett & Raab, 1997, p. 248). These lobbying groups were also financially supported by American business groups. Third, the newly instated national data privacy authorities acted as transgovernmental policy entrepreneurs and pressured their governments for supranational regulatory intervention (Newman, 2008b, p. 76).

The third feature of the legislative process is worth dwelling on. Newman (2008b, p. 77) highlights that national interests were decidedly against introducing supranational legislation. Both business elites and the governments of the biggest economies in Europe did not promote the harmonisation of data protection legislation. The Commission was equally uninterested in advancing this agenda and supported national regulation. The Commission's switch from resistance to promotion was not marked by changes in national attitudes but by the increased lobbying and even threats by the national DPAs. In the 1980s, the national DPAs were concerned with

[16] Simitis authored the world's first data protection regulation in the German state of Hesse in 1970. He served as the state's data protection commissioner from 1975 to 1991.

the lack of regulatory oversight in Belgium, Greece, Spain, Portugal, and Italy. If no common rules on data protection were introduced, the DPAs would block data flows to countries lacking legislation (Newman, 2008b, p. 89). In 1989, the French DPA *Commission nationale de l'informatique et des libertés* (CNIL) blocked the transfer of personal information on French citizens between Fiat's French and Italian corporate offices, forcing Fiat to sign a contract stating that Fiat Italy would handle French personal data under the French data protection regulation rules. The contract can be seen as a precursor of the current regime of binding corporate rules (BCRs). The French and German DPAs also managed to stall the Schengen agreement until Belgium had pledged to introduce appropriate legislation.

Owing to these developments, the Commission finally changed its position on harmonising data protection regulation, and the Directorate-General[17] for the Information Society and Media (DG INFSO) drafted a proposal that was presented in 1990. The wording of the first draft was heavily influenced by the national DPAs. The Commission's drafting committee comprised Commission officials and national DPA representatives (Newman, 2008b, p. 92). The private sector was largely left out of the drafting procedure but engaged in heavy lobbying after the draft was published. European business groups also lobbied strongly for subsidiarity and the preference of national legislation, supported by the governments of Denmark, Ireland, the UK, and the Netherlands. The national DPAs countered these initiatives by proposing that the Directive should require member states to set up supervisory authorities and that their transborder network would be formally recognised in the Directive as the *Article 29 Working Party*,[18] thus guaranteeing subsidiarity. The Article 29 Working Party (WP29) was advisory, but its interpretation of data protection legislation has been and is still highly influential within the field. Its papers have been frequently cited by European courts, and its interpretations of data protection law are quite authoritative. Nevertheless, the WP29 was strictly speaking an information network with no enforcement powers. Following Slaughter (2005, p. 169), the WP29 can be seen as a combination of hard and soft power: while the Working Party itself had no enforcement power, its members do in their national contexts. Furthermore, the representatives of the DPAs used their formal expertise in the negotiations, often sitting alongside their national governments while amendments to the

[17] The Commission is divided into specialised DGs that employ administrators with expertise in different sectors.

[18] The Article 29 Working Party was made up of national DPA representatives, a representative of the EU Commission and the EDPS.

Directive were being proposed. The German federal data privacy commissioner even represented the German presidency during the negotiations (Newman, 2008b, p. 93).

A common position was eventually agreed upon in 1995, although the UK abstained. Simitis (1995, pp. 450-451) notes that the Data Protection Directive is in many respects a combination of different legal traditions, with some principles corresponding to German data protection laws (purpose limitation), others British and Dutch (codes of conduct), and others French, Belgian, Spanish, and Portuguese law (prohibition against processing sensitive data). According to Simitis (1995, p. 449), the will to introduce parts of national legislation into the harmonised Directive was not a valuable aid but 'a serious handicap'. The primary aim of the Council appears to have been to introduce familiar rules instead of establishing a high level of protection. Simitis rightly predicted that the member states' initiative to transpose the Directive to national legislation would be more dependent on to what extent the rules in the Directive corresponded to national legislation.

Simitis (1995) is also more critical of the end-result than Newman (2008b) – possibly because Simitis, a former data protection commissioner, saw how the member states introduced exceptions to the Commission's draft that had been largely co-authored by the DPAs. Simitis (1995, p. 457) was especially concerned with the expanded research exception to the so-called finality principle, according to which data should not be further processed for other purposes, which in the Directive's wording would allow anyone to bypass the finality principle as long as they had a research department. Simitis (1995, p. 461) also demonstrates how the representatives of national governments acted in their own interest when they pushed for the right for political parties to collect data for acquiring new members or for fund-raising purposes without obtaining consent and without specifying any specific safeguards.

The legislative process of the Data Protection Directive corresponds to Slaughter's (2005) depiction of how national regulators have become the new diplomats, engaging in transnational networks. These networks have also become more prominent over time, extending beyond the EU (Raab, 2010). Slaughter (2005, p. 159), drawing on Dehousse's (1997) work on European information agencies, argues that the EU's approach has 'given rise to the need for a central node' in transgovernmental networks. In the case of data protection policy, the WP29 became that node. The review by Simitis (1995) shows how while the national DPAs managed to set the agenda and influence the initial draft, the Council introduced a range of exceptions deemed unsatisfactory by the network of regulators. Newman's (2008b) description of the legislative process also demonstrates that the private sector was largely

excluded from the negotiations and had to focus its lobbying activities especially on the national governments. These peculiarities of the data protection policy domain need to be taken into account when addressing the GDPR's legislative process.

In the years after the inception of the Data Protection Directive, data protection has even evolved into a right of its own in Europe, separate from the right to privacy. Article 8 of the Charter of Fundamental Rights of the European Union, which was ratified in 2000, states the following:

> *1. Everyone has the right to the protection of personal data concerning him or her*
>
> *2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.*

Data protection was also explicitly mentioned in the Treaty of Lisbon which was signed in 2007 and entered into force in 2009. Article 16 states that 'everyone has the right to the protection of personal data concerning them'.

Laurer and Seidl (*forthcoming*) attribute both of these developments to the WP29's efforts. In 1999, the WP29 chairman at the time, Stefano Rodotà, was appointed member of the drafting convention of the Charter. In an annual report cited by Laurer and Seidl, the WP29 'explicitly prides itself on having made a "major contribution" to anchor data protection in the charter'. The Charter would later influence the ultimately rejected Constitution for Europe which included a general article on the protection of personal data. That same article would later surface in slightly redacted form as Article 16 Treaty on the Functioning of the European Union (TFEU) in the Lisbon Treaty.[19]

When the Data Protection Directive was being drafted, the primary concern was the transfers that took place in the EU. However, it would not take long until the Internet would lead to large quantities of personal data being transferred to the U.S. and other so-called third countries. The problem with these transfers was that the EU did not formally regard U.S. data protection regulation as 'adequate', which was a prerequisite for transferring personal data to a third country unhindered (Schwartz, 2013, p. 1980). The EU's focus

[19] The introduction of this new right (or even rights) has caused some confusion as to the status of data protection (González Fuster & Gutwith 2013). Kokott and Sobotta (2013) have concluded that in the jurisprudence of the European Court of Human Rights and the Court of Justice of the European Union, there are some differences regarding the scope of the rights and their limitation.

on process and subject rights was not formally compatible with how information privacy was operationalised in the U.S. Stopping data transfers completely would still not be an alternative. Because U.S. privacy law would never be adequate by European standards owing to lack of political initiative within the privacy domain, a political solution was needed (cf. Farrell & Newman, 2019). Companies with EU subsidiaries could rely on a contractual solution for intra-group transfers, so-called BCRs[20], which extend data rights to processing taking place in a foreign jurisdiction. However, this alternative would not be available for external transfers.

To avoid disturbing trade relations, a special agreement between the EU and the U.S. was negotiated. The so-called Safe Harbor agreement comprised seven principles that U.S. corporations could adhere to in order to show that they respected the EU's data protection legislation (European Commission, 2000). The principles corresponded to the rules outlined in the Data Protection Directive but with a lot less detail and a lower level of protection more in line with the U.S. approach to information privacy. Significantly, the Safe Harbor agreement added procedural safeguards that did not exist in the U.S. The FTC was partly responsible for overseeing that the principles were followed. The enforcement of these principles was highly criticised in several reviews of the agreement, and reports highlighted both lack of compliance as well as a disappointingly low number of adherents to the agreement as key issues (Connolly & Van Dijk, 2016).

The Safe Harbor regime was demonstrably not very successful, and the personal data transferred to the U.S. were clearly not adequately protected. The ineffective agreement partly encouraged the Directorate-General for Justice (DG Justice) to draft the GDPR in the first place. The question had become more pertinent as non-EU actors were able to offer services to European citizens without any physical presence in the Union. Evidently, U.S. dominance in the ICT sector was a contributing factor: Google dominates the search market; Cisco has the largest market share of all switch vendors; Google, Amazon, IBM, Microsoft, EMC, and Dropbox provide the majority of

[20] BCRs can be employed by businesses that make intra-group transfers of data to countries outside of the European Economic Area (Article 29 Working Party, 2008; European Commission, 2012a, Article 43). Once a data protection authority approves the BCR, the company no longer needs to sign a new contract every time a transfer is made within the group. The validity of BCRs is dependent on formal approval by the national data protection authorities. The rules are used to make sure that the EU data protection legislation is respected regardless of where the company processes data. The Article 29 Working Party (2003) recognised BCRs in a Working Document from 2003, but they had previously been applied in national contexts. The BCRs are formally recognised in the new GDPR.

all cloud storage services for both consumers and enterprises; Amazon provides the infrastructure for a large part of the Internet; Facebook and Google dominate the online advertising market; and nearly all phones run either Apple's IOS or Google's Android. The duopoly of smartphone operating systems provided both Apple and Google detailed access to people's data and enabled this information to be transmitted to the developers of third-party apps. [21] Therefore, data on European citizens were constantly being transferred to the U.S., and any new laws that would either increase the liability of American companies or extend the reach of EU law were going to be prone to lobbying.

3.3 INFORMATIONAL SELF-DETERMINATION OR BUREAUCRATIC PROCEDURALISM

To assess the extent to which the GDPR is path-dependent of previous data protection policy, it is worth mulling over how data protection should be operationalised. In the EU's data protection policy, two of the most defining operational principles relate to whether information privacy should be achieved through bureaucratic procedures or by informational self-determination. The purpose here is not to provide a detailed evaluation of applications associated with these two operational principles but to provide a broader framework for understanding data protection legislation and the rationale behind including provisions that either serve informational self-determination or are more procedural in nature. These two operational principles can be connected to the French and German approaches to information privacy (cf. Whitman, 2004; Simitis, 1995).

Conceptually, many theoretical accounts are focused on the managerial aspects of privacy. A common characteristic found in surveys on people's attitudes to privacy is that they tend to circulate around questions of control and access. This is usually how information privacy is conceptualised in legal theory and policy research (Nissenbaum, 2010, p. 70). Some legal scholars, such as Westin (1967, p. 158), prefer to see privacy as the control one has of information about oneself. The data subject presides over their personal information and submits pieces of it to the public domain, organisations, or other people. Access, on the other hand, can be defined as 'the condition under which other people are deprived of access to either some information about you or some experience of you' (Reiman, 1976, p. 30). Access is partly decided by the data subject themself and partly by the rest of the society. In other

[21] Apple's App Store and Google's Android Market both opened in 2008.

words, information privacy is construed negatively as the possibility to withhold some information about oneself despite not being in full control. Thus, part of the body of personal information may be obscured by the subject, while some access to personal information is restrained by societal norms.

The managerial approach to data protection has been highly influential in Europe (Koops, 2014), resulting in a range of rights pertaining to how data is processed. Privacy activists frequently elevate the autonomy and self-determination of individuals when they advocate for stronger privacy rules – consent is often seen as the highest possible standard. Especially in the U.S., where the liberal market position has been dominant, consent has been seen as the best way to preserve privacy rights despite obvious shortcomings and power imbalances (Hoofnagle, 2018, p. 162). In the U.S. tradition, the freedom to agree to terms and conditions is unrestricted, regardless of how detrimental they might be to the privacy rights of the user himself/herself. Thus, consent has been an effective tool for U.S. companies to continue with their wide-reaching data processing activities. Companies employ highly complex end-user license agreements (EULAs) that outline all the possible ways companies may use data that have to be accepted prior to using software of one kind or the other. Europeans have to some extent adapted to the U.S. consent regime because most popular IT services are of North American origin. However, in Europe, consent alone has not sufficed. One of the key differences between the EU and the U.S. is that European data protection law has put greater emphasis on user rights as expressed by notice, access and correction rights (Schwartz, 2013, p. 1976). The U.S. model is frequently referred to as 'notice and consent', whereas European informational self-determination requires an additional set of rights that grant additional control to citizens.

In Europe, the managerial approach has resulted in a number of data rights, such as the need to consent to personal data processing (unless it falls under one of the exceptions), the right to be forgotten (or erasure), the right to rectification, and the right to object to processing. Common to these applications of informational self-determination is the idea that the individual should possess some degree of autonomy regarding information that concerns them. They are more closely connected to the notion of control, but the scope of this autonomy is heavily restricted by a number of exceptions. Sometimes the control is limited to being aware of how data is being processing – transparency – which can be either construed as a data subject right or as a data processor obligation. Transparency sets out principles for how the data should be processed and how this should be communicated. Data subjects should be aware of how and for what purposes their data is used. A recent study demonstrated that ad transparency undermines the effectiveness of ads

when marketing practices violate people's beliefs of what the information flows look like (Kim, Barasz, & John, 2019). Some level of transparency may thus trigger people's awareness of their privacy rights. However, the transparency of ad practices might not be all that forthcoming. A study of Facebook's ad transparency tools showed that the information Facebook provides on why people are targeted is often incomplete and sometimes misleading, while data explanations are often incomplete and vague (Andreou et al., 2018).[22]

Despite the operational approach being dominant in the U.S. and an important aspect of the data protection regime in Europe, many academics are critical of its presumed efficiency. Obar (2015, p. 5) calls it the 'fallacy of data privacy self-management'. Koops (2014, p. 252) argues that informational self-determination is deeply flawed and that consent is 'not a suitable approach to legitimate data processing'. Furthermore, he highlights that data subject rights remain theoretical because it is nigh impossible for a layman to use them efficiently. This can be connected to Gandy's (1993, p. 9, 43) view that individuals are generally 'contract term takers' in transactions that require personal information. The problem is that there is scant evidence of people seizing control over their data. Numerous studies in both Europe and the U.S. show that people are increasingly worried about their online privacy, yet they refrain from taking action that would secure their privacy in practice (Pew Research Center, 2015a, 2015b, 2016; European Commission, 2015a; Turow, 2003; Debatin, Lovejoy, Horn, & Hughes, 2009; Halbert & Larsson, 2015; Kennedy, Elgesem, & Miguel, 2015). This has been termed the *privacy paradox* (Utz & Krämer, 2009).

The privacy paradox is reinforced by another paradox, the *transparency paradox*, according to which detailed privacy policies are less likely to be understood if they state all the possible conditions for the use of personal data (Nissenbaum, 2011, p. 36). It is becoming increasingly difficult for regular users to understand how companies (and to some extent public authorities) process data. This challenge is likely to intensify during the coming decades,

[22] The problem is that Facebook's explanations show the attributes that match the most users, which is usually reduced to demographic data, even though the targeting is clearly based on behavioural data. In fact, when different types of targeting are employed, Facebook uses the following order to provide an explanation for the targeting: demographic > inferred interests > advertiser-provided database > behaviour on and off Facebook (Andreou et al., 2018, p. 10). The attributes that Facebook has acquired from its data broker partners Acxiom, DLX, Experian and Epsilon are, however, deliberatively never disclosed to users (Andreou et al., 2018, p. 13).

when an increasing amount of home appliances and devices are connected to the cloud.

Legislators have not been oblivious to this aspect of privacy, and a significant aspect of EU data protection law is that data controllers[23] are subject to data processing obligations (Koops, 2014, p. 253). These obligations apply irrespective of what individuals have consented to. I call it *bureaucratic proceduralism* owing to its focus on logging events, providing documentation, and following specific regulatory guidelines. For data controllers, the procedural approach is in many respects more cumbersome than respecting informational self-determination. Informational self-determination needs to be triggered by the data subjects themselves, whereas bureaucratic proceduralism requires controllers to take necessary steps to comply with the law. Whereas the former constitutes an ex post regime, the latter is an ex ante regime. The two approaches are concerned with transparency, although transparency serves different purposes under informational self-determination and bureaucratic proceduralism. In the former regime, transparency is used to provide necessary background information so that data subjects can make an informed choice. In the latter regime, transparency is more oriented towards documentation so that public authorities can review how data is being processed. Therefore, transparency can be regarded as an element of both informational self-determination and bureaucratic proceduralism. However, I would argue that transparency requirements are more consistent with bureaucratic proceduralism in the EU context because they oblige data controllers to document (and communicate) their procedures ex ante. Data protection focused on informational self-determination would also be more focused on the understandability of the privacy notices.

To better understand the nature of bureaucratic proceduralism Nissenbaum's *contextual integrity* framework can be of assistance. While it has not been used to inform information privacy legislation, it is helpful in explaining that information privacy legislation must be adaptive to context.

According to Nissenbaum (2010, p. 186), people's perception of information privacy depends on the time, setting, and actors involved in the disclosure of personal data. At the heart of the contextual integrity framework lies the examination of how information flows are governed by societal norms. The norms that govern the transmission, communication, transfer,

[23] A data controller can be defined as the entity who determines the means and purposes of the processing. In practice, this might be very difficult to determine, and in many cases, the data processor which should rely on the instructions of the data controller has more actual power over how personal data are processed.

distribution, and dissemination of personal information are called informational norms in Nissenbaum's (2010, p. 140) framework.

Informational norms are based on four building blocks: contexts, actors, attributes, and transmission principles. First, informational norms are always part of a wider normative system that governs conduct in general and, as a consequence, privacy in particular. Second, informational norms provide different roles for different actors – it is imperative to know in which capacity a person presides over, disseminates or receives personal information. Is the actor the recipient of information, the sender of information, or the subject of information? Third, the type of information involved will impact how it is and should be handled; however, attributes are also very sensitive to context. Finally, transmission principles provide additional rules for information flows, such as whether the disclosed information is confidential, that the information must be provided consensually, that the provider of information expects to be paid, or that the information may be sold or otherwise distributed (Nissenbaum, 2010, p. 145). An example of such a principle would be the right to be anonymous when speaking to the press, a right that is also legally recognised in many countries. Many informational norms have, in fact, been formally codified (Nissenbaum, 2010, p. 146). Therefore, the challenge with general, principle-based data protection legislation is to draft rules for a diverse set of contexts without making the law over- or under-inclusive.

Informational norms are breached when personal information disclosed in one setting is inappropriately shared in another or 'transgress context-relative norms'. If, for example, data is collected in conjunction with the use of a fitness app and used within this ecosystem, this is hardly regarded as invasive, but if this data is shared with insurers, people might experience that their privacy has been violated. Therefore, the challenge for legislators is to draft laws that permit uses of information in one sphere of activity but stops their transmission to another. This is why access to credit or health data has been more strictly regulated in the past. These types of personal information have been restricted to a specific set of actors that are, by way of their professional obligations, deemed worthy of having access to sensitive information. At the same time, they are also subjected to rules prescribing how the data should be handled.

The obvious shortcoming of bureaucratic proceduralism is that it is resource intensive for both data controllers and enforcement agencies. The administrative burden is heavy for both public administration and private companies. It requires highly skilled personnel, detailed bureaucratic structures, and the real possibility of a regulator actually evaluating these practices. A recent freedom of information request in the UK revealed that the

Information Commissioner's Office had spent nearly £1.3 million on the recent Cambridge Analytica scandal, of which Facebook was one of the 40 companies under investigation (Baines, 2018). To put that into perspective, Facebook was issued the maximum fine available under the old sanctions, £500,000. In other words, compliance investigations are expensive and the sheer volume of actors involved in data processing means that regulators are heavily understaffed compared with the task. Notwithstanding the most gruesome abuses of data protection principles, it is highly unlikely that smaller companies would ever be subjected to routine evaluations by a DPA.

Bureaucratic proceduralism has direct implications for how data protection law is enforced. The enforcement system in the EU is highly institutionalised as characterised by the requirement to set up independent 'supervisory authorities' or DPAs when the Data Protection Directive (95/46/EC) was implemented.[24] However, even though each EU member state is required to have a DPA, this does not mean that they are given adequate resources (Wright, 2016). In some countries, several DPAs might exist on a subnational level, such as in Spain and Germany. In Germany, for example, the regional DPA in Hamburg cracked down on Google's profiling activities (Essers, 2014). The DPAs and local courts might make quite different choices in their interpretation of rules, which challenges the harmonisation of data protection rules in the EU (Charlesworth, 2012, p. 90).

In addition to the national institutions, the European Data Protection Supervisor (EDPS) was instated by the Data Protection Directive. The role of the EDPS is mostly advisory, except in cases that concern the EU administration's processing of personal data. Conversely, in the U.S., privacy enforcement has been limited to self-regulatory instruments and oversight by the FTC, which can be denominated *bureaucratic liberalism*. Although the FTC's enforcement powers and resources are in many cases superior to that of the European DPAs, the lack of regulatory backing cripples the enforcement initiatives especially in relation to data brokerage and online marketing, as touched upon in the previous chapter.

In terms of policy applications, one initiative that can be considered bureaucratic liberalism is 'privacy by design', a conceptual framework

[24] DPAs are independent regulatory bodies focused on enforcing data protection regulation. Their powers are mainly investigatory, but the GDPR has granted supervisory authorities the power to issue sanctions, which was previously possible on a national level but not explicitly recognised in the Data Protection Directive. Sometimes the DPAs are called Information Commissioners, and sometimes they are part of other regulators. For reasons of clarity, the term 'data protection authority' will be used consistently in this study.

promoting that privacy aspects should be taken into account in all stages of planning and implementation of a software product (Cavoukian, 2009). Privacy by design was initially invented by the Information and Privacy Commissioner for the Canadian province of Ontario, Ann Cavoukian. It shuns procedural prescriptions, stressing instead the need for embedding privacy into the design of new products, the role of security, and the importance of default settings. Privacy by design has been adopted as a resolution by the International Conference of Data Protection and Privacy Commissioners and has been quite influential in policy circles (Levin, 2018).

While there is no conflict between the procedural approach and informational self-determination as such, relying too strongly on one might produce an adverse outcome for the right to privacy. Relying on informational self-determination to a very high degree might prove detrimental to the actual realisation of privacy rights because people are unaware of what they are agreeing to. Informational self-determination is further undermined by research that shows that even when people are presented with a choice, the default settings guide user behaviour to a large extent and should be seen as 'de facto regulation' (Shah & Sandvig, 2008; see also Lessig, 2006). Moreover, online service providers tend to design privacy choices in a way which favours data collection (Hartzog, 2018). On the contrary, cumbersome procedural obligations might result in non-compliance, require a lot of public resources for regulatory oversight, and burden smaller businesses.

3.4 THE INTERNAL CONFLICT IN DATA PROTECTION POLICY

This chapter has so far explained how data protection is conceptually linked to the right to privacy and the operational principles that guide data protection law in the EU. I have demonstrated how data protection policy can be traced back to 19th century jurisprudence and how especially technological innovation and the subsequent changing behaviour have resulted in new privacy laws.

I have demonstrated that the EU's data protection regulation is motivated both by ideas of informational self-determination and bureaucratic proceduralism, each contributing to concrete applications in data protection instruments. These two operational principles are not in conflict as such and might sometimes be mutually reinforcing, but advancing both at the same time adds complexity to the law. While increased complexity is somewhat problematic from a fundamental rights perspective, the more critical

operational conflict relates to the twin goal of data protection. One of the main arguments of this chapter is that there is a *purpose paradox* in the EU's data protection law. At the same time, as data protection law is to protect the fundamental right to privacy, it is also to advance the free movement of personal data.

The purpose paradox can be partly attributed to a logical fallacy. In theory, the EU's data protection law rests on the assumption that the same level of privacy protection will be awarded to whoever processes the data, as long as the EU's data protection rules apply. This conceptual ambiguity is connected to the EU's principle of *mutual recognition*, recognised in the landmark case *Cassis de Dijon* (C-120/78), which fortified the principle of the free movement of goods within the Union. The principle of mutual recognition stipulates that a product that is lawful in one member state should also be regarded as lawful in another, unless there are 'overriding reasons of public interest' (see TFEU, article 36). EU legislation cannot (and will not) support an interpretation of the law that would promote protectionist measures to realise privacy rights. The fundamental idea behind harmonisation is that EU law should provide a common baseline in the member state jurisdictions, although the protections awarded need not be identical. Similarly, although not explicitly stated as one of the aims within the actual Regulation, international transfers of data are to be facilitated as well.

Therefore, it is possible to extend data protection rights and obligations to other jurisdictions via contracts or other regulatory tools, such as the Commission recognising other jurisdictions as demonstrating an 'adequate' level of protection. However, privacy scholars argue that it is precisely the free movement of data that erodes the right to privacy (Ohm, 2010). Therefore, the purpose paradox does not exist in abstraction but in practice, where each transfer of data potentially constitutes a risk to the right to privacy. Data protection regulation, with a focus on bureaucratic proceduralism, does very little to address this problem, and it cannot do so because the other goal is to advance the free movement of data.

Policy goals with paradoxical measures can be attributed to the ambiguities surrounding how conceptual notions should be operationalised and applied in practice (Napoli, 2001, pp. 69-70). In the case of data protection legislation, I would still argue that the ambiguities are more connected to the competing interests than the difficulties in applying concepts of privacy in practice. The strong push to enable wide-scale personal data collection, processing, and sharing in combination with unease regarding the consequences of such actions enables this tension. The policy entrepreneurship of DPAs was highly decisive in getting data protection on the EU's regulatory agenda, but their

influence could only reach so far. Strong governmental interests as well as successful business lobbying managed to shape the Data Protection Directive in a direction which did not overtly challenge data accumulation and exploitation. The years that followed its inception would demonstrate that the Data Protection Directive was not sufficient to restrain datafication.

The twin goal of data protection has provided interest groups a broader framework for suggesting policy applications to legislators. Whereas an instrument focused solely on the aspects of privacy would not provide room for regulatory amendments that seek to improve and ease the transfer of personal data, data protection law seeks to advance datafication at the same time because its purpose is to contain it. The consequences of these possibilities should not be examined in abstraction but be connected to the legislative processes that shape future legislation. For this reason, it is necessary to look at how interest representatives participate in the EU's legislative process. This will provide a useful backdrop for understanding how lobbyists can capitalise on the twin goal of data protection to advance their agenda and how the nature of the legislative process shapes the EU's regulatory output. The next chapter will provide a theoretical overview of including third parties in the legislative process, how they operate, and what effect they might have on the EU's regulatory output.

4 PARTICIPATORY DEMOCRACY AND LEGITIMACY

The previous chapters have outlined the current media and communication landscape and the development of data collection practices within all aspects of public and private life. I have demonstrated how epistemological shifts have contributed to the development of a big data paradigm. Although big data is not as frequently mentioned in innovation policy discourse as it used to be, its paradigmatic repercussions have not waned. The datafication of social relations is ongoing, and although challenged by notions such as fairness, accountability, and privacy, its hegemonic status as a key producer of social knowledge remains firm but contested. One such area of contestation is the evolution of information privacy legislation. Chapter three outlined the origins of the right to privacy and how data protection law evolved in Europe. In particular, drawing on the research by Newman (2008a, 2008b), the empirical account of Simitis (1995), and the later research by Farrell and Newman (2019), I have demonstrated how the contents of data protection policy instruments have been heavily influenced by not only national DPAs but also industry lobbyists.

Many of the key principles in European data protection legislation have been and are still contested. Exactly why the GDPR looks the way it does is partly explainable by looking at these underlying conflicts of interests. However, such an assessment would be incomplete without first exploring the legislative system in which actors with opposing interests operate. In particular, it is worth departing from historical institutionalism to look at how and to what effect interest groups manage to influence the development of policy.

The current chapter seeks to explain the theoretical underpinnings of including third parties in the legislative process as well as explore the possible effects such strategies have previously had on the policy output of the EU. The GDPR's legislative process is, in many ways, similar to the policy processes of a range of other issues, although some features of the process make it unique. What sets the GDPR off from many other EU regulations is its extra-territorial application. Therefore, it is important to have a critical look at the EU's legislative process before addressing the consequences of lobbying.

As noted in the introduction, during the past twenty years, the EU has sought to improve the legitimacy of its policies partly by introducing third parties to the legislative process. One concrete measure has been the

institutionalisation of public consultations with stakeholders. In 2001, the Commission published a White Paper on European Governance which highlighted the need for 'wide participation throughout the policy chain – from conception to implementation', emphasising the role of including third parties in both legislative form and subsequent enforcement (European Commission, 2001, p. 10). Between 2013 and 2018, the Commission has launched approximately 500 public consultations (European Commission, 2018). The strategy is part of the Commission's (2015b) 'better regulation agenda' that seeks to involve citizens and stakeholders to a higher degree to increase the quality of its policy output.

The inclusion of third parties is conspicuously vague as to which actors it might include. Beyers, Eising, and Maloney (2008, p. 1106) also recognise that this is an issue that 'plagues the field of interest group studies', citing a broad variety of terms used to describe what these third parties are: 'interest groups, political interest groups, interest associations, interest organisations, organised interests, pressure groups, specific interests, special interest groups, citizen groups, public interest groups, non-governmental organisations, social movement organisations, and civil society organisations'.

To provide some clarity, they propose that three factors define an actor as an interest group: organisation, political interests, and informality. To put it differently, an interest group must be at least loosely organised, advocate for certain political solutions, and not seek political office or government status (Klüver, 2013, p. 6). Klüver (2013, p. 7) highlights that many types of interest groups exist, such as trade unions, employers' associations, companies, and professional associations, and distinguishes between two major types of interest groups: associations and companies. Importantly, the interest group definition excludes political parties, government agencies, and broad social movements. While this taxonomy of interest groups provides much needed clarity to the definition, I believe it is too limiting in scope. Particularly, it is problematic that political parties and public authorities are excluded from the definition.

In contrast, the Transparency Register (2019) categorises interest representatives in the following subsections: 'I - Professional consultancies/law firms/self-employed consultants, II - In-house lobbyists and trade/business/professional associations, III - Non-governmental organisations, Think tanks, research and academic institutions, V - Organisations representing churches and religious communities, and VI - Organisations representing local, regional and municipal authorities, other public or mixed entities, etc.' These categorisations matter. One of the organisations involved in lobbying decision-makers during the GDPR's

legislative process, the European Privacy Association, initially classified itself as a think tank. The Corporate European Observatory made a complaint stating that it was, in fact, an industry lobbyist, funded by Google, Facebook, Microsoft, and Yahoo, to name a few. As a result, the organisation had to change its status in the Register (Fontanella-Khan, 2013).

Table 4.1 A taxonomy of stakeholder terminology

Lobbyist	**Interest group**	**Interest representative**	**Stakeholder**
Professional consultancies and in-house lobbyists	Trade unions and professional associations	Professional consultancies and in-house lobbyists	Professional consultancies and in-house lobbyists
Trade unions and professional associations	Trade and business networks and associations	Business networks and associations	In-house lobbyists and business networks and associations
Trade and business networks and associations	Non-governmental organisations	Non-governmental organisations	Non-governmental organisations
Non-governmental organisations	Think tanks, research and academic institutions	Think tanks, research and academic institutions	Think tanks, research and academic institutions
		Public authorities	Public authorities
			Political parties
			Citizens

As was already clear in the examination of how the Data Protection Directive came to be, excluding public authorities from this study would not be feasible. Moreover, it is sometimes necessary to highlight the role of political parties outside their regular structures. However, I recognise the need to maintain conceptual clarity, and to avoid muddying the definitional waters further, I have decided to use the term stakeholder to cover all of these groups. The benefit of the term stakeholder is that it covers individuals, political parties, companies, associations, and governmental agencies. In contrast, I choose to define an interest group slightly more strictly than Klüver by excluding individual companies from the definition. While corporations may of course be seen as an entity composed of individual shareholders and therefore a

'group', I believe that it is lexically sounder to consider companies as unitary actors. I also choose to exclude professional consultancies from the interest group definition, although they might of course represent multiple clients. In contrast, I choose to exclude political parties, research institutions, and public authorities from the term 'lobbyist'; the first would only be seen as a stakeholder while the two latter categories qualify as 'interest representatives'. Table 4.1 outlines the taxonomy employed here.

Lobbying has been defined as 'the activity of interest groups trying to influence the government and to affect public decisions' (Bitonti, 2017, pp. 19-20). The definition is obviously very constrained by what one defines as an interest group. However, I argue that in the EU context, political parties and politicians may also engage in lobbying when they aim to influence actors outside their formal spheres of power. A national minister can, in my view, try to lobby a Commission official, as can a public authority official.

There are, of course, national precedents to the Commission's increased focus on stakeholder involvement. However, the EU is an unusual case in that its democratic legitimacy rests on weak foundations. The first part of this chapter will outline the origins of the EU's democratic deficit as well as the strategies employed to reduce it. In particular, I will address how the question of legitimacy is paramount to understanding the EU's focus on stakeholder involvement. Second, I will address what this means in practice in terms of how interest representatives are received in the EU, what tactics they employ, and what purpose they serve from an institutional perspective. Finally, I will address what this means for data protection policy.

4.1 LEGITIMACY ARGUMENTS FOR INCLUDING INTEREST REPRESENTATIVES

It is a matter of fact rather than a matter of debate that the EU suffers from a democratic deficit (see e.g. Majone, 2005; Michalis, 2007; Harlow, 2006, p. 204; Follesdal & Hix, 2006; Weiler, Haltern, & Mayer, 1995; Dunin-Wasowicz, 2009). The deficit can be traced back to the EU's Realpolitik origins, where the efficiency of policies was often regarded as more important than the transparency of procedure. The primary vessel of European integration, the so-called community method, relied on the transfer of sovereign power to a supranational organ, the Commission. The EU's expansion into further areas of policy has led to the increased erosion of national powers which challenges the old policy-making process (Dehousse, 2003). In a review of his earlier work, Majone (2014a) emphasises that where he thought indirect legitimacy

could legitimate limited competences on the supranational level before, the gradual expansion of supranational competences from the Maastricht Treaty onwards has made the legitimacy problem far more pronounced.

The problem with legitimacy in the EU, as Scharpf (1999, p. 187) argues, is the triple deficit of 'the lack of a pre-existing sense of collective identity, the lack of Europe-wide policy discourses, and the lack of a Europe-wide institutional infrastructure that could assure the political accountability of office holders to a European constituency'. Because the primary mode of input legitimacy is provided by elections and local demonstrations, the EU's input legitimacy is systemically questioned by the fact that its executive arm, the Commission, is not elected (Schmidt, 2013, p. 9). Furthermore, although the European Parliament became directly elected in 1979 and its powers have gradually increased, the EU election is treated as a secondary election with very low average voter turnout, thus failing to reduce the democratic deficit (Majone, 2014b). Moreover, the elections rarely raise questions that are relevant in the EU but are seen as an additional platform for addressing national policy issues.

Moravcsik (2002, p. 619) argues against this critique and stresses that because the EU-related issues are not likely to be salient in national public discourses, it is impossible to judge the EU's legitimacy based on public participation and that the EU's legitimacy rests primarily on the democratic accountability of national governments. Nicolaïdis (2013, p. 352), supportive of Moravcsik, argues that the EU should not be judged as a democracy but as a *demoicracy*, 'a Union of peoples who govern together, but not as one', which puts less stress on the need to have a European public sphere and more focus on the institutional and regulatory frameworks that constitute the EU (for a similar argument, see also Cheneval, Lavenex, & Schimmelfennig 2015). According to Nicolaïdis (2013, p. 258), the core norms behind the European project are transnational non-domination and mutual recognition, which require that power asymmetries in the EU are mitigated by a strong Commission and the European Court of Justice. The Commission's legislative powers are also usually justified by reference to the quality of policy output and the efficiency of supranational decision-making (Moravcsik, 2002; see also Coen, 2007, p. 335 for an overview). This is what, according to Scharpf (1999), constitutes 'output legitimacy'. Nevertheless, as Bellamy (2010) points out, legitimacy refers to the agency of the constituency and not whether a decision is perceived as the best possible, which in any case is hardly clear cut, a question of normative choices, and a matter of political debate. In a response to Moravcsik and Majone, Follesdal, and Hix (2006, p. 546) also maintain that

because positions are rarely articulated in EU policy, no debates exist that could increase the salience of the EU-related issues.

Regardless of how one chooses to evaluate the EU's democratic qualities (or lack thereof), the solutions that aim to alleviate the democratic deficit and existing power asymmetries are usually focused on improving the formal structures of participation and increasing transparency in the EU (Smismans, 2014). For example, access to Commission and Council documents was first implemented by way of Council and Commission decisions (Diamandouros, 2008), and in 1999, the right to access documents was formally incorporated in the Treaty of Amsterdam. In 2001, the Transparency Regulation (1049/2001/EC) that provided public access to documents held by European institutions was adopted. Inspired by the Nordic countries' access to information laws, the EU decided to make the legislative process more transparent: drafts were to be published online and third parties could participate in the legislative process in a more open manner (European Commission, 2000, p. 70). The Lisbon Treaty of 2007 introduced additional insight into and access to the legislative process. Although better transparency does not serve as a full proxy to legitimacy (Dunin-Wasowicz, 2009, p. 495), it at least provides an information supply on which to base legitimacy assessments.

Initiatives that relate to the representativeness of interest group participation have focused on mainly the Commission's consultations with stakeholders. A notable example is the introduction of public consultations in 2001. The public consultations can be traced back to ideals of participatory or deliberative democracy, where the legitimacy of policy is connected to the institutions and procedures that provide venues of deliberation (Greenwood, 2011a; Kohler-Koch, 2010; see also Habermas, 1999). Although online consultations do not really provide a setting for political discourse, it can be argued that they have a deliberative character owing to the diversity and rationality of arguments. The inclusion of interest groups can contribute to the legitimacy of a policy process not only by representing the larger constituency but also by enhancing the deliberative quality of legislative processes through increasing the diversity of arguments presented (Kochler-Koch, 2010; Quittkat & Kohler-Koch, 2013, p. 181).

While deliberative democracy may serve as an underlying ideological framework, the EU's version of participatory democracy is closer to the pragmatist approach of input–output legitimacy (Cengiz, 2018). The input–output legitimacy model sees the involvement of citizens in the policy-making process (input) and the presumed positive effects of those policies (output) as separate contributing factors to the legitimacy of the political system (Scharpf,

1999, pp. 7-12). The input level of participation can be characterised as 'government by the people', whereas the policy effects are associated with the principle of 'government for the people'. Whereas input legitimacy relies on public deliberation, output legitimacy relies on the presumed positive effects of enacted policies (Schmidt, 2013, p. 5). Quittkat and Kohler-Koch (2013, p. 48) argue that while including citizens in decision-making is a publicly stated goal, 'it is hard to avoid the impression that efficient governance is given more and more priority'. In a way, public consultations can be seen as a middle ground between Bellamy's (2010) idealism and Moravcsik's (2002) cynicism: they generally lack input from citizens and are used instrumentally by the Commission to inform policy, but they constitute an attempt to ground policies in viewpoints from outside the corridors of Brussels. Nevertheless, Bellamy (2010, p. 11) is also worried about regulatory capture owing to the closeness of the EU legislators to businesses and unions, highlighting that 'selective consultation with "stakeholders" creates a parallel dilemma, with the agenda potentially being set by the very groups whose interests' regulation should be seeking to harmonize with the public interest'.

The main difference, then, between deliberative democracy and the EU's input–output model of legitimacy is that the former presupposes that the purpose of deliberation is to reach consensus (see e.g. Cohen, 2011), whereas the latter is more focused on representation. The EU's input–model of legitimacy encourages participation; however, the goal is not consensus but to amass a wide variety of ideas that can be used to formulate policy. As such, the deliberative function of public consultations is only secondary because no consensus between the participating parties must be reached to draft rules and regulation. Policy input usually requires a national level of political activism which, in turn, is difficult to conjure on the EU level. Because the input of public consultations cannot readily be equated with 'government by the people', Schmidt (2013) proposes instead that the inclusion of citizens and interest groups in policy-making on the EU level should be categorised as 'interest-based throughput', where interest articulation is formally introduced to the policy-making process. This type of 'governance *with* the people' is thought to counterbalance the lack of input by the people (Schmidt, 2013, p. 15, emphasis in original). The way interest group participation is institutionalised in the EU's policy processes is radically different from input as a result of public campaigning or aggressive lobbying, which is why it is fruitful to evaluate this aspect of EU policy-making with reference to throughput legitimacy (Schmidt, 2013, p. 7).

The EU's throughput legitimacy has been called into question as well. The Commission has often been accused of drafting laws behind closed doors and

meeting with industry representatives without public insight (Schmidt, 2013, p. 15). It is in light of this critique that transparency requirements have been instated. One consequence is that public consultations are included in the legislative process when a policy area is regarded as having a major impact on society (European Commission, 2002). Another consequence is that the Commission has suggested that the EU Transparency Register (2019) should be mandatory, requiring interest representatives to register in order to gain access to EU institutions and officials (European Commission, 2016a). However, it must be stressed that the Transparency Register was voluntary and not as well maintained during the GDPR's legislative process and that many of the participants to the public consultation were not registered at the time.

During the public consultations, private and public stakeholders are invited or encouraged to participate by submitting documents which either outline what legislation should be implemented or suggest how the current legislation and its enforcement could be improved. As Coen (2007, p. 336) proposes, lobbying is a two-way street because the EU institutions also seek out and, in some cases, even fund private and public interests. Grossman (2004, pp. 648-649) sees the Commission's approach to invite stakeholders to participate in the policy process as opportunistic as it will not 'hesitate to "betray" … contacts and "partners" in order to further its own competencies and European integration in general'. Extending invitations to participate is, of course, about legitimating policy and finding different rationales for going ahead with a preferred policy position. Choosing to frame this type of behaviour as betrayal is rather surprising but underlines that the inclusion of interest groups is also self-serving.

The incorporation of public consultations in the legislative process is an example of institutional change that also shapes policy actors' behaviour. However, while some institutions change, others remain. Here I draw on Armstrong and Bulmer's (1998, p. 52) definition of institutions as 'formal institutions; informal institutions and conventions; the norms and symbols embedded in them; and policy instruments and procedures'.[25] Although the policy procedures undoubtedly have changed as the EU has instated more transparency requirements in the Maastricht and Lisbon Agreements, informal institutions and conventions are likely to remain. According to Armstrong and Bulmer (*ibid.*), 'institutions structure the access of political forces to the political process, creating a kind of bias'. In other words, even as

[25] This definition is quite close to Scott's (2014, p. 56) conception of institutions, according to which 'institutions comprise regulative, normative, and cultural cognitive elements'.

public consultations are included in the policy process, this does not necessarily mean that a wider range of stakeholders are consulted or, more importantly, listened to. Therefore, it is important to look at the 'institutional logic of interest intermediation' in the legislative processes (Woll, 2006, p. 460).

Coen's (1997) conceptualisation of the EU institutions as an elite pluralist environment is a fruitful starting point for exploring the EU's legislative process. According to Coen (2007, p. 335), EU policy-making has produced an 'élite trust-based relationship between insider interest groups and EU officials'. The EU's interest intermediation is heavily biased in favour of large European firms and Eurogroups with significant economic power and the ability to represent Europe-wide interests, respectively (Eising, 2007, p. 399). In some cases, however, public interest groups or organisations may also be insiders if the directors of Directorate-Generals (DGs) are sympathetic to their cause (Richardson, 2000). For example, the European Commission has often been criticised for advancing the interests of large European corporations and favouring an economic approach instead of focusing on the rights and freedoms of citizens when drafting media policy (Harcourt, 2005, p. 199; Hirsch & Petersen, 2007, p. 31). The Commission is also known for actively seeking out and involving ICT industries (Michalowitz, 2007, p. 139). However, it is quite difficult to make definite, generalisable statements on the actual influence of different societal actors on the EU's policy processes, and the only certain conclusion which can be drawn is that the 'level of access expected and provided can vary markedly for private and public interests across sectors, directorates, and policy areas' (Coen, 2007, p. 339).

Some of the problems associated with the EU's governance processes are unequal access to the legislative processes, the lack of meaningful transparency in a policy environment that is notoriously information-heavy, and the accountability of the Commission and Council, which are not directly elected but rather an extension of political power relations on the national level (Schmidt, 2013, p. 16). For Schmidt (2013, p. 18), one solution to improve throughput legitimacy is to find more ways to include citizens, for example, by having national governments introduce civil society into national formulation processes. However, she also notes that 'stakeholder democracy, even if improved, is not necessarily public interest-oriented democracy' and cannot substitute the lack of input entirely. Kohler-Koch (2010) highlights that while the participation of civil society organisations has been lauded as a political goal in the EU, it is questionable whether these organisations can contribute to better representation. To what extent, then, the views of interest groups should be taken into account remains an open question because the ideals of

deliberation are clearly not met. Nevertheless, the increased importance of including interest groups in the legislative process means that analysing who takes part in public consultation is potentially indicative of the output of the EU institutions as well. Therefore, it is imperative to examine the throughput and output of policy processes together.

4.2 LOBBYING IN THE EU: WHO, HOW, AND TO WHAT EFFECT?

While the above discussion demonstrates the rationale behind introducing public consultations and formally including interest groups in the legislative process, it is worth examining the dynamics of interest group participation more closely. Peters (1994, p. 11) claimed that agenda-setting was already easier during the European Community than in national contexts because there are more points of access, many influential policy advocates, and a wide range of policy options that have already been legitimated in the member states. While most studies on agenda-setting have focused on the role of EU institutions and particularly the Commission's actions (Alexandrova & Carammia, 2018), the theoretical contribution of Peters did not preclude policy entrepreneurship to the EU institutions nor did that of Kingdon (2013, p. 122): 'These entrepreneurs are not necessarily found in or out of government, in elected or appointed positions, in interest groups or research organizations ... their defining characteristic, much as in the case of a business entrepreneur, is their willingness to invest their resources – time, energy, reputation, and sometimes money – in the hope of future return'. While the role of the formal institutions needs to be recognised, the role of external policy entrepreneurs that attempt to shape the agenda need to be considered as well.

During the drafting of the EU legislation, interest groups aim to influence all the three institutions involved: the Commission, the Parliament, and the Council. They all play significant roles in the process, and as such, they are suitable targets for lobbying. Consequently, the 'three EU institutions need to be investigated simultaneously to understand the logic of interest politics at the European level' (Bouwen, 2002, pp. 366-367). According to previous studies, interest groups tend to be more active during the design stages rather than when policies are being implemented (Eising, 2007, p. 397). A logical conclusion is that the most efforts to influence policies are made in the very first stages of policy formulation, that is, when the Commission is drafting its first policy documents on a specific topic (Eising, 2007, p. 398).

In particular, getting the right DG to advance a policy is of importance. However, the DGs can sometimes have highly overlapping tasks, and policy issues can sometimes fall between them (Peters, 1994, p. 14). This provides policy entrepreneurs with more options to set the agenda because getting a particular DG to advance a policy issue will be instrumental in developing favourable policy applications (Peters, 1994, p. 14).

When it comes to specific policy proposals, the Commission is considered the most important target for lobbying (Eising, 2007, p. 387). Policy entrepreneurs who wish to advance a specific policy are best positioned to do so before the Commission has put forth a formal position. Although the Council and the Parliament can make amendments to the Commission's proposals, the Commission sets the agenda and the changes made at a later stage will not be major (Boräng & Naurin, 2015, p. 501). Interest groups also recognise that it is difficult to obtain significant changes to a Commission proposal after it has been submitted to the Council and the Parliament (Eising, 2007, p. 387).

However, the Parliament's regulatory influence has increased in recent years (Rittberger, 2007), which means that it has also become a suitable target for lobbying (Lehmann, 2009). While Eising (2007, p. 398) found that many associations regarded the Parliament as less important than the other EU institutions, large firms still chose to lobby MEPs to the same extent as the Commission. Whether this is a conscious strategic choice or lack of insight in the policy formulation process and/or connections to the institutions is difficult to assess.

Although interest group participation in the legislative process is used partly to increase the EU's throughput legitimacy, the Commission is heavily reliant on good relations with the industry when it drafts new policies and legislation (Coen, 2007, p. 335). According to Bouwen (2002), whether an interest group or firm will be heard depends on the 'access goods' it can provide. These access goods are not synonymous with economic power, but financial and technical means are of great importance. Bouwen (2002, p. 369) has identified *expert knowledge*, *information about the European encompassing interest*, and *information about the domestic encompassing interest* as the three main types of access goods. Expert knowledge refers to the expertise of the industry within specific policy areas. Without proper understanding of the workings of a policy domain, it is difficult to draft efficient legislation. Dominant industry actors will therefore be able to access the legislative process by their knowledge of the market mechanisms involved.

European encompassing interest refers to an association's or firm's access to the interests and needs of a sector affected by EU policy. This particular

access good is naturally provided by Eurogroups such as the EBF or the European Association of European Internet Services Providers Associations (EuroISPA). Domestic encompassing interest refers to an association's or firm's access to the needs and interests of how a sector is affected by EU policy on the national level, typically represented by national associations or business networks. Because the EU regulation needs to be adhered to by a large variety of industry actors, it is of course desirable that as many corporations as possible are not hostile to the Commission's new policies. In some cases, as in the ICT sector, the Commission is directly dependent on telecommunications companies to succeed in realising its digital strategies. It follows that any new legislation that affects the telecommunications industry would also have to contain some concessions to the most powerful telecommunications companies. In media policy, the European Commission has often been criticised for advancing the interests of large European corporations and favouring an economic approach instead of focusing on the rights and freedoms of citizens (Coen, 2007, p. 335; Hirsch & Petersen, 2007, p. 31; Harcourt, 2005, p. 199).

Not surprisingly, Bouwen's (2002, p. 383) research confirmed that large individual firms have the best access to the European Commission out of the three organisational forms, which supports the elite pluralism hypothesis provided by Coen (1997). However, the level of access is not always determined by some sort of transaction. Sometimes cause groups have prioritised access to Commission fora because of sympathetic political leanings of DG directors (Coen, 2007, p. 339). Nevertheless, in an analysis of 100 policy decisions in the EU, Bernhagen, Dür, and Marshall (2015) concluded that the informational resources lobbyists provide were important when facing a friendly DG, but that friendliness alone did not move the Commission's policy position closer to the lobbyists' positions.

The access goods outlined above partly ignore the potential benefits of listening to public interest cause groups. Other scholars highlight the importance of citizen support, which can contribute to a higher degree of the output legitimacy of enacted policies. Drawing upon the rational choice theory (Downs, 1957; Coleman, 1990), Klüver (2013) departs from deliberative democracy and argues that lobbying can be seen as an exchange between interest groups and decision-makers, and the relevance of the exchange is determined by mutual benefit. Decision-makers expect that interest groups should have wide citizen support, economic power, and expertise in the policy issue (Klüver, 2013, p. 41, 48, 53). Interest groups, on the contrary, demand influence (Klüver, 2013, p. 24). A cause group with significant citizen support but limited financial resources may still be highly influential because it will be

able to sway potential voters' opinions, which would matter especially in the European Parliament. Therefore, it is fair to assume that the same interest groups can be very differently received depending on the EU institution or individual politician they choose to interact with.

However, the rational choice theory tends to ignore ideological factors. Supporting the mechanisms which uphold the big data paradigm cannot be reduced to a survivalist approach arguing that the primary purpose of politicians is to secure their seats in future elections. However, for corporations, this approach might hold true: if a business' primary business model is to process, analyse, and sell databases of personal data, any legislation which might encumber this capacity will be seen as a threat. Similarly, cause groups with a communication rights approach would naturally engage in a discursive struggle to strengthen data protection legislation by lobbying decision-makers and raising public awareness through various publicity stunts and website launches.

Notwithstanding the potential benefits of listening to cause groups, it is worth noting that business associations and firms are usually better staffed and funded, which facilitate their ability to influence policy outcomes at all levels of governance. Other resources include legitimacy and representativeness, knowledge, expertise, and information (Dür & Mateo, 2012, pp. 971-972). This is exemplified by public consultations, which, aside from the occasional engaged citizen, mostly attract participation from the industry (Quittkat, 2011). The industry responses are also the most carefully drafted because they would possess the resources necessary to submit well-written reports. Nevertheless, Bunea (2017) found that the stakeholders themselves did not perceive that the public consultations contributed to reinforcing an elite bias.

However, the public consultations cannot be viewed in isolation of other lobbying activity. Dür and Mateo (2012, p. 978) found that business associations have 'noticeably better access to executive institutions' and also slightly better access to 'both members of the European Parliament and … national parliaments than other associations'. Furthermore, they found that business associations have a clear advantage with respect to the number of direct contacts with officials, access to meetings, and ability to prepare position papers (Dür & Mateo, 2012, p. 979). Thus, the paradox of EU politics is that as transparency increases and participation in the legislative process is encouraged, business interests tend to dominate and eschew the balance further, thus maintaining the democratic deficit of the Union. This is the main challenge for achieving throughput legitimacy in the EU (Schmidt, 2013).

Coalitions and large associations are successful in lobbying because they can offer citizen support, economic power or information in greater numbers (Klüver, 2013, p. 45). If the issue at hand is highly complex and the institutional actor has limited knowledge of the policy domain, the 'information supply' by lobbying coalitions has an especially positive effect on their influence (Klüver, 2013, p. 58). Interest groups have usually been well received by especially MEPs for this reason (Kohler-Koch, 1997, p. 6). Where Klüver calls the exchange of information between interest groups and EU officials a 'mutual benefit', Coen (2007, p. 334) is more critical and calls it a 'significant resource dependency'. The two approaches differ in their fundamental approach to democratic theory: while Klüver clearly favours a more utilitarian, transactional, and output-oriented view on legislative processes, Coen is more concerned with (input) legitimacy. Greenwood (2017, p. 226), who has studied interest representation extensively, seems to land somewhere in the middle: while acknowledging that the EU relies on an informational exchange with elite tendencies, he argues that the plurality of interest groups and the fragmentation of their positions together with the design of procedural regimes 'ensures sufficient checks and balances'.

Because the data protection policy domain is inherently transnational, it follows that many U.S.-based companies aim to influence EU policy. This could mean that lobbying methods such as ad hoc issue coalitions are employed more frequently within this particular policy domain. [26] Many companies operate on the same premises regardless of the state of origin, and a video streaming service such as Dailymotion is likely to meet the same regulatory challenges as YouTube, despite the former being French and the

[26] Although the primary focus of this study is not lobbying coalitions, the Advocacy Coalition Framework (ACF) serves as a basis for understanding lobbying activity (Sabatier, 1998). ACF conceptualises policy subsystems as groups of people and/or organisations that interact regularly over a longer period of time to influence policy within specific policy areas or domains (Sabatier, 1998, p. 113). The subsystems are further divided into advocacy coalitions, which are composed of actors from both public and private organisations who share normative beliefs and engage in a 'non-trivial degree of co-ordinated activity over time' (Sabatier, 1998, p. 103). The division of interest groups and firms into policy subsystems and coalitions is a way of understanding how public and private interests converge. Whether a co-ordinated coalition factually exists is, in this particular case, secondary because the primary focus lies in identifying the stakeholders that shape data protection policy rather than examining exactly how the interest groups are organised. As earlier research has shown, a large part of the EU interest groups is already formally organised as advocacy coalitions in European or national umbrella associations that represent various trade groups; as such, the need to form less-formalised ad hoc issue coalitions is less acute than that in the U.S. (Mahoney, 2007, p. 377). Interestingly, it is the wealthier organisations that choose to pool their resources rather than poorer ones (Mahoney, 2007, p. 378).

latter a Google company. Thus, lobbying efforts might be coordinated among ICT companies to reach the same goals. There is empirical evidence of companies forming coalitions on specific issues, despite a lack of formal partnerships (Klüver, 2013, p. 54). Klüver (2013, p. 53) argues that the collective resources of lobbying coalitions need to be taken into account when measuring influence.

Political scientists are often eager to point out that access does not necessarily equal influence (see e.g. Beyers, 2002; Dür, 2009; Eising, 2007). While better access to the EU institutions should not be seen as synonymous with influence, the ability to set the agenda on a policy issue *is* determined by access. Having privileged access to the EU institutions might not equate significant influence, but not participating in the policy process at all guarantees a complete absence of influence. For the above-mentioned reasons, it is important to look at which actors are represented in the public consultations on data protection policy. Several studies have confirmed that business networks and associations represent the majority of all EU interest groups (Greenwood, 2011b), and it would be highly surprising if this were not the case in the data protection policy domain.

However, there are other ways to study the influence of interest groups. Apart from subjective studies where policy-makers and interest groups themselves estimate their success (cf. Whiteley & Wingard 1987; Heinz et al., 1993; Egdell & Thomson, 1999; Pappi & Henning, 1999), a few studies have been conducted where objectively observed policy outcomes are compared with the positions of lobbyists (McKay, 2012; Bernhagen, 2012; Klüver, 2013; Dür, Marshall, & Bernhagen, 2019). Klüver's (2013) and Dür, Marshall, and Bernhagen's (2019) studies on the influence of interest groups in the EU have come up with the results that challenge the notion that the EU is generally supportive of corporate interests.

Klüver (2013) has studied influence through quantitative text analysis based on the prevalence of certain keywords and phrases that are associated with different policy positions and their occurrence in subsequent legislative drafts by the European Commission. Klüver (2013, p. 207) found that citizen support and economic power are *equally* important factors to consider when measuring the influence of lobbyists. Corporations were certainly better represented than citizens and consumers, but this did not translate into influence (Klüver, 2013, p. 214).

Dür, Marshall, and Bernhagen (2019) come to a slightly different conclusion using a spatial approach to measuring interest group success. In their approach, actors' policy positions are assigned on a scale of 0–100, where success is determined by the distance between an actor's ideal policy point and

the final outcome (Dür, Marshall, & Bernhagen, 2019, p. 48). Low values on the scale represent less regulation and high values represent more regulation. The policy positions were quantified by EU officials (Dür, Marshall, & Bernhagen, 2019, p. 26). In their analysis of 70 regulatory proposals, containing the policy positions of 853 interest groups, the authors concluded that citizen groups were more successful than business groups (Dür, Marshall, & Bernhagen, 2019, p. 77). They explain this by pointing out that businesses tend to be supportive of the status quo, whereas citizen groups are more inclined to push for more regulation. Nevertheless, Dür, Marshall, and Bernhagen (2019, p. 77) acknowledge that businesses tend to be successful when the policy issue is less conflictual, and they are met with limited opposition from other interest groups. This can be connected to the research on lobbying success that suggests that businesses are more successful in periods of 'quiet politics' when political salience is low (Culpepper, 2010; Rasmussen, 2015). Furthermore, they point out that industry lobbyists tend to be accomplished at loophole lobbying, succeeding to add important exceptions to otherwise disadvantageous rules (Dür, Marshall, & Bernhagen, 2019, pp. 84-85, 90, 95, 104). This is also consistent with studies suggesting that lobbyists are more successful when issues are complex (Rasmussen, 2015), and Boräng and Naurin's (2015) study of frame congruence that concluded that civil society frames were more often similar to the frames employed by EU officials.

A more detailed review of estimating influence is provided in chapter 5, but it is interesting to note at this stage that different methodological approaches have resulted in quite varying results. The dominant idea that business groups are more influential is convincingly challenged by the two quantitative approaches presented here. It is true that when the EU is intending to introduce new legislation in a policy domain, many businesses stand to lose. As such, the balance is already tilted in favour of more regulation. However, many policy proposals contain both favourable and detrimental regulatory obligations and rights for many different actors. Therefore, qualitatively assessing which actors promote what policy applications is instrumental in examining relative influence within a policy domain, regardless of whether the introduction of a new regulation may be considered a policy failure for an interest group.

In the introduction to this chapter, I have highlighted that policy entrepreneurs would be inclined to attempt to frame policy issues in a certain way to set the agenda early on. While one aspect of this is getting a policy in front of the right DG, another is establishing the appropriate frame for a policy issue. Therefore, it is important to note that interest groups use different

arguments in different venues, so-called policy frames (Rein & Schön, 1994; Harcourt, 1998; Baumgartner & Mahoney, 2008; Klüver, Mahoney, & Opper, 2015, p. 483; Boräng & Naurin, 2015; Eising, Rasch, & Rozbicka, 2015; De Bruycker, 2017; Voltolini & Eising, 2017). In the EU, political scientists have tried to empirically analyse to what extent the frames employed by interest groups have had an influence on the Commission's position by comparing framing congruence over time (Boräng & Naurin, 2015; Klüver & Mahoney, 2015), framing strategies by interest groups (Klüver, Mahoney, & Opper, 2015, p. 483), and the Commission's use of different frames (Harcourt, 1998; Morth, 2000; Thomas & Turnbull, 2017).

While many policy studies use the definitions of framing employed in social movement studies (cf. Benford & Snow, 2000) and communication studies (Entman, 1993), van Hulst and Yanow (2016) convincingly argue that Rein and Schön's conceptual framework is best adapted to policy processes. As such, the idea of framing is closely related to that of agenda-setting and policy entrepreneurs. Rein and Schön (1994, p. 32) differentiate between rhetoric frames and action frames, where the former are used to influence policy debate and the latter shape actual policy practice. Therefore, position papers and lobbyists' proposals are usually focused on shaping action frames. One of Rein and Schön's (1994) arguments is that policy issues are more easily defined early on in the policy process and more difficult to reframe later on. van Hulst and Yanow (2016) develop Rein and Schön's original processes of framing, naming, selecting, and storytelling and add two additional processes, sense-making and categorising. According to van Hulst and Yanow (2016, pp. 97-99), actors first try to make sense of the issue at hand, after which they will proceed to select which aspects of the issue to focus on and then name and categorise it. Last, framers attempt to establish a narrative around the issue: '[i]n telling about policy action and its human and non-human actors, policy framing stories implicitly or explicitly attribute blame or praise and suggest causes of harm or success' (van Hulst & Yanow, 2016, p. 101). While the present study is more focused on influence as demonstrated by concrete policy applications and not a detailed depiction of framing strategies, action frame congruence between lobby proposals and the EU policy output is also indicative of influence.

Using different frames in different settings makes sense as the composition and roles of the three EU institutions are radically different. Within the institutions, there are also significant differences that need to be taken into account. Strategies that refer to the public interest may be less effective on the Commission officials than the ones that focus on technical and economic arguments for the simple reason that they are not democratically elected (see

Coen, 2007, p. 340). Nevertheless, interest groups are much more likely to use public interest frames when a proposal is drafted by the DG Environment, DG Justice, or DG Health and Consumer Protection (Klüver, Mahoney, & Opper, 2015, p. 491). However, it may be noted that Klüver, Mahoney, and Opper (2015) had labelled 40% of all studied policy frames as either technical or legal. An alternative interpretation of the results could instead highlight that ideological choices are often enshrouded in technical or legal jargon, which quantitative text analysis tools have difficulties identifying.

In the data protection policy domain, three DGs have at different times spearheaded the development of new policy: DG INFSO (now DG Communications Networks, Content, and Technology) drafted the first Data Protection Directive, the Directorate-General for Internal Market (now DG Internal Market, Industry, Entrepreneurship, and SMEs) provided the review of the Directive, and DG Justice and Consumers drafted the GDPR. The different foci of the DGs imply that interest group framing strategies of data protection policy have probably differed depending on which DG was in charge.

The Parliament, on the contrary, is quite fragmented, with 751 MEPs in eight political groups that are sometimes unsuccessful in negotiating common strategies. Although the MEPs have assistants, the Parliament possesses less technical expertise than the Commission. Because all the proposed EU legislation cannot possibly be the responsibility of all MEPs, the Parliament is divided into 20 parliamentary committees with different foci. In the case of the GDPR, the Parliament's amendments were prepared by the Committee on Civil Liberties, Justice, and Home Affairs (LIBE), while the Committee on Employment and Social Affairs (EMPL), the Committee on Industry, Research and Energy (ITRE), the Committee on the Internal Market and Consumer Protection (IMCO), and the Committee on Legal Affairs (JURI) provided opinions (European Parliament, 2013).

Therefore, interest representatives would likely focus on using employment, consumer protection, industry, as well as civil liberties frames while addressing MEPs in the corresponding committees. Earlier research has shown that the chairs of the committees have been frequent targets of interest groups (Klüver, Braun, & Beyers, 2015, p. 454). Drawing on Bouwen's (2002) model of access goods, Eising (2007, p. 392) concluded that the Parliament demanded information on both the European and national encompassing interests yet were less interested in market knowledge provided by large firms. In the particular case of data protection, the exception to this rule might be the ITRE committee, whose purpose is to some extent oversee the industry's interests, which are likely to differ in the EU member states. Although MEPs

are accountable to their electorate, many also depend on the support of trade unions and business organisations.

From an EU lobbying perspective, the Council is a sub-optimal target: the ministers seldom convene in Brussels, which means it is more effective to lobby local governments via national routes (Eising, 2007, p. 388; Coen, 2007, p. 341). As a result, Council lobbying is not as well-researched as lobbying in the Commission and the Parliament (Hayes-Renshaw, 2009). Furthermore, the Council is mostly concerned with the domestic consequences of policies to begin with (Bouwen, 2004), which would require lobbyists to employ national frames when addressing the ministers in the Council. Because the Council is especially susceptible to lobbying from corporations with a strong presence in the member states (Klüver, 2013, p. 39), one would assume that American corporations are at a disadvantage. However, owing to favourable taxation policy, many ICT companies have decided to base themselves in Ireland. Therefore, it is possible that American companies can influence the Irish government and Irish MEPs.

4.3 DATA PROTECTION: WITH THE ELITES, FOR THE PEOPLE?

The above discussion has outlined three important trends in EU policy-making. First, the EU institutions are becoming more accessible and transparent, but the so-called elites still have privileged access to the EU institutions. Second, this elite pluralism can largely be attributed to the EU institutions' origins and their close relationships with the industry. After all, a functioning single market is only partly dependent on harmonised legislation, and the cooperation of dominant market actors is equally important. Third, EU legislators navigate an intrinsically complex regulatory environment with countless actors and interests, and listening to stakeholders is a prerequisite for being able to draft efficient policies and legislation. When legislators lack expert knowledge in policy areas, this relationship might evolve into one of dependency instead of mutual benefit. These trends contribute to creating an understanding of why lobbying is such an integral part of the EU. However, such a determinist approach overemphasises structure over ideology and disregards the ideological choices of political actors, windows of opportunity, and path dependencies of policy domains.

Data protection regulation in Europe has activist origins, and the Data Protection Directive was initiated in a manner which is slightly alien to the EU's decision-making process. The role of DPAs cannot be understated, and

their participation in the GDPR's legislative process is unquestionable. However, owing to their special relationship to the national ministries of justice as well as their institutionalised role in EU data protection governance, their input cannot be compared with that of individual lobbyists. It is, nevertheless, precisely this institutional advantage and prioritised access to law-makers that encouraged the Commission to be more inclusive in the GDPR's legislative process. After all, the private sector hardly participated in the early drafting of the Data Protection Directive. While that may to some commentators seem as an inherently positive feature of the legislative process, it is unquestionable that the companies that were directly affected by a new law had very little to say about its contents. In that respect, the Data Protection Directive's legislative process was very far from the ideals of deliberative democracy – closer, in fact, to enlightened absolutism: 'everything for the people, nothing by the people'.[27] The heart of the legitimacy problem is perhaps not solved by including interest groups, but excluding the private sector from the legislative process is equally problematic.

The legitimacy dilemma can be summarised as follows: because there is no hope of creating a truly European public sphere, we are left with the solution to institutionalise the involvement of interest groups, but as policy elites dominate these processes, they cannot serve as a proxy for deliberated societal consensus. Within the data protection policy domain, there is an added level of complexity. Data transfers are not limited by geographical borders, and information society services can be efficiently provided from one jurisdiction and consumed in another. If one chooses to ignore this aspect of the economies of personal data, the rights of EU citizens are heavily weakened. On the contrary, if one engages in extra-territorial law-making,[28] one creates responsibilities for actors that never had a say in the legislative process by way of political representation. To what extent is the legislature obliged to include non-nationals of member states in the legislative process? Furthermore, many of the world's largest IT companies are based in the U.S. but have European subsidiaries. What level of influence can be considered appropriate in those particular cases, knowing that these companies will mainly seek to transfer data outside of the EU's jurisdiction?

A legitimate policy process would have to take all of the following factors into account: the global nature of data protection, the unequal division of power, the EU law-makers' lack of policy expertise, the growing importance of

[27] Allegedly, this was the motto of Austrian emperor Joseph II who lived in the 18th century.

[28] Legal scholar Anu Bradford (2012) has coined this type of unilateral regulatory globalisation as the 'Brussels Effect'.

national DPAs, the ever-increasing lobbying activity in Brussels, and peoples' expectations of privacy. Owing to the data protection domain's cross-sectoral nature, even identifying all relevant sectors and interests is a challenge, much less including them in the decision-making process. The Data Protection Directive's legislative process revealed that at least the advertising industries, credit and financial actors, DPAs, and arms of the national governments are worth examining more closely. While the private sector might argue that they are fighting an uphill battle owing to the path dependence of data protection regulation in Europe and the undeniable influence of national regulators, the amount of resources spent on lobbying tells a different tale. If lobbying was a complete waste of time and money, specialised data protection lobbyists would not exist. Given the multitude of factors to consider when analysing the GDPR's legislative process, correctly identifying influence is of principal importance. The approach taken in this study is presented in the following chapter.

5 EVALUATING LEGITIMACY AND INFLUENCE

The previous chapters have outlined some paradigmatic shifts connected to the evolution of the surveillance society, the right to privacy, and, finally, the EU's legislative process. The challenge at hand is to make sense of these ideological, economic, political, technical, and legal developments without ascribing too much importance to one or the other. Policy processes are complex, and data protection policy is no exception. This chapter will outline the methodological approach taken to assess the degree of influence that certain positions have had on the GDPR's legislative process. The focus is on concrete policy applications and frames rather than individual actors. This is because the primary sources are documents and the paper trail leading up to the finalised regulation. Thus, it is impossible to say with absolute certainty which individual actors were influential, but it is possible to connect certain successful policy positions to a group of actors.

To reiterate, the following are overarching research questions of this study:

1. What policy alternatives were put forth by the EU institutions in the course of the GDPR's legislative process, and how did they correspond to the ideas, issues, and frames promoted by interest representatives?

2. What does the influence of organised interests and stakeholders in GDPR decision-making reveal about the democratic legitimacy of the process?

The following operational research questions are a way to trace the steps that transformed the GDPR into what it is today:

- Whose views have been heard during the legislative process?

- Which actors supported the creation of a new GDPR? Why did these actors support this mode of regulatory intervention?

- What are the main dividing lines between the suggestions made by different interest representatives in the two Commission consultations (2009 and 2011)?

- How are the interests of stakeholders reflected in the following: (1) the European Commission's Communication on data protection (2010);

(2) the Commission's Proposal for a General Data Protection Regulation (2012); (3) the European Parliament's amendments to the Proposal (2014); (4) the EU Council's adopted version (2015); and (5) the finalised Regulation (2016)?

To answer these questions, a variety of sources and tools are used. I will begin by outlining the sources consulted in the course of my research. The nature of the sources has significantly guided the research process, and the methodological choices made are reflective of an iterative process. The tools employed are primarily adapted for this particular study, which is why I choose to describe my sources prior to diving into the methodology (see Table 5.1). The methods used to explore influence are inspired by some of the EU policy studies that were presented in the previous chapter, but as I will demonstrate below, there are some key differences to the approach taken here.

5.1 SOURCES: POSITION PAPERS, SECONDARY TESTIMONIES AND POLICY OUTPUT

As mentioned in the introduction, the Commission launched three public consultations with the aim of mapping industry and civil society interests pertaining to data protection issues. In total, 523 position papers and comments have been submitted to the Commission and at least 73 have been distributed among MEPs (this number is likely to be higher). The three rounds of consultations served slightly different aims. The first consultation was a review of the initial Data Protection Directive that entered into force in 1998, although some of the provisions were transposed into national legislation much later. The review gathered interests mostly from business associations and law firms, but many of the position papers were extensive and quite detailed. While these position papers are indicative of the dedication of certain lobbyists and persistency of some grievances, a more detailed analysis of their contents has not been included in this study. The review clearly flagged the Data Protection Directive for an update, but as no steps were taken to revise the Directive, the impact of these replies on the GDPR's legislative process is negligible, at least compared with the two subsequent consultations.

Table 5.1 Primary and secondary sources used in the study

Primary sources	**Secondary sources**
2002 Consultation of EU countries (N = 14) and DPAs (N = 14) on the implementing measures	
2002 Summary of DPA and member state questionnaire answers	
2002 Position papers on implementation by stakeholders (N = 68)	
2002 Summary of online consultations with citizens and controllers	
2009 Consultation replies (N = 167)	
2010 Commission summary of replies to consultation	
2010 Communication	
2011 Consultation replies (N = 288)	2011 Eurobarometer on data protection
2012 Commission proposal including market impact assessment and summary of consultations (European Commission 2012a; 2012b; 2012c)	2013 Fontanella-Khan's (2013) article in the Financial Times
2014 Position papers submitted to MEPs (N = 73)	
2014 Parliament 1st reading of the GDPR	2014 Lobbyplag.eu influence analysis
2015 Council proposal	2015 Eurobarometer on data protection II
2015 EDPS commentary	2015 Lobbyplag.eu Council analysis
2016 Final GDPR	2016 Albrecht's (2016) account of the process
	2018–2019 Research by Rossi (2018), Laurer and Seidl (*forthcoming*), Kalyanpur and Newman (2019)

The two more decisive consultations were launched by DG Justice, which had been designated the lead on the data protection reform. The *Consultation on the legal framework for the fundamental right to protection of personal data*, as it was called, was launched in 2009 to determine whether the legislative

framework provided by the Directive was sufficient, and if not, what amendments citizens, NGOs, governments, and corporations requested. Some of the respondents replied to the consultation on request of the Commission, whereas others submitted papers on their own initiative.

The Commission asked the respondents to address the following questions:

- Please give us your views on the new challenges for personal data protection, in particular in the light of new technologies and globalisation.
- In your views, does the current legal framework meet these challenges?
- What future action would be needed to address the identified challenges?

The questions reveal that the Commission was aware of the need to update the EU's data protection framework and that it wished to receive general opinions on the subject which could legitimate a revision of the Directive from 1995. Although the public consultation was only a first step towards the GDPR, it laid the legitimate foundation on which the Commission would continue to draft both its 2010 *Communication on a comprehensive approach on personal data protection in the European Union* (European Commission, 2010a) and the proposal for a new General Data Protection Regulation (European Commission, 2012a). The Commission provided a 14-page summary of the replies on November 4, 2010, nearly a year after the consultation had ended (European Commission, 2010b). The summary does not provide a detailed account of who expressed what views; it merely lists the issues addressed. The summary will be used to support the results of this study.

The second public consultation, *the Consultation on the Commission's comprehensive approach to personal data protection in the European Union*, was launched alongside the publication of the 2010 Communication. As the Communication was partly inspired by the previous consultation, DG Justice wanted to obtain views on the Commission's ideas … on how to address the new challenges for personal data protection' (European Commission, 2011a). Whereas the first public consultation had been an open call asking for general feedback and comments, the Commission expected comments on its concrete suggestions in the second consultation. Many of these suggestions would eventually end up in the Proposal for a General Data Protection Regulation (European Commission, 2012a). The public consultation was open between 4

November, 2010 and 15 January, 2011, and during this time, the Commission received 288 position papers. The position papers vary in length and complexity, some simply expressing a few main points in one to two pages and others providing a comprehensive overview of the issues at hand spanning over fifty pages.

The purpose of the second consultation was to strengthen the Commission's proposal and preferably gain the affected industries' and civil society's support for the Regulation – in other words, the Commission aimed for increased throughput legitimacy by including the interested parties in this step of the process. Concurrently, the Commission commissioned an EU-wide survey on citizen's views on privacy and personal data (European Commission, 2011b). Thus, the consultation and the survey would serve as the key initiatives that would aim to legitimise the regulatory output of the Commission.

DG Justice finally drafted its proposals for a GDPR and a Directive on the processing of data related to law enforcement on January 25, 2012. In the previous rounds, it was not entirely clear that there would be a separate regulatory instrument for law enforcement. However, owing to the EU's limited competences in this regard, it is not entirely surprising that law enforcement was ultimately excluded from the GDPR. The two proposals were accompanied with a comprehensive market impact assessment report.

The Commission's proposal served as the starting point for the Parliament and the Council such that both based their revised proposals on this text. However, it would take up to three years until actual negotiations between the EU institutions took place. In the European Parliament, the proposal fell under the responsibility of the committee of Civil Liberties, Justice and Home Affairs (LIBE), with Jan-Philipp Albrecht (Greens/EFA) as lead rapporteur and Axel Voss (EPP), Marju Lauristin (S&D), Sophie in't Veld (ALDE), Timothy Kirkhope (ECR), Cornelia Ernst (GUE/NGL), Kristina Winberg (EFDD), Marine Le Pen (ENF) as shadow rapporteurs. Four additional committees, Industry, Research and Energy (ITRE), Legal Affairs (JURI), Committee on Employment and Social Affairs (EMPLO) and Internal Market and Consumer Protection (IMCO), submitted their own opinions suggesting amendments, which were taken into account in the final proposal.

The European Parliament adopted its opinion on the first reading in March 2014. During this process, over 5,300 amendments were suggested (Parltrack, 2016). Many of these amendments were, in one way or another, provided by lobbyists. Lobbyplag (2013), a project launched by the NGO OpenDataCity and Max Schrems, drew attention for revealing that certain MEPs had been copy-pasting amendments from position papers. They exposed that the position papers by interest groups influenced amendments to the GDPR heavily – for

better and for worse. The project website provides visitors with access to position papers and compares them with the amendments to the GDPR made by the MEPs. These position papers are used to a lesser extent in this study because they provide a less complete picture of interests than the consultation position papers. Nevertheless, Lobbyplag's analysis will be conjoined with the qualitative document analysis.

The Council worked on the Commission's proposal for over three years and significantly amended the Commission's proposed legislation. The final draft, signed at Brussels on 15 June, 2015 contained amendments to nearly every article in the Regulation. It is very clear that the EU's legislative process is not equally transparent during the different stages. Whereas notes from meetings that have addressed the development of the Council's version are available, apart from a few exceptions, position papers that were directed at the ministers have not been leaked to the public. However, Lobbyplag (2016) did manage to obtain documents that contained the individual positions of the different member states, spanning a total of 11,800 pages. While these documents are of interest, the primary focus of this study is the influence of interest representatives on the policy output of the EU institutions. As such, a more granular analysis of both individual MEPs' contributions and the different member states falls outside the scope of this study. Thus, the analysis is limited (although not strictly) to the version the Council agreed upon in June 2015 and how it compares to the earlier position papers.

5.2 ASSESSING INFLUENCE

One of the most difficult questions in policy research is ascribing influence with certainty (Dür, 2008). As noted in the previous chapter, access has often been used as a short-hand for influence – not in the sense that the relationship would be perfectly correlated but as a prerequisite for and an indicator of influence.

At this point, it is worth underlining that this study does not go into the details of the sources of power touched upon in the previous chapter – I will not provide a detailed analysis of the 'access goods' (Bouwen, 2002) interest representatives offer but look for evidence of influence in the policy output. Therefore, it is important to define what counts as influence. In this study, influence is defined as the ability to shift policy positions towards the goals that are aligned with one's own policy objectives. This might entail softening or strengthening a provision in a legislative draft, introducing new terminology or even convincing a political actor to shift frames entirely.

In formalised policy processes, such as the EU's legislative process, the effects of influence are, at least in theory, easily available. The result is a formalised policy, a law with discernible consequences. Moreover, owing to increased demands of transparency and critique of the EU's democratic deficit, the EU has provided improved insight into policy processes and the participation of stakeholders. It is possible to draw a parallel with the practice of studying algorithms. By analysing the input and output of an algorithm, it is possible to make some assumptions of the black box's contents (Bucher, 2016). Similarly, whereas a combination of personal factors, power relationships, path dependencies, and happenstance contributes to the final policy, I argue that it is possible to infer influence based on how the input – policy positions – and output – the different legislative proposals – communicate.

Within policy studies, this is often termed *process tracing*, where detailed knowledge of the process is used to find out the causes behind specific outcomes (Collier, 2011; Deters, 2013). In particular, process tracing is well equipped for studying complex phenomena such as path dependence (Bennett & Elmer, 2006). Therefore, process tracing can be used to determine the level of influence different interest groups have had on policy outcome or help explain how framing processes work (Voltolini & Eising, 2017). Bennett and Checkel (2014, 7) define process tracing as 'the analysis of evidence on processes, sequences and conjunctures of events within a case for the purposes of either developing or testing hypotheses about causal mechanisms that might causally explain the case'. In essence, process tracing is not limited to specific sources or even methodological tools, but it is generally 'backward-looking' (Scharpf, 1997). However, most research that uses process tracing tends to rely on interviews (Dür 2008, p. 563).

Dür (2009, pp. 1223-1224) notes that one problem with these studies is that assessing *the degree of influence* is difficult. Analysing evidence from a broad range of background documents and interviews can lead to difficulties in determining the weight of equivalent empirical sources. Nonetheless, although it would be valuable to determine influence more exactly, influence is hardly a matter which is entirely quantifiable in a reliable way. Another problem that might arise is that interest representatives might over-estimate their influence, while EU officials might also wish to portray legislative processes in a particular way (Dür 2008, p. 564).

Another way of determining influence is by assessing the distance between the preferences of actors and comparing it to the policy outcome (Mahoney, 2007), sometimes termed the preference attainment model. By determining the preferred policy position by different actors and comparing that position

to the enacted policy, it should be possible to discern whether an actor tends to be influential in policy processes. Dür (2009, p. 1224) rightly acknowledges that this approach also has its drawbacks because 'different causal effects may explain closeness'. Proximity is not always the same thing as causality.

In an effort to reap the benefits from both approaches, Klüver (2013) draws on the preference attainment model but uses computerised quantitative document analysis to gain insights into the process. Klüver (2013, p. 63) claims that 'comparing the policy preferences of interest groups with the Commission's preliminary draft proposal, the Commission's final proposal, and the final legislative act adopted by the Council and the European Parliament allows one to objectively assess who was successful in shifting the policy output over the course of the legislative process towards their ideal points'. With these types of computerised analysis, it is also possible to calculate the degree of proximity by comparing the distribution of word frequencies.

Klüver's methodological approach is more reliant on formal policy input than process tracing; nevertheless, compared with the preference attainment model, she pays further attention to what preceded the outcome. While the computerised quantitative content analysis is an efficient way of figuring out whether policy positions have shifted over time, the method's main drawback is that it must rely on word occurrences and policy documents that are comparable. For example, reliably comparing position papers with the articles of final directives and regulations is not possible, but the analysis must be limited to documents of the same kind. Moreover, as with the preference attainment model, analysis does not discriminate between causation and correlation.

The present study is inspired by these three approaches but relies mostly on qualitative document analysis. The critique towards process tracing is not devastating in this instance because no attempt is made to generalise the findings to all the policy process in the EU. Nonetheless, it will be important to be able to generalise the findings in the selected documents to achieve *internal validity*. Noting that it would not be feasible to qualitatively analyse all 596 position papers, I have chosen to analyse 20 position papers from the 2009 public consultation and 44 position papers from the 2011 public consultation. Although it would be possible to quantitatively assess all submitted position papers to draw some general insights from the legislative process, I have instead decided to limit my analysis to specific actors from a wide range of sectors to gain deeper knowledge of the actual issues at hand.

My reasons are the following: first, the participation of stakeholders in public consultations is strongly indicative of other lobbying activities, but it is

(probably) not a conclusive list of the actors who have contacted the EU institutions to influence the outcome of the Regulation. Thus, a quantitative analysis of all the position papers would not be any more valid. Second, the mere presence of an opinion in several position papers does not guarantee an equivalent amount of influence. As earlier studies have shown, other factors have to be considered, such as the possession of expert knowledge or connections to political constituencies (Klüver, 2013; Bouwen, 2002; Kohler-Koch, 1997; Dür & Mateo, 2012). The most important question is whether a particular stakeholder's views can be seen as representative of the goals of a sector. Thus, the selection of position papers from the pool of replies to the consultations is largely based on how reasonable it is to generalise the views in a position papers and *attribute them to a sector as a whole*. The Commission provides a crude categorisation of the stakeholders who submitted papers to the consultation, dividing the position papers into individuals, organisations, non-listed organisations, and public authorities. However, whether an organisation is listed bears little relevance to the purpose of this study, and to select a representative sample from the submitted replies to the consultation, it is thus necessary to re-categorise the respondents.

The method applied here can be summarised as follows. The first step of the analysis includes a categorisation of all the position papers to the 2009 and 2011 consultations to find appropriate position papers for the qualitative analysis. I will categorise the position papers according to (1) type of actor,[29] (2) country of origin,[30] and (3) sector.[31] In addition to these categories, I will collect data on the size of the organisation as well as annual budget or revenue. Because the actors differ in organisational structure, it is not feasible to compare them according to size or revenue, the exception being publicly listed companies which are required to disclose information on their operations. However, the figures do shed light on the economic powers involved, which according to Klüver's (2013) study was a factor which affected the policy

[29] 1 = Citizen, 2 = NGO and other non-profits, 3 = corporation, 4 = public authority, 5 = regional or national business network, 6 = international business network, 7 = research institution or association, 8 = political party, 9 = trade union, and 10 = professional association.

[30] This includes the categories 'global' and 'Europe' for associations that are not based in one nation state. Multinational corporations have been coded according to their headquarters and not the local subsidiary, regardless of what part of the company participated in the consultation. However, stock ownership has not been regarded.

[31] Twenty different sectors, of which some are more generally defined as some business associations and corporations span several industries. Sectors with fewer than two representatives in either consultation were added to the 'other' category.

output of the EU institutions. The most important factors taken into consideration while choosing the qualitative sample, in addition to the three categories provided above, were the primary business model, size, level of multinationality, and international recognition. Bouwen's (2002) categorisation of access goods helped inform the choices. For example, quite often it is more useful to analyse a position paper submitted by an umbrella association instead of a single company. However, an approach solely focused on size and scope would ignore smaller actors with considerable clout. The full list of analysed position papers can be found in Appendix 1.

The second step of the research comprises the qualitative assessment of the position papers in the 2009 consultation. To complement the qualitative analysis, I use Boolean search strings to comb through the entire material for keywords that appeared extensively in the papers chosen for the qualitative analysis. This analysis is secondary and not as advanced as the approach taken by Klüver, but it allows me to find whether specific terminology has been employed by certain interest representatives in the early stages of the lobbying process and whether the same terminology has surfaced in the EU institutions' output. The second step concludes with a comparison between the lobbyists' positions and the Commission's 2010 Communication.

The third step of the research focuses on the qualitative assessment of the position papers in the 2011 consultation. These papers are more extensive, and their contents are analysed with more detail than the first round of position papers. In addition to the qualitative analysis, the positions are formally coded to more precisely map the positions and ensure consistency over time (see section 5.3). These positions are used as a baseline for comparing the formal output of the different institutions: the Commission's draft proposal (2012), the Parliament's first reading (2014), and the Council's general approach (2015). The Parliament's first reading is viewed in light of the findings presented by Lobbyplag (2013) and therefore includes references to some of the leaked position papers that were directed towards MEPs. The Council's position is similarly analysed with the help of Lobbyplag's (2016) analysis of the leaked documents from the Council's proceedings. The Parliament's and Council's draft versions are also contrasted with the EDPS's commentary (2015).

The fourth step focuses on the analysis of the final Regulation, as agreed upon as a result of the trilogue negotiations. This analysis will be more cursory than the previous overview and focus on some of the key questions that were subject to the most extensive amendments. The final Regulation is obviously a compromise between the EU institutions' versions, but to reiterate, the purpose of this study is to find out whether certain positions presented by

lobbyists have been more willingly received by one EU institution or the other. Thus, I will look for key differences in the draft regulations and compare my findings to the positions advanced by interest representatives. In particular, it will be important to examine how the stakeholders relate to the elements of the big data paradigm: are they in favour of monitoring practices and extensive databases at the expense of privacy, or does the protection of personal data take the central stage? Rather than treating interest representatives as an unspecified, undemocratic mass aiming to influence decision-makers, I will try to discern what the representatives of diverse sectors advocate. Although interest representatives from different sectors might agree on some issues, I also suspect that there are diverging opinions on others. To make any meaningful and valid inferences, it is of utmost importance that stakeholder positions regarding information privacy are determined in a nuanced way. To do so, I have developed a taxonomy of information privacy principles that correspond to the privacy framework developed in chapter three.

5.3 DETERMINING STAKEHOLDER POSITIONS

Owing to the complexity of data protection legislation, it is quite difficult to create a workable taxonomy of different stakeholders' attitudes to information privacy. There are very few instances where an entity would be unequivocally for or against the regulation of information privacy. Rather, there is significant overlap between sectors on some issues and highly divergent opinions on others.

In chapter three, I presented how the right to data protection and its provisions could be deconstructed with reference to the two operational goals of data protection: the free movement of data and the protection of individuals. Whereas some articles in data protection legislation might advance the free movement of data, others protect the privacy of individuals. This inherent normative conflict is often ignored when focus is given to individual clauses or paragraphs in legal documents.

Nevertheless, individual position papers more often than not argue more forcibly for one of the twin goals of data protection, even though individual applicational propositions might be more closely associated with the other goal. Therefore, the question is whether the sum total of the concrete provisions presented by an actor primarily advances the free movement of data or the protection of individuals. To create a workable analytic tool for making this assessment, I have created a list of variables connected to the fundamental applicational domains associated with European data protection

law, which are assigned to either of the two operational goals (see table 5.2). Enforcement can be based on both approaches, as sanctions can be based on failure to provide user rights or failure to follow procedure regarding processing activities.

The process has been iterative, meaning that some of the variables have been added during the course of the analysis. The applicational domains associated with the free movement of data are co-regulation, self-regulation, law enforcement derogations, EU Commission powers, exceptions to data transfer legislation, and increased DPA cooperation. The applicational domains associated with the protection of privacy are binding regulation in lieu of other solutions, user empowerment, transparency, data minimisation, security, privacy by design, and sanctions. To clarify the role of different institutions, I have also identified whether each principle is connected to informational self-determination or bureaucratic proceduralism. This is not an exclusive list of the issues raised by interest groups or the Commission but includes some of the most salient issues that have been discovered in the course of the analysis. Most sectors have some special issues that are of utmost importance for their respective industries which might not be relevant for other sectors. One example is the case of derogations for research purposes or journalistic work – these are usually key issues in the position papers of research institutions and media outlets but are generally ignored by others.

This division is not entirely flawless, as some of these applicational domains can also be associated with the other goal, such as the role of increasing cooperation between regulators. While the goal with increasing cooperation is to facilitate global data flows, DPAs also enforce data protection legislation which means that they could obstruct data transfers more efficiently if the cooperation between authorities was more seamless. These applicational concepts and principles are further concretised into tangible propositions that are marked as observed variables, such as seals and marks in the case of self-regulation, contracts that are used to facilitate data transfers outside the EU, encryption and anonymisation technologies in the case of security, and so on (see table 5.2). Note that this is not a comprehensive list of all the concepts featured in the position papers or the proposed GDPR.

The papers from the first consultation are analysed with a focus on the core messages that the interest representative wishes to convey summarised in a few paragraphs. The goal is twofold – to determine the most salient issues of stakeholders and to identify keywords that are circulated in several of the position papers. After the qualitative analysis, a quantitative search for keywords will be conducted using Boolean search strings. Therefore, the

taxonomy in table 5.2 is of lesser importance in the first three steps of the analysis.

Table 5.2 Classification of observed variables.

Observed variables	**Applicational domain**	**Operational principle**	**Operational goal**
DPOs, data protection impact assessments (DPIAs), self-regulation with DPA oversight	Co-regulation	Bureaucratic proceduralism	Free movement of data
Certification, seals and marks, best practices	Self-regulation	Bureaucratic liberalism	Free movement of data
Data retention, law enforcement exceptions	Law enforcement	Bureaucratic proceduralism	Free movement of data
Commission adequacy decisions, delegated acts and implementing powers	Commission powers	Bureaucratic proceduralism	Free movement of data
BCRs, standard contract clauses, accountability principle, no to adequacy decisions	Data transfers	Bureaucratic proceduralism	Free movement of data
Lead authority, data supervisor board	DPA coordination	Bureaucratic proceduralism	Free movement of data
Consent, data portability, right to be forgotten, joint judicial remedy, access & rectification, right to object	User empowerment	Informational self-determination	Protection of privacy
Mandatory data breach report, understandability, obligatory privacy notices, accessibility, user communication	Transparency	Informational self-determination and bureaucratic proceduralism	Protection of privacy

Retention time limits, original purpose requirement, necessity requirement	Data minimisation	Bureaucratic proceduralism	Protection of privacy
Data protection risk assessment, privacy-enhancing technologies	Security	Bureaucratic proceduralism	Protection of privacy
Formal recognition of Privacy by design principles	Privacy by design and/or default	Bureaucratic proceduralism	Protection of privacy
Fines, controller/processor liability, compensation	Sanctions	Bureaucratic proceduralism	Protection of privacy

The position papers from the second consultation are more closely analysed according to the taxonomy presented in table 5.2. The stakeholder's policy position regarding each applicational principle is determined by examining the position paper and scored on a scale of 1–5, where 1 equals highly opposed, 2 equals opposed, 3 equals neutral or no opinion, 4 equals in favour, and 5 equals highly in favourIf an interest representative has not provided commentary on an issue, it will be coded as neutral. I will divide the stakeholders from the second consultation into three groups based on the coded position papers: 1) free data lobbyists, 2) privacy advocates, and 3) mixed approach proponents. In the second consultation, stakeholders were asked to comment on the Commission's outlined approach, which structures the position papers. Thus, it is easier to discern the interest representatives' policy position in the second consultation.

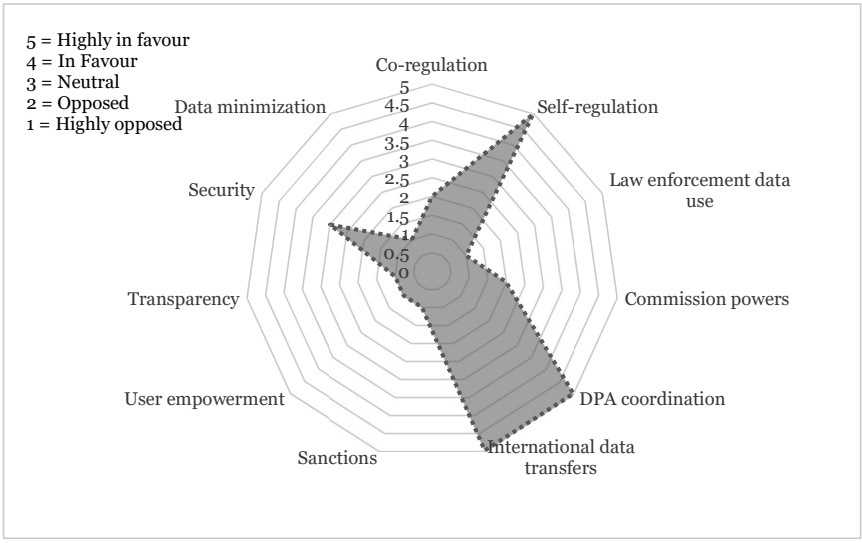
To underline the differences between the models, I provide radar charts of how a typical candidate would approach data protection legislation. This of course does not mean that there would not be significant variation within the three groups. To display the differences within the groups, I can compare tables and radar charts over how different actors approach specific concepts. The radar charts based on the position papers can then be compared with the model chart for each of the three models to exhibit key common characteristics as well as key differences.

5.3.1 FREE DATA LOBBYISTS

The free data lobbyists are united by their wish to ease the flow of personal information within the EU and beyond. However, the group is highly

heterogeneous because it contains every sector imaginable from advertisers to aviation, research institutions, and the telecommunications industry (see table 5.2). The typical free data lobbyist is a multinational corporation of either European or American origin, with significant activities in several EU member states. While the name implies professional interest representation, by way of their expressed interests, public authorities or even government ministries can be included in this category.

Figure 5.1 Free data lobbyist model type

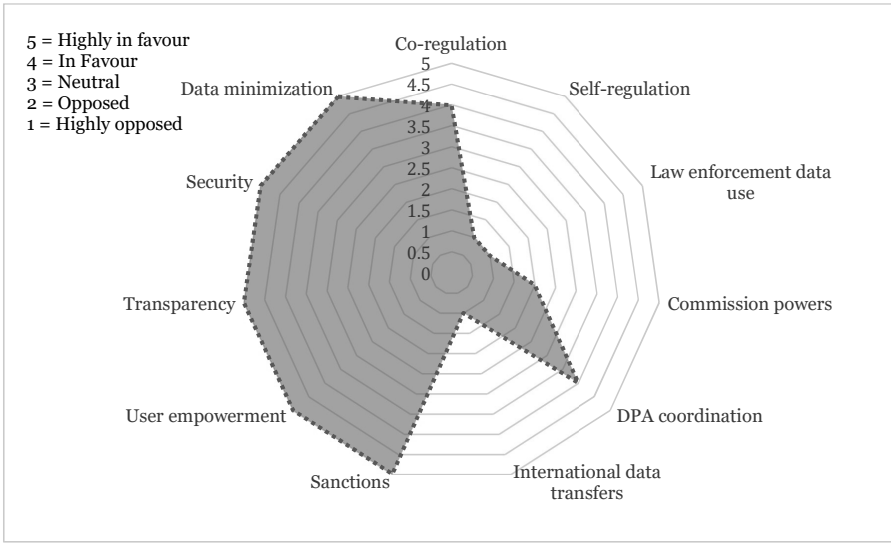


The crucial questions for free data lobbyists revolve around the ability of users to take control over their personal information and the data controllers' ability to transfer personal data from one country to another. Their attitudes towards different applicational domains (see figure 5.1) mirror this purpose. The free movement of data is often interpreted as minimising the amount of interference by public authorities.

5.3.2 PRIVACY ADVOCATES

Whereas the free data lobbyists generally support the second goal of data protection, the privacy advocates support the first goal, the protection of information privacy of citizens. On a general note, data privacy advocates are supportive of all measures that empower citizens, such as rights that enable the right to object, access, rectification, or be forgotten.

Figure 5.2 Data privacy advocate model type



Unsurprisingly, the ideal data privacy advocate model (figure 5.2) is almost the mirror image of the free data lobbyist model (figure 5.1).

5.3.3 MIXED APPROACH ADVOCATES

The mixed approach advocates are the interest representatives that cannot be easily placed in either group. It might be that they support user rights but simultaneously focus on self-regulation and data transfers to such a degree that placing the advocate in either category would not be justifiable. This group will also likely contain a very diverse set of actors.

The results from the second consultation and the three advocacy models are then used to evaluate the positions of the different EU institutions. The qualitative analysis along with the policy position coding are compared to the approach advanced by the Commission, the Parliament and the Council. These positions are then finally compared to the finalized GDPR.

The results from the second consultation and the three advocacy models are then used to evaluate the positions of the different EU institutions. The qualitative analysis along with the policy position coding is compared with the approach advanced by the Commission, the Parliament, and the Council. These positions are then finally compared with the final GDPR.

The reliability and validity of the analysis are further tested by asking for commentary by people who have been involved in the GPDR's legislative

process in one capacity or another. This commentary is informal in nature and mainly used to guide the analysis. Therefore, the comments are not included as source material but rather as a way to assure that the analysis is sound. Bearing in mind the drawbacks associated with process tracing and the preference attainment model (Dür, 2009), it is worth noting that this model of inquiry partly suffers from the same weaknesses as the three methods presented above. First, it is assumed that proximity equals influence. However, this inference is based on not only proximity but also novelty, which is easier to distinguish via qualitative analysis.

Second, owing to the qualitative nature of the study, some position papers have been left out and therefore the influence of some interest representatives might not be known. Nevertheless, as I have argued above, this would be the case even if all position papers were included in the sample because participation in formal public consultations is not the only lobbying strategy employed – some interest representatives might choose to leave no paper trail behind. Third, the evaluation of stakeholder interests and the choice of applicational principles to code are undoubtedly subjective. However, the position papers are publicly available (although no longer directly downloadable) and it is possible to test their validity should a classification raise doubts.

The results of this study will be presented in the following chapter. The chapter will begin with a brief overview of the stakeholders' characteristics as determined by the first step of the analysis, after which I will continue to present my study on influence according to the procedure outlined above. These results are then used to assess the legitimacy of the process.

6 LOBBYING IN THE EARLY STAGES OF POLICY FORMULATION

Chapter four elaborated on the question of the EU's democratic deficit and how the inclusion of interest groups impacts various aspects of the EU's legitimacy. To address the main research questions of this study that relate to the influence of organised interests and the legitimacy of the process, it is first necessary to provide an overview of the public consultations that preceded the draft of GDPR and the positions that were expressed by various interest groups.

It is important to first identify who participated and second, determine what opinions were expressed in the position papers:

1. Whose views have been heard during the legislative process?

2. What are the main dividing lines between the suggestions made by different interest representatives in the two Commission consultations (2009 and 2011)?

3. Which actors supported the creation of a new GDPR? Why did these actors support this mode of regulatory intervention?

The structure of this chapter follows the chronological order of the legislative process. First, I will present a brief overview of the legislative process beginning with the first reviews of the GDPR's predecessor, the Data Protection Directive, in 2002. Second, I will address who participated in the later public consultations organised by DG Justice and present a categorisation of the type of actors involved (1). This will allow me to evaluate to what extent the consultations contribute to the legitimacy of the legislative process such that the participating parties can be perceived as representative of different societal actors. Third, I will address the contents of the positions adopted by different interest representatives. This will be done in two steps. First, I present the concerns raised in the first consultation of 2009. In the next step, I will present both the Commission's 2010 Communication and the positions raised in the 2011 consultations that sought concrete comments on the Commission's proposal (2). The two are causally linked; therefore, I will touch upon the question of influence already at this stage. Crucially, I will look for the policy applications associated with different operational principles of information privacy. Third, drawing mainly on the position papers in the

second consultation, I will be able to demonstrate what type of actors favoured the drafting of a regulation instead of either amending the Directive or drafting a new one (3). After the characteristics of the interest groups and the applications they favour have been presented, I will present the congruence of these suggestions with the legislative drafts by the EU institutions in chapter seven.

6.1 AN OVERVIEW OF THE GDPR'S LEGISLATIVE PROCESS

The first steps outlining a legislative update can be traced back to 2002 when the Commission reviewed the original Data Protection Directive. [32] DG Internal Market provided one questionnaire for the DPAs (European Commission, 2003a) and another for the member states (European Commission, 2003b), organised a public survey for citizens (European Commission, 2003c) and controllers (European Commission, 2003d), and invited stakeholders to submit position papers.[33] The goal was threefold – to see whether the member states had implemented the Directive, to ask whether the national governments and DPAs had any suggestions on how to amend it and to see how controllers and data subjects viewed the regulatory framework.

The results from the review detail highly divergent practices between member states, which can largely be traced back to the respective member states' diverging policies on data protection. However, the most telling aspect of the review was the concluding remarks in which the member states were asked to address the difficulties in implementing the directive. Whereas some member states, such as Belgium, were happy with the status quo, others requested 'simplified' provisions focusing on misuse (Sweden). In what would be seen as a highly ironic statement considering Ireland's lacklustre position on enforcing data protection rules vis-à-vis U.S.-based technology companies, Ireland stated that 'The growth of the Internet, the rapid pace of technological change, and the globalisation of business, pose particular challenges for data protection rules' (European Commission, 2003a, p. 79). Nevertheless, one of the most obvious conclusions was that the Data Protection Directive did not sufficiently consider data that is processed online and did not provide clear

[32] The results from the review were previously available on the Commission's website but have since been taken down.

[33] Sixty eight position papers were submitted to the Commission. Many of the lobbyists would also submit position papers to the other consultations and participated in lobbying MEPs and the Council.

answers to how the transfer of data that is required for the web to work should be regulated. It may be noted that this review took place before the ePrivacy Directive was updated. However, the ePrivacy Directive is directly dependent on many of the key provisions in the Data Protection Directive, and any update to the latter would influence the former.

Regardless of the obvious shortcomings of the Data Protection Directive, the Commission would not proceed with a revision of the law until a few years later. It was not until social networking sites had become commonplace that the Commission decided to take the points raised by the member states, DPAs, and other interested parties into further consideration. The first concrete steps taken to update the European data protection legislation were in 2009 when the European Commission launched its first public consultation on the topic (see table 6.1). The initiative was taken by DG Justice and not DG INFSO, which had been the DG in charge of the previous Data Protection Directive, nor DG Internal Market, which had launched the review in 2002.

Laurer and Seidl (*forthcoming*) argue that DG Justice took the lead because the Lisbon Treaty had established data protection as a rights-based issue and because DG Justice provided the secretariat of the WP29. Therefore, it was 'an obvious choice', as expressed by Alexander Dix, who was the commissioner for data protection and freedom of information for the Berlin State Parliament (Laurer & Seidl, *forthcoming*).

Cloud computing was also becoming more prevalent at the time, and it was clear that any modifications to the data protection regime would have to take cloud-based services into account. The 2009 public consultation was the first of two public consultations in the Commission's legislative process. The public consultation platform was open to the general public and anyone could submit a position paper online. The *Consultation on the legal framework for the fundamental right to protection of personal data*, as it was called, was launched to determine whether the current legislative framework was sufficient, and if not, what amendments citizens, NGOs, governments, and corporations required. Some of the respondents replied to the consultation on request of the Commission, whereas others submitted papers on their own initiative.

Table 6.1 The GDPR's timeline.[34]

Year	Event	Primary actor(s)
2009	Consultation on the legal framework for the fundamental right to protection of personal data (European Commission 2009).	European Commission, interest groups
2010	Communication on a comprehensive approach on personal data protection in the European Union (European Commission 2010a).	European Commission
2011	Consultation on the Commission's comprehensive approach on personal data protection in the European Union (European Commission 2011a).	European Commission, interest groups
2011	Special Eurobarometer 359: Attitudes on data protection and electronic identity in the European Union (European Commission 2011b).	European Commission, TNS Opinion & Social
25 January 2012	Proposal for a new General Data Protection Regulation (European Commission 2012).	European Commission
12 March 2014	Proposal passes the European Parliament's first reading	European Parliament
15 June 2015	Council's position accepted by the EU Ministers' of Justice (Austria and Slovakia voted against)	European Council
2015	Trilogue meetings: seven in total between 24 June and 15 December	European Commission, the European Council and the European Parliament
17 December 2015	LIBE Committee adopts the result of the negotiations[35]	European Parliament

[34] Mainly sourced from Eur-lex (2016).

[35] The negotiated text was backed by 48 votes to 4, with 4 abstentions (European Parliament 2015).

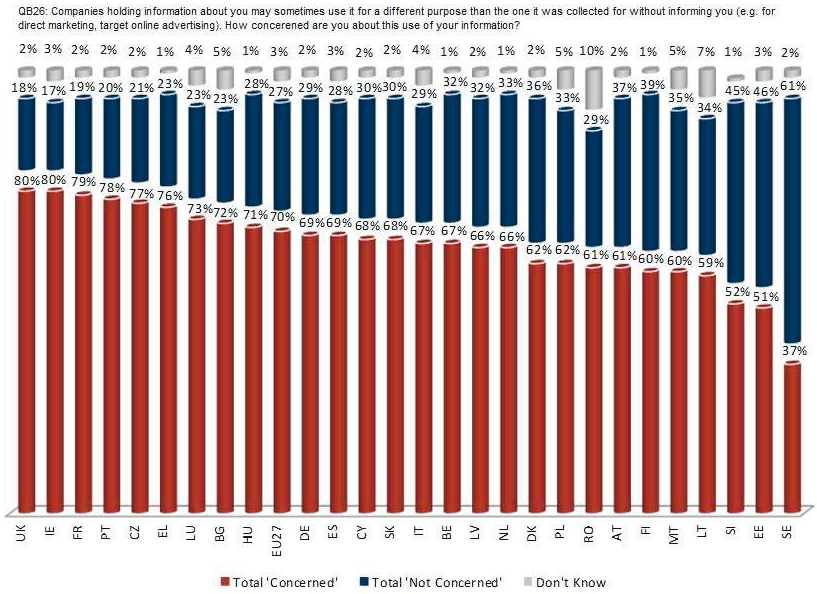
Year	Event	Primary actor(s)
8 April 2016	Council's position at first reading and statement of reasons	European Council
11 April 2016	Adoption by Commission of its communication on Council's position at first reading.	European Commission and the European Council
14 April 2016	Parliament's second reading, accepted without amendments	European Parliament
27 April 2016	Signature by the President of the European Parliament and by the President of the Council	European Council and the European Parliament
25 May 2018	Regulation in force	All member states

Although the public consultation was only a first step towards the GDPR, it laid the foundation on which the Commission could draft its 2010 *Communication on a comprehensive approach on personal data protection in the European Union* (European Commission, 2010a) which would set out the path for enacting a new data protection law. The second consultative round, the *Consultation on the Commission's comprehensive approach to personal data protection in the European Union* (European Commission, 2011a) was initiated so that stakeholders could comment on the Communication. Concurrently, the Commission commissioned a report on the *Attitudes on data protection and electronic identity in the European Union* (European Commission, 2011b).[36]

The report revealed that '**[n]ine out of ten Europeans** (92%) say they are concerned about mobile apps collecting their data without their consent' and '**[s]even Europeans out of ten** are concerned about the potential use that companies may make of the information disclosed' (European Commission, 2011b, pp. 1-3).

[36] The survey was requested by DG INFSO, DG Justice and the Joint Research Centre, and co-ordinated by DG Communication. The survey was conducted by TNS Opinion and Social.

Table 6.2 Europeans' concern about the undisclosed use of personal data per country (European Commission, 2011b).



The stakeholder proposals and the results from the survey were taken into account in the Proposal for a new General Data Protection Regulation (European Commission, 2012a), which was presented to the European Parliament and the Council in 2012 under the ordinary legislative procedure. However, exactly what weight the different positions were given was not clear. It can be noted that the original proposal was quite ambitious and clearly disregarded many of the more self-regulatory solutions promoted by lobbyists.

The public consultations did draw significant interest from different interest groups, yet the full force of lobbying would be revealed at a later stage when the European Parliament made amendments to the Commission's proposal. The Parliamentary readings proved to be thorough: in total, over 5,000 amendments were submitted in the committees involved in the Regulation (Parltrack, 2016). At the time, it was called one of the most lobbied legal documents in the history of the EU. Owing to leaks from MEPs, many of the lobby documents submitted to MEPs were made available to the public, sometimes revealing a high degree of both material and ideational overlap in the amendments provided by lobbyists and the amendments suggested by MEPs. The Parliament's first reading of the GDPR eventually passed in March

2014 with 621 votes in favour, 10 against, and 22 abstentions (European Commission, 2014). The overwhelming support of the first reading has largely been attributed to the change in salience caused by the Snowden revelations (Kalyanpur & Newman, 2019; Rossi, 2018; Laurer & Seidl, *forthcoming*).

The Council of the European Union adopted its position at a later stage in June, 2015. Whereas the different versions circulated within the Council are accessible to the general public, there are far fewer official and unofficial records of lobbying activity. After the Council had presented its version of the new Regulation, the trilogue negotiations between the Council, the Parliament, and the Commission were initiated. Although it had taken several years for the Council and the Parliament to reach their respective positions, the trilogue negotiations moved on comparatively swiftly and were formally concluded in December, 2015. The Council (2016) adopted its first reading on 8 April, which was in line with the compromise text, and the Parliament adopted the text without amendments in its second reading on 14 April, 2016. Between 2014 and 2016, 22% of all co-decision legislation was agreed upon in an early second reading (European Parliament, 2019), indicating that while the GDPR was slightly more difficult than the majority of files (75% of the decisions are already reached in the first reading), it was by no means exceptional. The President of the European Parliament and the President of the Council signed the new GDPR on 27 April, 2016.

The GDPR entered into force on May 25, 2018, slightly over two years after it was signed by the EU institutions. The compromise text was met with slight criticism from the digital rights groups that had attempted to influence the contents of the legislation, but it was mainly regarded as a satisfactory compromise (Järvinen, 2015). However, the new sanctions did cause quite a stir and many organisations struggled to interpret and implement the new provisions of the law during spring 2018, most notably causing a cascade of re-consent emails being sent to Internet users across Europe.

The GDPR's extra-territorial effects have also been covered in especially the U.S. press, often citing concerns about how U.S. companies will fare under the new regulations, and have sometimes been used as a critique against the U.S.'s own lacking privacy protections (Searls, 2018a, 2018b). The timing of the GDPR's entry into force could not have been better. In March 2018, several of the U.S. and U.K.'s leading newspapers broke news about Cambridge Analytica's questionable business practices and Facebook's careless data sharing practices. In the wake of the scandal, the FTC (2018) opened an investigation into Facebook's data sharing practices, Facebook CEO Mark Zuckerberg testified before the U.S. Congress (Wong, 2018) and the European Parliament, and the British Parliament issued an ultimatum to Zuckerberg to

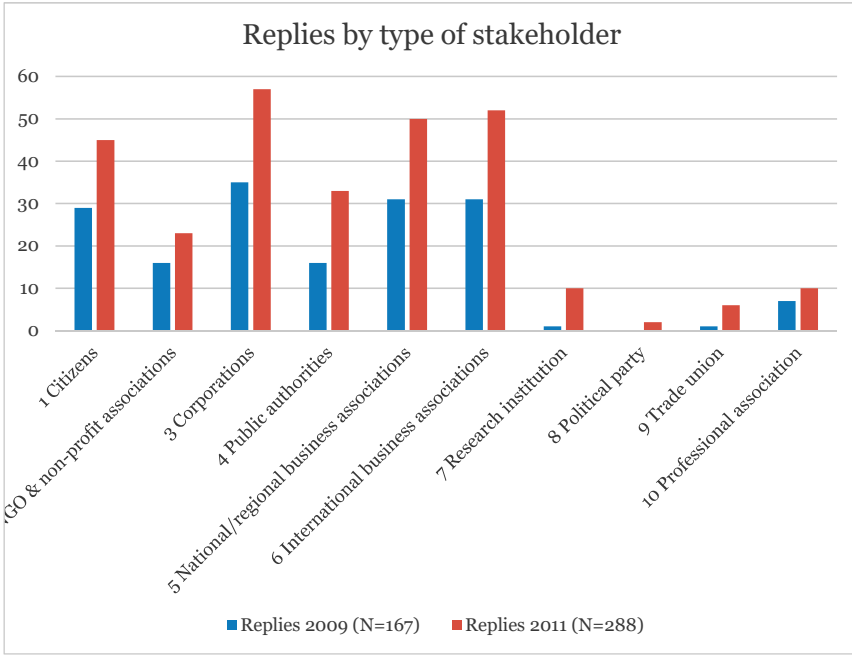
either appear before the Digital, Culture, Media, and Sport Committee voluntarily or face a formal summons to appear when he is next in the UK. The apparent failures of the world's largest social networking site and the world's second largest online advertising platform underlined that data protection needs to be taken seriously and that even the most technologically advanced and financially strong actors are capable of making severe mistakes. The GDPR could not have received a better introduction.

Nevertheless, there are several aspects of the legislative process that merit further study. First, owing to the intense lobbying that took place, the GDPR is an apt case study for examining the role of interest group influence in the EU and its consequences for the legitimacy of legislative processes. Second, it is necessary to look at not only who were ultimately successful in shaping the legislative agenda but also in what way. Following the arguments raised in chapter four, I will begin with an examination of the public consultations that preceded the Commission's proposal. I will examine them from two perspectives – whether the inclusion of interest groups can be seen as a proxy for legitimacy owing to the representativeness of the interest groups and if the legitimacy stems from the diversity of viewpoints presented.

6.2 REPRESENTATIVENESS AS A PROXY FOR LEGITIMACY

As I have touched upon above, the Commission did not provide any details on the characteristics on the respondents to the two public consultations. If the consultations are to contribute to the throughput legitimacy of the legislative process, some degree of representativeness is required (Schmidt, 2013). Through categorising each respondent in the two consultations, I can demonstrate whether the representative function of the consultations was fulfilled in the GDPR's legislative process.

Figure 6.1 Replies by type of stakeholder



The categorisation of respondents reveals that the majority of all replies to the consultations represented private interests rather than public ones, which support Dür and Mateo's (2012) claim that resource-rich organisations, such as business networks, are at an advantage vis-à-vis cause groups and other public interest associations. The results reaffirm Quittkat's (2011, p. 677) study of online consultations across different policy domains, where she found that around half of the submissions to consumer policy consultations come from either business interest associations or corporations.

In total, 455 position papers were sent to the two consultations. [37] The 2009 consultation attracted 167 submissions and the 2011 consultation 288 position papers, a 72% increase.[38] The results demonstrate that the biggest group of respondents could be categorised as either trade associations or

[37] The total number of participating organisations, public authorities, corporations, associations, and individuals was slightly higher, as six associations sent in joint replies. Therefore, I will refer to the submitters of these position papers as *entities* – a joint reply by two associations would therefore be registered as one entity and not two associations.

[38] One reply to the second consultation was clearly a joke and therefore removed from the results.

business networks in both consultations (62 in 2009 and 102 in 2011) (see figure 6.1). The trade associations were, to a high degree, regional, national, or international chambers of commerce or specialised business networks that represent the ICT sector, which is consistent with Coen's (1997) elite pluralism thesis.

Including the submissions by individual corporations, corporate interests where represented in 97 replies in 2009 and 152 replies in 2011. Compared with Quittkat's (2011) sample, the number of individual corporate submissions is exceptionally high. Surprisingly, the number of NGOs or other cause groups increased only moderately between the two consultations compared with other types of actors. Nevertheless, the second consultation drew more replies from public authorities than the previous consultation. While research institutions were largely absent in the first consultation, several institutions participated in the second round.

Of the 288 entities that participated in the second consultation, 90 entities had also participated in the first consultation in some capacity. The absolute number of corporations is probably higher owing to mergers, reorganised association structures or new network memberships, but the lack of consistency is still remarkable. Note that 47% (77) of the other entities that submitted to the first consultation refrained from submitting proposals to the second consultation. For example, there was a significant increase in citizen replies to the consultation (55%), but only two of the citizens had participated in the previous consultation. This lack of follow-up is perplexing, given previous research results that have stressed the importance of lobbying in the early stages of the decision-making process (e.g. Pierson, 2000; Eising, 2007).

Turning to the question of geographical representation, which might be considered a key issue from a legitimacy perspective, it is easy to discern that the population size of different member states is poorly correlated with the participation in public consultations. The size of the economy is a slightly better predictor, although not entirely consistent with the results. The three countries from which most proposals were submitted were the UK, Germany, and the U.S. This is hardly surprising as the UK and Germany are the two biggest economies in Europe. Germany is also known for its strict data protection policies. Perhaps most strikingly, U.S.-based associations, corporations or networks submitted 20 positions papers to the first consultation and 30 to the second, where stakeholders in many EU member states failed to send even one.

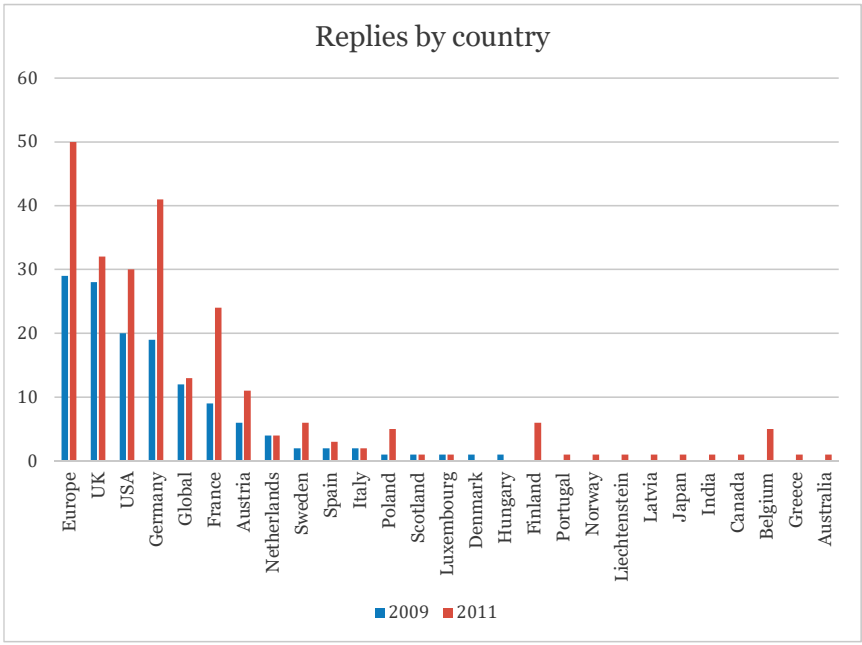
Most of the replies to the consultations came from organisations or associations with either European or global reach (see figure 6.2). On closer examination, the global trade associations also usually represent many

American corporations. Because the citizen respondents' backgrounds were often not explicitly stated, they were not included in the tables on sectors and countries of residence. However, it may be noted that most of the citizens had a background in either law or academia and many of them were German residents, which is consistent with research showing that German citizens are concerned with data retention and surveillance issues (Bug, 2013).

These results also confirm Quittkat's (2011, p. 668) results, where participants from countries central to EU-decision-making (France, Germany, and the UK) are highly over-represented whereas newer member states hardly participate. Quittkat's analysis did not include the participation of non-EU countries –because of either lack of data or differences in categorisation.[39] It must be stressed that in this study, country of residence has been assigned according to the headquarters of the company and not the local subsidiary. Therefore, Facebook's contribution is categorised as a U.S. submission and not an Irish one. However, this rule does not apply to the associations that span several countries or continents. It would be counterintuitive to categorise international business interest associations by their strategic location in Brussels. Therefore, they have been categorised as either 'European' or 'global'. This is not only an important methodological note in this study but also an issue which should be taken into account when the Commission reports on who participates in the consultations. Presently, the Commission reports that many replies come from Belgian associations. This is neither informative nor reflective of the actual interests represented.

[39] If one categorises companies according to the location of the subsidiary rather than the headquarters, the number of U.S.-based companies would not stand out.

Figure 6.2 Replies by country based on the location of headquarters, 2009 and 2011 consultations.[40]



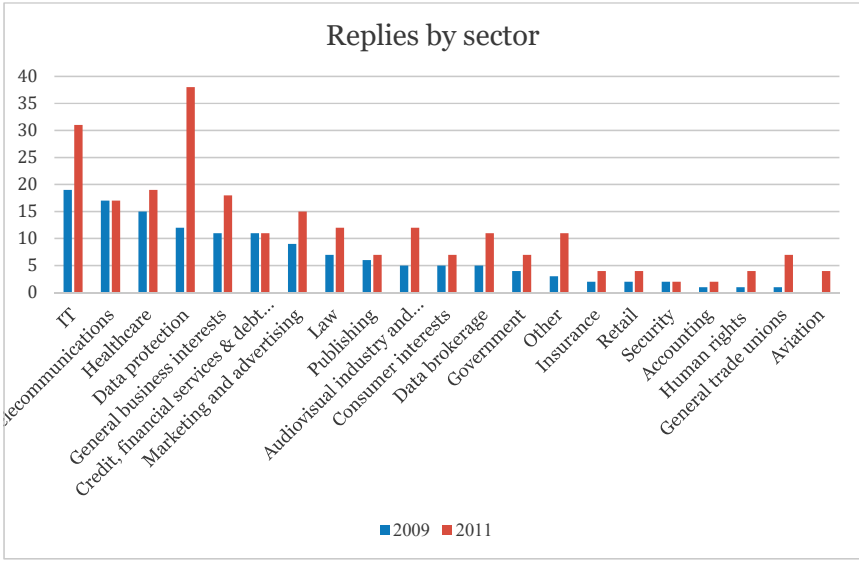
Because this study is focused on a single policy domain, it is worth looking at what different sectors are represented on a more granular level than the one provided by the Quittkat (2011). Although industry convergence and group mergers make a strict division of sectors difficult, it is possible to label the respondents to the consultations according to 21 broad categories (see figure 6.3).[41] The best-represented sectors were IT, healthcare, telecommunications, general business interest advocacy, data protection advocacy, credit and financial services, and marketing.[42]

[40] Citizen replies not included due to lack of information on country of residence.

[41] These sectors could also be labelled as policy subsystems (Sabatier, 1998) because most of them comprise actors from both the public and private sector.

[42] Data broker services could in many instances be included in the marketing category, but because these services are not used exclusively for marketing, it is better to keep them separated.

Figure 6.3 Replies by sector, 2009 and 2011 consultations.[43]



General business interests were represented by a large variety of national and international chambers of commerce, whereas consumer organisations, data protection officials, and NGOs represented citizen interests.[44] The findings further support Mahoney's (2007) conclusion that European firms and associations prefer formal coalitions to ad hoc ones. Most of the position papers were submitted by formal umbrella associations and business networks. Nevertheless, there were some signs of especially firms engaging in more loosely arranged networks. Some companies and organisations united under networks that could also be categorised as ad hoc coalitions, such as the Data Industry Platform, which comprises national direct marketing associations and some news publishers, Axciom, and commercial broadcasters. The most striking result is the significant increase in replies by

[43] The "Other" category contains replies by sole respondents of a single sector. The replies submitted by citizens are not included.

[44] The IT and data protection sector replies came from individual firms as well as business networks. Although quite a few law firms participated in the consultation, many of them did so on behalf of clients and it would therefore not be unfeasible to include them in the business advocacy category. However, because they did not always disclose who their clients were, I have decided to include them in the 'law' category.

specialised organisations or associations. Between 2009 and 2011, associations or firms which specialised in data protection increased by over 200%. It is also notable that a wider array of sectors was represented in the second consultation.

The data protection consultations are an example of how companies lobby EU institutions through several different associations and networks as well as in their own capacity. Microsoft, for example, participated through the European Privacy Association, Digital Europe, the Business Software Alliance, and AmCham,[45] to new a few, and in its own capacity.[46] Drawing final conclusions on these networks is difficult because not all associations or networks openly state their lists of members. A network analysis of the Transparency Register could shed some light on this question.

The wide range of sectors represented in the consultations further exemplifies how the use of data and, in particular, personal data has come to permeate the entire society. It confirms the theoretical considerations presented in chapter two, according to which the weight attributed to data-based decision-making in a range of different industries has become a fundamental part of modern bureaucracies, both private and public. The participation of different industries in the development of new regulatory instruments shows that the practices are often sought to be formally codified, and when such codification poses challenges or hurdles for increased datafication, such regulation will be resisted through lobbying decision-makers.

While industry domination was to be expected, the difference in the level of private interest participation compared with public interest replies was quite striking, which supports the elite pluralism paradigm. Although a wide range of sectors did participate, the position papers came, in most of the cases, from extremely resource-rich associations and firms and also from a limited number of countries, confirming Coen's (2007) critique. What is perhaps most disquieting is that some of the member states were represented in no capacity in either of the two consultations while organisations from three countries, the U.S., the UK, and Germany, put forth over a third of all position papers. Because a key argument for including stakeholders in the legislative process is the ambition to increase the representativeness of different societal groups

[45] According to Hayes-Renshaw (2009, p. 82), AmCham is regarded as the most successful interest group in Brussels.

[46] In 2014, Microsoft listed that it belonged to a total of 33 networks and associations in the Transparency Register.

and thus increase the legitimacy of EU policy (Schmidt, 2013), it can be argued that the public consultations on data protection were a failure in this regard.

However, if one approaches the question of legitimacy from a more input-oriented perspective, the goal is rather to make sure that a diversity of opinions is expressed according to the ideals of deliberative democracy (Kohler-Koch 2010; Quittkat & Kohler-Koch 2013). In that case, the slanted participation need not be a problem as long as the ideas raised by marginal actors are also taken into account in the legislative process. As such, the legitimacy of the process cannot be properly reviewed without also addressing the policy output. This analysis is dependent on a prior assessment of the views that were presented in the consultations. I will now turn to the concerns raised by the different stakeholders.

6.3 PARTICIPATION AS DIVERSITY

6.3.1 THE 2009 CONSULTATION

The mere categorisation of sectors or number of submissions to public consultations is a poor indicator of what issues are raised and to what extent these issues have been taken into account. Moreover, following Kohler-Koch's (2010) Habermasian perspective on including stakeholders for their contributions to the policy discussions and not for their level of representation, the central question is connected to the concrete input of the interest representatives. However, it would be fair to state that an issue raised by a wide degree of stakeholders has a better chance of making it into actual data protection legislation than concerns which are raised independently. After all, this is why strategic alliances are formed (cf. Sabatier, 1998).

Twenty three position papers from the 2009 consultation were selected for more detailed qualitative analysis (see Appendix 1).[47] The responses were approximately 10 pages on average, the shortest paper being only two pages while it was not uncommon for papers to span more than 30 pages.[48] Drawing on Bouwen (2002) and Klüver (2013), the papers were chosen after reviewing their relevance in terms of the access goods interest groups provide: policy expertise and sector-specific insights, size of enterprise or geographical reach, and citizen support. Following the results from the mapping of participants to the two consultations, it was clear that some stakeholders would be better

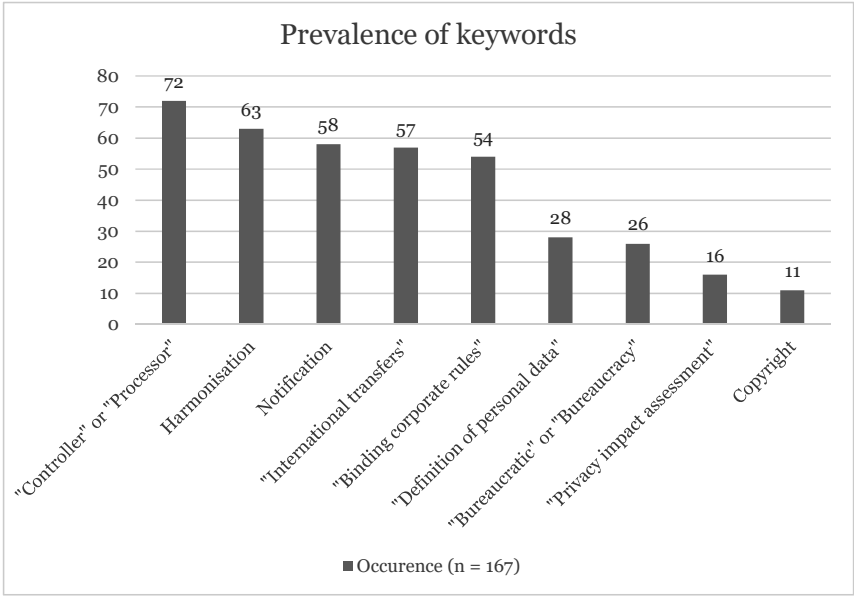
[47] Although the consultation deadline was 31 December, 2009, some of the replies were submitted in January, 2010.

[48] One individual even submitted an entire book to the consultation process.

represented than others and often lobbied through various business associations. Owing to these considerations, priority was given to so-called Eurogroups and umbrella associations representing a wide range of industries. The sample also included public authorities and civil society organisations.

The position papers reveal that there is wide agreement on the lack of harmonisation and specificity of the definitions in the original Data Protection Directive. These concerns unite all types of stakeholders. For example, the core definitions are too vague, even to the extent that the terms 'personal data', 'data controller', and 'data processor' are interpreted inconsistently across the member states.

Figure 6.4 The prevalence of data protection keywords in the 2009/10 position papers.



A quantitative analysis of the prevalence of certain keywords in all the position papers reveals three common trends: the ambiguity of definitions, a request for more harmonisation, that international transfers should be facilitated, and that the current framework seems bureaucratic.

However, the question of *how* they should be defined is tackled differently by free data lobbyists and privacy advocates. The definition of personal data takes two forms: for example, the broad and the relative approach. The former is supported by communication rights activists and data protection officials in Europe, whereas the latter is supported mainly by U.S. companies with

significant European presence. The broad approach to personal data was first presented in an advisory opinion by the Article 29 Working Party (2007). The advisory opinion provides an extensive analysis of how the Data Protection Directive's definition of personal data should be interpreted; to summarise, one could state that the broad approach suggests that data is personal if it is about a person or if this person is either identified in the data or reasonably identifiable by looking at the different data categories. The theoretical possibility of identification is not sufficient but determined by the resources which could be used for identifying a person behind the data categories.[49] Because the national DPAs also have the possibility of denying transfers of data, it is fair to say that the Working Party's opinions can be very influential within the EU data protection policy discourse. Several privacy advocates cited the advisory opinion in their submissions.

However, according to the relative approach, 'data is considered personal for someone who can link the data to identified individuals' (Appendix 1: AmCham, 2010, p. 7). In other words, if a marketer has access to a database with different consumer profiles but these profiles lack names or other clear identifiers, the data should not be considered personal. The relative approach has not been successful in shaping European data protection policy, but its existence shows that the vague definition provided by the Data Protection Directive can result in highly varying interpretations of what data may be processed and how. The public consultations provided interest representatives with an opportunity to suggest their definition of personal data. I will now proceed with presenting how these two types of interest representatives argued for more substantial privacy applications.

6.3.1.1 Free data lobbyists

Companies and business interest associations request, as a rule, more harmonisation across member states, fewer regulations on international transfers, and self-regulation instead of binding legislation, largely corresponding to the 'free data lobbyist' model presented in the previous chapter. Most of the suggestions relate to the procedural approach to personal data, which is largely perceived as 'bureaucratic'.

On an operational level, the procedural approach to privacy was heavily contested by firms and business interest associations, who rather seek to regulate data protection through self-regulation with some transparency

[49] For a more detailed description of the broad and relative approaches to personal data, see Hildén (2017).

requirements. While the underlying logic of the Data Protection Directive is largely challenged in the corporate position papers, the corporations rarely present a viable alternative to achieving a higher level of protection. The applications that these corporations favour are rarely connected to public interest goals. For example, a common position is the one presented by the Confederation of British Industry (Appendix 1: CBI, 2009, p. 3) that wants to limit access requests, claiming that they can place a 'significant burden' on businesses.

Whenever questions of public interest are raised, they usually relate to criminal activity, and the frames used are most typically associated with surveillance for security purposes (cf. De Landa, 1991; Lyon, 1994). The audio-visual industry representatives, including the Motion Picture Association and the International Video Federation, hold that privacy is necessary but that it 'should not be used to protect criminals or those who have been involved in illegal or harmful activities' (Appendix 1: MPA et al., 2009, p. 3). They claim the following:

> *At this stage there is a huge risk of forum shopping by rogue service providers and no enforcement of the rules against them. In other words, it seems easier for a rogue ISPs to hide behind/play with privacy rules rather than for legitimate users to protect their rights granted by existing laws.* (Appendix 1: MPA et al., 2009, p. 7)

What the audio-visual industry representatives are criticising in their reply to the consultation is, in fact, primarily the Directive on electronic commerce (2000/31/EC), which states that hosting service providers are neither responsible for the illegal content hosted on their servers nor are they required to monitor the content. However, because rights holders need to link IP addresses to illegal file-sharers to sue them for copyright infringement, data protection law becomes relevant as well. The approach taken by the copyright industries is rather belligerent and oppositional towards ISPs.

While the telecommunications industry was generally supportive of the measures that limit the scope of obligations of data controllers, they were equally eager to point out that the same level of obligations that telecommunications companies are subjected to through specialised legislation should also apply to online companies. On the contrary, while arguing that consumers demand targeted advertising (Appendix 1: Telefonica, 2009, p. 4), they simultaneously advocated for a 'level playing field' (Appendix 1: ETNO, 2009). In other words, competition regulation frames were used in the context of privacy regulation. Therefore, it is to some extent possible to simultaneously advocate for data maximisation and promote that procedural

obligations should be extended to other industries. Moreover, EuroISPA (Appendix 1: 2010) simultaneously argued that data retention for anti-terrorism purposes has 'eroded' the framework of data protection.[50]

Notwithstanding the concerns raised by telecommunications companies, there is a wide degree of interest overlap between corporations and governments. The problem multinational corporations face is that all countries have slightly different notification requirements, meaning that several different notification procedures need to be managed at the same time. Therefore, many firms either wish to abolish the notification procedure altogether or, at the very least, apply a 'home country rule' so that it would only be necessary to notify one DPA.[51] Regarding international transfers, many multinational corporations address the need to further develop 'BCRs', which are enforceable intra-group contracts stating that EU rules on data protection apply regardless of where the company's subsidiaries are situated. In other words, the rules are extra-territorially applied by way of contracts.

The Dutch government was very critical of the notification regime's effectiveness and state that the Netherlands will aim for compliance through self-regulation. In addition, the Dutch government and the UK Ministry of Justice stress the need for easier international transfers for law enforcement purposes. The approach is similar to that of multinational corporations, bearing in mind that the field in which the principles would be applied is quite different. One of the most important aspects of the big data paradigm is the ability to not only collect vast quantities of data but also use this data for any purpose that might emerge in the unforeseeable future (Lyon, 1994; Bogard, 2012; Christl, 2017). This position is routinely criticised by the privacy advocates and largely ignored in the corporate position papers. Data maximisation is routinely assumed to be the most beneficial mode of operation from a societal perspective, as exemplified by Acxiom's (Appendix 1: 2009) position paper that even included a case study explaining how transactional data are collected and processed across continents.

The coinciding interests of governments and multinationals correspond to Simitis's (1995) depiction of the Data Protection Directive's legislative process, where the governments of the member states effectively weakened the level of protection across the board to make sure that the rights of public authorities

[50] The Data Retention Directive (2006/24/EC) was still in force at the time, requiring telecommunications companies to retain communications metadata on all of their customers. The Directive would later be declared invalid by the CJEU in 2014.

[51] Axciom, AmCham, BSA, CBI, CIPL, Digital Europe, IAB, the publishers' associations ENPA and FAEP, Telefonica, Visa, ACRO, EuroISPA, EPOF, and the Dutch government. See Appendix 1.

to process data are not limited. In other words, the goals of surveillant administration and bureaucratic efficiency are adjoined with the business models of companies that rely on large-scale processing of personal data. It is also worth noting that the public consultations on data protection reveal an important aspect often ignored in interest group studies: that governments actively participated in the early stages of the policy-making process to influence the contents of the Commission's proposal. Their participation critically undermines the representativeness criteria and participation as diversity arguments for including interest groups in the decision-making process. The governments of the member states should not be part of the public consultations because they will have the possibility to make further amendments when the proposal is passed to the Council.

However, the research of Klüver, Mahoney, and Opper (2015) on frames suggesting that civil liberties frames are more prevalent when facing DGs such as DG Justice does not seem to hold in this case. The position papers in the present sample are more focused on their own needs and worries and more inclined to refer to the difficulties they face and the obstruction that procedural rules have to businesses; this corresponds to Cohen's (2016) claim that data protection regulation is seen as a hindrance to innovation.

6.3.1.2 Privacy advocates

The concerns raised by privacy advocates are generally less sceptical of the procedural approach and are more focused on increasing the self-determination of data subjects. Although the right to access one's own data was already ensured in the Data Protection Directive, civil society organisations argued that obtaining access in practice was complicated. European Digital Rights (Appendix 1: EDRI, 2009, p. 3) suggests that data controllers should '(i) indicate in an easily accessible and user-friendly way how long they store personal data, (ii) keep logs of each time personal data is being accessed or processed, and (iii) provide data subjects access to the logs pertaining to their own data'. On the topic of how data breaches should be communicated, the European Consumer Organisation (BEUC) proposes that the EU legislation should include a general obligation to disclose whenever there has been a data breach, a requirement which at the time of the consultation only concerned telecommunications companies (Appendix 1: BEUC, 2009, p. 18).

The most radical position is presented by Privacy International (Appendix 1: 2009) that criticises the way security frames have been used to advance exceptions to privacy laws, connecting government surveillance aims with

efforts to promote post-privacy positions in order to introduce more profiling of individuals:

> *The way policymakers regard users of social networking as though they have abandoned all hopes and expectations of privacy is the same way they described the need to promote mining, profiling, and retention after terrorist attacks. Two years ago proponents of reduced privacy spoke of privacy as standing opposed to the survival of a free Internet, just as we hear proponents of body-scanning technologies speaking of processing naked scans of passengers is necessary to the survival of the air-travel industry. Privacy regulations are said to be standing in the way of progress while policymakers focus on regulating for public security. (Appendix 1: Privacy International, 2009, p. 3)*

Privacy International also highlights that the primary focus of future regulation should be focused on the protection of information privacy rather than the relatively obscure language of 'data protection', a clear stand against the twin goal of data protection.

Nevertheless, the position papers reveal that public authorities have very different views on how data protection regulation should be applied in practice, even within the same country. The UK National Information Governance Board for Health and Social Care (NIGB) was one of the most outspoken critics of international transfers of data and data aggregation technologies that endanger the anonymity of medical information. The NIGB (Appendix 1: 2009, p. 2) proposes that the EU legislation would include four additional safeguards which are present in UK data protection law:

> *For person-level data which has been de-identified using pseudonymisation, the additional protections required include:*
>
> *an undertaking not to link the data provided with other person-level data which could render the data more identifiable;*
>
> - *Not to seek in other ways to render the information more identifiable;*
> - *Not to disclose the data onto other parties;*
> - *To provide a similar level of protection for pseudonymised data as would be given to identifiable personal data.*

The NIGB's position is focused on the procedural approach to privacy in a way which is reminiscent of Nissenbaum's contextual integrity model. Central to

Nissenbaum's (2010) thesis is the appropriateness of information flows. Addressing the specific issue of medical data, NIGB stresses the need to contain such data within the medical context. This position is also in line with Ohm's (2010) position that the biggest risks to the right to privacy are connected to the number of parties personal data are transmitted to.

The joint submission by the WP29 and the Working Party on Police and Justice (WPPJ), ambitiously named 'The Future of Privacy', was focused on both informational self-determination and procedural approaches. The submission highlighted that 'the challenges are immense' and that current developments 'may lead towards a more or less permanent surveillance society' (Appendix 1: Article 29 Working Party & WPPJ, 2009, p. 26). To empower data subjects, the two working parties suggest increasing transparency and enabling collective action. However, while empowering data subjects was seen as part of the solution, the approach is not really reminiscent of informational self-determination. Testimony to this is the scepticism expressed towards the applicability of consent as a way to ensure an appropriate level of privacy. Most suggested applications were concerned with requiring procedures and documentation to enable enforcement by the DPAs. Some applications were also directly related to the procedural safeguards that data controllers need to implement.

To summarise, aside for a few notable exceptions, operational principles were conspicuously absent in the position papers and were rather expressed indirectly by way of specific applications. These were frequently associated with the free movement of data and data maximisation. It shows that the inclusion of 'the free movement of data' in the title of the Data Protection Directive later enabled technical, applicational arguments to be used extensively when arguing for updates to data protection regulation. Given the uneven representation of stakeholders in the public consultation, the result is that far more concrete applications supporting the big data paradigm are suggested than the applications that would seek to enhance the protection of individual privacy. However, given the status of some of the civil society actors and public authorities, it is important to assess whether this imbalance had any concrete impact on the Commission's policy proposal.

6.3.2 THE CONSULTATION'S INFLUENCE ON THE COMMISSION'S COMMUNICATION ON PERSONAL DATA PROTECTION

Informed by the 2009 consultation, the Commission published a Communication in November 2010. The 20-page document served as an indication of what the final proposal for a new regulation would look like two

years later. Contrary to the positions presented by free data lobbyists, the Commission strongly favoured stricter data protection rules. While the Commission (2010a, p. 10) acknowledged the need for better harmonisation and less bureaucratic procedures, it did not support narrowing the scope of the Data Protection Directive simply because online business practices had become more surveillant in nature.

> *Basic elements of transparency are … particularly relevant in the online environment, where quite often privacy notices are unclear, difficult to access, non-transparent and not always in full compliance with existing rules. A case where this might be so is online behavioural advertising, where both the proliferation of actors involved in the provision of behavioural advertising and the technological complexity of the practice make it difficult for an individual to know and understand if personal data are being collected, by whom, and for what purpose. (European Commission, 2010a, p. 6, emphasis added).*

The concerns that have been addressed by representatives from several different industries seem to have had the most impact on the Communication. The notification procedure is an example of this. The Commission recognises the following:

> *There is general consensus amongst data controllers that the current general obligation to notify all data processing operations to the Data Protection Authorities is a rather cumbersome obligation which does not provide, in itself, any real added value for the protection of individuals' personal data. (European Commission, 2010a, p. 10, emphasis added)*

Throughout the document, references are made to the rights of citizens and obligations of data controllers. While there were clearly more lobbyists representing various business interests as noted in the previous section, privacy advocates were just as successful in their attempts to influence the Commission. This would confirm Coen's (2007) observation that cause groups may have privileged access to law-makers when their interests are aligned with the DG officials. For example, the right to be forgotten and data portability were only mentioned by BEUC, yet the Commission not only added these two concepts to the Communication but also gave them significant weight (European Commission, 2010a, p. 8).

Although some corporations sought to soften the current level of legislation by promoting stronger self-regulatory rules and procedures, the Commission responded by promising to examine the possibility of enhancing data controllers' responsibility by co-regulatory measures. Such initiatives include

making the appointment of independent data protection officers (DPOs) mandatory and including an obligation to carry out 'privacy impact assessments' before processing sensitive data (European Commission, 2010a, p. 12), both suggestions made by BEUC. Although the Commission failed to be explicit, it supported the accountability principle as a way to introduce more co-regulatory systems of control. Whereas the Data Protection Directive had required controllers to send fairly formalistic notifications to DPAs, the co-regulatory accountability principle sets out that controllers should be able to demonstrate exactly how they process data and for what purposes.

In other words, the accountability principle does not include any new obligations *per se* but aims to clarify the old ones. As the Article 29 Working Party (2010) explains, 'In sum, the new provision does not aim at subjecting data controllers to new principles but rather at ensuring de facto, effective compliance with existing ones'. Nevertheless, a move from notification obligations to an accountability regime is dependent on granting DPAs more powers to impose sanctions for efficiently enforcing data protection legislation. If DPAs are not strengthened, the accountability principle would likely weaken the privacy rights of citizens.

6.3.3 THE 2011 CONSULTATION: THE OPPOSING INTERESTS OF FREE DATA LOBBYISTS AND PRIVACY ADVOCATES

Whereas the 2009 public consultation sought answers to broad questions, 'what are the new challenges to data protection?', 'does the current framework meet these challenges?', and 'what would be needed to address them?', the 2011 consultation launched conjointly with the 2010 Communication, asking for specific input on the proposal. Owing to the increase in the number of submissions to the second consultation, I expanded the analysis to 44 papers mainly because a wider degree of sectors was included in the second consultation and I wanted to ensure that the most salient issues would be included. To complement the qualitative analysis, I used Boolean search strings to comb through the entire material for the keywords that appeared extensively in the papers.

As with the position papers submitted to the previous consultation, the length and detail of the position papers significantly varied. Some submissions followed the same structure as the Commission's Communication, whereas others focused on a much narrower set of policy issues. It may be noted that the position papers in the second consultation were notably more detailed and more extensive than the position papers in the 2009 consultation. Owing to the more concrete nature of the submissions, the papers in the 2011

consultation have been categorised in a more structured fashion with a greater focus on concrete policy proposals to trace whether the applications have also been included in the Commission's draft GDPR.

The analysis of the contents of the position papers allows me to put the different actors into three different categories with the twin goal of data protection as the basis for the categorisation. Drawing on Sabatier (1998), public and private actors are not categorised by their institutional status but by the position they wish to advocate (see table 6.3). As has been noted above, the categories do not indicate that all stakeholders within one group would be identical and equally concerned with the same issue. Instead, this division is an analytical tool to see the main reason for lobbying activity. Regardless, three actors were placed in the 'mixed approach' category because their position papers demonstrated a will to preserve the privacy of citizens yet at the same time facilitate data flows. Nevertheless, these entities are the exception, and most of the analysis is focused on determining how free data lobbyists and privacy advocates construct data protection and, in extension, the right to privacy.

However, it may be noted that of the entities analysed, only public authorities were present in all three categories. Bearing in mind that this is by no means a complete list of participants to the consultation, it appears that sector adherence is highly indicative of the stakeholder's position, regardless of how the entity is funded.

The division of actors according to the primary operational principles of data privacy or free movement of data provides an entry-level analysis of the motivations of the entities involved in the legislative process. However, it is important to look at how these actors address more applicational principles that relate to data protection. In table 5.3, I determined whether a certain applicational principle and its observed variables relate to the operational principles of informational self-determination or the procedural approach to privacy. I will use this operational division to assess the different proposals by the interest representatives.

Table 6.3 Interest representatives in the legislative process. [52]

Sector	Free data lobbyists	Privacy advocates	Mixed approach
Justice & Law	Ministry of Justice (UK)	CCBE	LV Ministry of Justice (LV)
		Bar Council of England and Wales	
Workers' rights		ETUC	
		UNI Europa	
Digital rights	Data Protection at Centre for Socio-Legal Studies, University of Oxford	Datainspektionen	
		EDPS	
		Privacy International	
		EDRI	
Consumer rights		BEUC	FTC
Healthcare	Johnson & Johnson		THL
IT	BSA		Symantec
	Microsoft		
	Digital Europe EGDF		
Advertising and marketing	IAB Europe		
	WFA		
	Data industry platform		
	EFAMRO and ESOMAR		
Finance and credit institutions	BBA and AFME		
	EBF		
Data brokerage	World-Check		
	EADP		

[52] Most of the abbreviated entities listed above are either international or European business networks, with some notable exceptions such as the European bar association (CCBE), the European Consumer Organisation (BEUC), the Federal Trade Commission (FTC), the Finnish national welfare authority THL and the European trade union ETUC. Please consult Appendix 1.

Insurance	CEA		
Retail	Carrefour		
Foreign Business lobbying	AmCham		
	DCSI		
	JBCE		
	CIPL		
	General Electric[53]		
Telecom	ETNO		
	EuroISPA		
Social media	Facebook		
Broadcasting	ACT		
	EBU		
	BBC		
Audio-visual industry & publishing	IFPI		
	MPA, IVF, FIAD & FIAPF (joint response)		
	ENPA & FAEP		
Aviation	IATA		

6.3.3.1 Free data lobbyists

Informational self-determination

The notion of strengthening people's privacy by empowering them with certain data-related rights is, as noted in chapter three, an integral part of informational self-determination or the self-managerial approach to information privacy. The Data Protection Directive already awarded users significant data-related rights in the EU, but these rights were often not respected.

For free data lobbyists, a regulatory framework which empowers users is highly undesirable. First, limiting data processing to situations where explicit consent has been provided may negatively impact the flow of information, thus actively limiting the number of information sources available and potentially

[53] As General Electric operates in several sectors it was difficult to assign the company to a specific sector. As the company wields significant economic and political power the general category of foreign lobbying was deemed appropriate.

challenging the quality of predictions. Second, these rights may introduce significant costs associated with putting systems in place that provide users with access and rectification rights, the right to be forgotten, and data portability. Third, especially dominant actors would be reluctant to allow for data portability because it would also be possible for users to more easily change to a competitor's service if all of their data could be easily transmitted to another service.

For example, the Business Software Alliance (Appendix 1: 2011) and Microsoft (Appendix 1: 2011) want to create separate rules for user-created and user-generated data that would require different levels of consent. While some of the free data lobbyists may accept that users should have some control over the pictures and texts they have uploaded to social networking sites, this would not extend to the data that is created in the course of their online activities. According to Andrejevic (2012), it is actually user-generated data that tends to be commodified and not the user-generated content, which should prompt legislators to limit the processing of user-generated data more and not less. The role of user-submitted data is marginal compared with the information that can be derived from web browsing or Facebook likes (cf. Kosinski, Stillwell, & Graepel, 2013). Moreover, the data a user generates is usually far more sensitive than the data he or she decides to upload.

A common strategy among free data lobbyists is to move away from user rights and instead focus on 'accountability' (addressed below under processing obligations). Yet, the actors that are most vocal in their support of introducing more accountability instead of prescriptive rules or more user rights also heavily object to the introduction of collective redress mechanisms which would make it possible for the civil society to initiate class action lawsuits.

The procedural approach to data protection

From a privacy perspective, the most important processing obligation is the principle of data minimisation, which in theory requires that processing of data should be limited to a specific purpose for a specific time period. For data-intensive industries, the whole idea of data minimisation goes against the supposed benefits of big data, according to which the processing of large data sets might lead to surprising insights that would be impossible to infer intuitively (Athique, 2018; Brown & Korff, 2009, p. 124; Pridmore & Zwick, 2011, p. 272; Zwick & Knott, 2009, p. 234; Hildebrandt, 2006, p. 548). Therefore, it is not surprising that the free data lobbyists are for a weaker application of the principle. However, how they choose to frame their viewpoint depends.

The World Federation of Advertisers (WFA) expresses that 'the quantity of data processed is not a problem in itself. On the contrary, the wealth of data available in the digital era is arguably one of the greatest assets of a dynamic digital economy' (Appendix 1: WFA, 2011, p. 4). The European Games Developer Foundation, on the contrary, repeats the 'post-privacy' paradigm as presented by Heller (2011) and Schramm (2012) and states that 'It is well known fact that younger European generations have a very different attitude towards what is private and what is not than older generations' (Appendix 1: EGDF, 2011, p. 3). Direct marketers and data brokerage companies express on their part that 'Businesses are using data for the benefit of the European citizens' (Appendix 1: Data Industry Platform, 2011, p. 7). Some, such as the airlines represented by the International Air Transport Association (IATA) (Appendix 1: 2011), cited other regulatory obligations. Others, such as the British Bankers' Association (BBA) and the Association for Financial Markets in Europe (AFME) stated that they are 'best placed to determine what personal data they need to keep and for how long, in light of their legal and regulatory obligations' (Appendix 1: BBA & AFME, 2011, p. 5).

The opposition to increase the transparency of data processing activities is not argued in terms of competitive disadvantages or unnecessary bureaucracy but with 'notification fatigue'. According to the free data lobbyists, users get tired from reading privacy notices and eventually stop reading them altogether if they are displayed too frequently (Appendix 1: Microsoft, 2011; CBI, 2011; Nokia, 2011; BBC, 2011). The description of notification fatigue resembles Nissenbaum's (2010, p. 36) 'transparency paradox', according to which privacy policies are less likely to be understood if they are detailed. Therefore, there is a slight change in tone compared with the previous consultation, where economic arguments were frequently used to motivate applications that favour industries. Similar reasons are cited when explaining why data breach reports should be limited to specific cases where users are at risk. The so-called risk-based approach is mentioned in AmCham's (Appendix 1: 2011) and EPOF's (Appendix 1: 2011) position papers, and some of its iterations can be found in several position papers by the representatives of the IT industry. According to the risk-based approach, users only have to be notified when there is a 'significant risk of harm' as a result of a data breach. If the data is encrypted or otherwise unreadable, the breach can be disregarded. Notwithstanding this argument, the free data lobbyists do not support introducing requirements to encrypt data because they are highly critical of any measures that might introduce technology mandates.

The wide use of public interest framing to advocate for limited procedural obligations supports the findings of Klüver, Mahoney, and Opper (Appendix

1: 2015) that revealed that interest groups tend to use public interest frames when addressing DGs with a public interest focus. However, the free data lobbyists are less diplomatic when explaining their support for abolishing the general notification obligation, describing the procedure as 'burdensome', 'bureaucratic', 'cumbersome', and 'useless' (see Appendix 1: DP socio-legal studies at Oxford, 2011).

Limiting bureaucratic record-keeping is also consistent with a general hostility towards public interference in general. This means that private corporations are generally quite sceptical of the instruments that grant law enforcement unfettered access to personal data. The most notable exception is the International Federation of the Phonographic Industry (IFPI) (Appendix 1: 2011) that wishes to limit privacy rights to enforce copyright and would therefore like to see that law enforcement had easier access to ISP data. This position is largely just a reiteration of what the copyright industries stated in the previous consultation. This particular concern sets the copyright industries apart from the online and telecommunications industries that, although generally in favour of intellectual property rights in the form of patents, are adamantly opposed of any enforcement provisions that require data retention or provide access to data for law enforcement purposes. Consequently, self-regulation is nearly always preferred over co-regulation or binding regulation. This might seem contradictory to the fact that big ICT companies want a Regulation to harmonise EU legislation. On a more applicational level, however, even the most multinational entities prefer self-regulatory initiatives. For example, while privacy by design[54] is universally supported, the free data lobbyists underline that the principles should not be binding or include technology mandates of *any* kind. The Interactive Advertising Bureau's(IAB) position is reminiscent of the 'surveillance-innovation complex' described by Cohen (2016), according to which any regulatory intervention is perceived to encumber innovation.

> IAB supports the application of privacy by design in internal processes, starting with educating developers about privacy. … Mandatory standards or measures would likely decrease this competitive element and 'lock down' innovation to a standard, which might increase privacy when it is adopted but might prevent more innovative solutions that would not be covered by that standard. (Appendix 1: IAB Europe, 2011, pp. 5-6)

[54] See chapter 3, subsection 3.1.3 and 3.3.

Second, free data lobbyists want to move away from a prescriptive, rule-based, ex ante regime to an ex post legal system guided by an *accountability principle*.[55] The Digital Europe (Appendix 1: 2011, pp. 15-16) lobby coalition provides an example of what this might entail:

> *[Accountability] can be summarised as 'the obligation and/or willingness to demonstrate and take responsibility for performance in light of agreed-upon objectives and as going beyond responsibility by obligating an organisation to be answerable for its actions'.*

The accountability regime was also mentioned in the submissions to the 2009 consultation. For free data lobbyists, the accountability principle was proposed as a way of substituting formal rules for international data transfers. While accountability as such is often supported, accountability that takes the form of liability and criminal sanctions for failing to respect data protection legislation is met with strong opposition. Nevertheless, Microsoft (Appendix 1: 2011, p. 15) supports the introduction of sanctions in the form of fines and cites the UK's Information Commissioner's Office (ICO) as a commendable example of a sanctions regime reserved for 'truly bad actors'. Facebook was issued the maximum fine of £500,000 for its role in providing Cambridge Analytica access to personal data. Whether Microsoft would be inclined to consider Facebook a truly bad actor is questionable.

However, in the Commission's 2010 Communication, the accountability principle was based on the Opinion of the Article 29 Working Party (Appendix 1: 2010, p. 3), which stated that 'a statutory accountability principle would explicitly require data controllers to implement appropriate and effective measures to put into effect the principles and obligations of the Directive and demonstrate this on request'.

Co-regulation proved to be a divisive issue among the free data lobbyists. Although there are many different kinds of co-regulation with various degrees of public involvement (see Marsden, 2011), the Commission's Communication presented a solution where controller obligations can be supplanted through the appointment of an independent DPO and notification regimes replaced with data protection impact assessments (DPIAs). For bigger corporations, the appointment of a DPO is not an issue, and many would appoint one without it being an explicit requirement. Smaller businesses and their representatives are generally supportive of limiting controllers' obligations through instating a DPO but heavily critical of the legal obligations to appoint one. Therefore,

[55] The accountability principle first surfaced in the Organisation for Economic Cooperation and Development's (OECD) privacy guidelines adopted in 1980.

the pressing question is when an entity's processing activities are so pervasive that the appointment of DPOs and DPIAs is mandatory. For example, IAB Europe (Appendix 1: 2011, p. 5) and World-Check (Appendix 1: 2011) support the mandatory appointment of DPOs and DPIAs but only for large controllers (without specifying when a controller is 'large'). Although there is a lack of consensus on whether DPOs and DPIAs should be mandatory, free data lobbyists wish that at least smaller companies should be exempt from this requirement.

While the interest representatives do demonstrate differences in their approaches especially regarding emphasis, it is quite remarkable that such a wide set of entities have curiously aligned interests. Data processing is as central to the operations of businesses as accounting practice – regardless of industry, the same questions arise and the same needs are expressed. BBC's (Appendix 1: 2011, p. 3) position even expressed that the original purpose of the Data Protection Directive was to 'encourage the free passage of information inside a single market, whilst protecting the data and rights of individuals' and expressed worry that 'the dual purpose has become obscured', effectively turning the priorities of data protection regulation on their head. While privacy is not directly opposed, it is clear that there is a fundamental incompatibility with privacy rights and maintaining the speed, variety, and complexity of information flows, which are an inherent part of the big data paradigm (Barocas & Nissenbaum, 2014; Kitchin, 2014).

It is only on the level of industry-related exceptions that free data lobbyists propose significantly different solutions, such as when publishers wish to retain journalistic exceptions to data processing, when bankers seek to clarify how their obligations to report financial crimes are compatible with data protection clauses, or how airlines should limit transfers of private information while still complying with various border control regimes and immigration policy. Nevertheless, it is also clear that the advertising and data brokerage industries are becoming increasingly reliant on surveillant technologies and generally demonstrate the most adversarial attitudes towards the measures that aim to increase the information privacy of citizens. Profiling restrictions and consent requirements are generally met with suspicion. There is also a different perception of how people relate to privacy: especially industries that rely on online advertising tend to have a transactional view of privacy, where information about oneself can be traded for a service that benefits them. The critique against this view of privacy and the numerous studies that have debunked this claim are routinely ignored (cf. Turow, Hennessy, & Draper, 2015).

6.3.3.2 Privacy advocates

The results from the previous section demonstrate why it is unlikely to find corporations among the privacy advocates. The retention, analysis, and transfer of personal information are so pervasive in all industries that more effective enforcement of data protection legislation unavoidably results in compliance costs. The privacy advocates in this sample are therefore professional associations in the form of one Pan-European and one national Bar Council, two European trade unions, the EDPS and the Swedish DPA, Privacy International and the European Digital Rights initiative (EDRI), and BEUC. The relevant sectors are law, workers' rights, digital rights, and consumer rights (see table 6.1 above). The EDPS opinion differs from the civil society organisations in that they clearly support the provisions that were envisioned to facilitate some data transfers. However, it would be a mistake to label the EDPS's approach as mixed because it is based on the realistic expectation that data transfers both happen and need to happen in an increasingly interconnected world. In contrast, Privacy International (Appendix 1: 2011, p. 3) questions the feasibility of having two conflicting goals (the protection and free movement of personal data), stating that 'the effectiveness of personal information protection and effective enforcement should be the prime and overriding objectives, while lessening administrative burdens, making transfers simple, etc. should come as secondary objectives, albeit desirable'.

Informational self-determination

Privacy advocates tend to favour informational self-determination and often push for more self-determination. A closer examination of the interest representatives presented above reveals that this is not always the case. Although one would expect Privacy International and EDRI to have the same opinions on most matters, their approaches are surprisingly different. Whereas EDRI saw user consent as the most important piece of the puzzle, Privacy International was somewhat sceptical towards the measures that are focused on user consent and instead encouraged direct intervention with dubious practices. Privacy International's position is therefore more reminiscent of the views taken by Gandy (1989), Obar (2015, p. 5) and Cohen (2016), promoting public oversight instead of individual agency. While EDRI supports the abolition of the general notification obligation, both Privacy International and BEUC support the notification procedure.

The diverging approaches could be explained by looking at their ideological foundations. EDRI can be conceived as a digital rights group that adheres to

libertarian ideals which stress personal autonomy. Privacy International, in contrast, represents a more social and liberal approach to privacy, where a strong DPA should protect the interests of the collective (cf. Venturelli, 2002, p. 76). Privacy International has historically focused broadly on the questions of surveillance, regardless of technology involved. In the consultations, Privacy International was more focused on the obligations of data controllers and the enforcement of rules and remained sceptical towards awareness-raising campaigns and that more explicit rules of consent would have a meaningful impact on the right to privacy of citizens. BEUC (Appendix 1: 2011, p. 10) had similar views and was largely in favour of the procedural approach to privacy instead of informational self-determination. They highlighted that people are rarely aware of what behavioural advertising is and criticise the initiatives that would put a 'disproportionate burden on users to protect themselves'.

The EDPS, Peter Hustinx, also contributed to the consultation, even though the EDPS has numerous other ways of affecting the outcome. The position paper spans over 36 pages and is a lot more explicit and detailed than most position papers. It is not possible to address all the questions that were addressed in the position paper, but one of the most important points raised was the need to place the fundamental rights perspective 'at the heart of the review process' (Appendix 1: EDPS, 2011, p. 34). Whereas his approach was clearly grounded in what is happening in the sphere of data processing, it was also highly normative. While the legitimate interests of businesses must be considered, the rights of users take precedence. For example, Hustinx advocated for data portability, additional rules for consent, and a collective redress mechanism (Appendix 1: EDPS, 2011, pp. 18-20).

The trade unions' submissions are quite unique to the process as they do not emanate from a perspective of consumption or citizenship but labour rights. Both of the trade unions in the sample underlined the importance of considering how data processing in the workplace affects worker's rights (Appendix 1: ETUC,[56] 2011; Uni Europa,[57] 2011), an issue that is often highlighted in the surveillance literature (see e.g. Dandeker, 1994; Gandy, 1989; Lyon, 1994).[58] They criticised the Commission for ignoring the question altogether in its Communication. Workplace communications surveillance is

[56] The European Trade Union Confederation (ETUC) represents most trade unions in Europe.

[57] Represents services workers.

[58] Seven trade unions participated in the Consultation – three from Austria, one from Germany and one from Sweden. The two trade unions selected for the sample are umbrella associations with a Pan-European reach.

not as commonplace in Europe as it is in the U.S., but there is a clear fear of U.S. practices extending to the EU as well. ETUC (Appendix 1: 2011, p. 2) was especially concerned with the blurring of work and private life, in part driven by technological change. Moreover, ETUC was concerned with employers forcing workers to accept workplace surveillance as a condition for employment. Both trade unions agreed that a collective redress mechanism should be instated.

The procedural approach to data protection

The privacy of citizens can also be enhanced through imposing obligations on whoever is processing personal information. The principle of data minimisation was fully supported by the privacy advocates, and they also addressed that data retention periods should be kept to a minimum. The EDPS even stated that data should have an expiration date (Appendix 1: EDPS, 2011, p. 19).

The processing obligations suggested by the privacy advocates can best be described as various requirements of 'privacy by default'. This is clearly reflected in Privacy International's (Appendix 1: 2011, p. 4) position paper, where they advocated not only for privacy by design but also for a 'maximum privacy by default'. Whereas privacy by design relates to how applications are programmed, privacy by default suggests how settings are calibrated.

How the different privacy advocates see the role of transparency also depends on if they primarily rely on data self-determination or the procedural approach to privacy. Transparency can be viewed from both perspectives: either as a requirement to log and demonstrate exactly how data processing takes place or as a requirement to communicate data processing practices when soliciting user consent. A sceptical take on privacy notices reminiscent of the 'transparency paradox' critique by Nissenbaum (2010, p. 36) need not indicate that transparency as such is irrelevant but that such information should never be directed at data subjects. The requirements to issue privacy notices were supported by the trade unions ETUC and UNI Europa and BEUC, but Privacy International was less enthusiastic. Privacy International (Appendix 1: 2011, p. 5) remained 'cynical', as the language of privacy notices had not improved significantly despite 'years of relatively fruitless discussions'. However, Privacy International fully supported mandatory breach notifications which are handled by DPAs.

Even the privacy advocates were positive towards the introduction of a statutory principle of accountability. However, they underlined that they wish to see it as an 'additional obligation' (Appendix 1: Privacy International, 2011,

p. 9). Thus, they agreed with the proposition to make the appointment of DPOs and DPIAs mandatory, with some threshold limits.

Therefore, the pressing question is whether the introduction of an accountability principle would exclude or include specific obligations for controllers and more powers for DPAs. Without a strong legal regime, the accountability principle would be a dead letter, and enforcement would be impossible if DPAs lacked resources and a mandate to issue meaningful sanctions. The privacy advocates were aware of this, which is why they supported the introduction of collective redress mechanisms, heavy sanctions, and fines for the controllers that fail to comply with data protection legislation in addition to privacy by design and default as explicitly recognised principles.

Because one of the main arguments of the privacy advocates was that DPAs should have more authority, it is revealing to look at the opinions of the Swedish DPA that would be directly affected by these amendments. On a general note, the Swedish DPA's opinions were highly in line with both the EDPS and the above-mentioned NGOs: DPAs should be able to issue stronger sanctions and have powers over data controllers as well as processors. They should also be able to represent individual data subjects in court (Appendix 1: Datainspektionen, 2011). The Swedish DPA agreed with EDRI that the notification obligation is unnecessary, highlighting that only an estimated 10% of all registers were even notified to the DPA.

The submission by the Swedish DPA reflects Klüver's (2013) proposition that interest groups seek to advance their own position in a rational manner, as the Swedish DPA aimed to advance its own powers yet reduce its administrative burden. However, the Swedish DPA also issued the need for 'simplified rules for the everyday processing of personal data' that is 'unstructured', citing the updated Swedish data protection legislation as a source. This particular amendment is not without its critics because it opened a loophole. Businesses have been known to store personal data outside of databases in 'unstructured' documents to avoid being subject to data protection legislation.[59] It is also precisely these kinds of national solutions that were cited as a challenge to full harmonisation.

After looking at both the procedural and self-managerial applications promoted by both free data lobbyists and privacy advocates, it is worth looking at some of the approaches that contain elements of both the camps.

[59] This information was provided during informal interviews with industry representatives.

6.3.3.3 Mixed approach advocates

It is telling that of the 44 position papers selected for closer analysis, only four could be labelled as 'mixed approach': the FTC's contribution, Latvia's Ministry of Justice, Symantec, and the Finnish National Institute for Health and Welfare (THL). They are in the mixed approach category because the positions they advanced can be both supportive of stronger privacy regulations and advocate for the free movement of data. However, it must be stressed that the four actors did not raise the same issues and have highly conflicting views in some areas.

Even businesses that are literally in the trade of protecting people's personal communications, such as Symantec, the security software company, are for the free movement of data. This is understandable, because Symantec is dependent on detailed information about possible computer viruses in order to be able to provide an effective service. On the one hand, Symantec (Appendix 1: 2011: 4-5) welcomed the proposition that processing should be more transparent, recognized access and rectification rights, and that there should be additional security requirements for entities that process children's data. On the other hand, Symantec (Appendix 1: 2011: 3, 7) was critical of narrowing the scope of legitimate grounds for processing without explicit consent and wanted to include a different category of data, 'attributable data', that would merit some protection but not to the same extent as personal data. This position can be traced to the U.S privacy law that makes a distinction between 'identifiers' and 'protected information'.[60] It also highlights the critique raised by Ohm (2010) that the European definition of personal data can expand almost *ad infinitum* owing to the increasingly sophisticated identification techniques, possibly losing track of what is truly 'personal'.

Latvia's Ministry of Justice (Appendix 1: 2011) was noticeably most concerned with retaining national exceptions to the general approach, but carefully supportive of strengthening the rights of individuals, citing the right to be forgotten as 'an issue that needs to be dealt with' and that strengthening the rules of consent should be reviewed, while critical of the need to expand the sensitive categories of data.

THL (Appendix 1: 2011), which processes large quantities of health-related data, was critical of access and rectification rights as well as expanding the role of consent – in many ways the opposite of Symantec, which was generally positive towards user empowerment and informational self-determination. THL stressed the need for exemptions for research purposes but was at the same time positive towards expanding the categories of sensitive data.

[60] The HIPAA Privacy Rule distinguishes between protected health information (PHI) and identifiers.

The FTC's contribution is one of the most interesting submissions of the entire consultation – a foreign consumer protection agency participates in a consultation on legislation which it will neither be subject to nor have any obligations to enforce, except indirectly through the Safe Harbor agreement. Their participation supports Slaughter's (2005) depiction of regulators as the new diplomats and Raab's (2010) argument that these networks are growing in importance. The FTC's position paper reveals that the Commission and the FTC had been meeting each other at regular intervals (Appendix 1: FTC, 2011). For example, the FTC (Appendix 1: 2011, p. 1) disclosed the following:

> *In July 2010, EC Vice President Viviane Reding (EU Commissioner for Justice, Fundamental Rights and Citizenship) and the Director-General for Justice, Françoise Le Bail, visited the FTC and met with FTC Commissioner Edith Ramirez, Bureau of Consumer Protection Director David Vladeck, and other FTC staff.*

This was only a few months before the call for the second consultation was initiated and the Commission published its Communication. Such a high-level, private meeting with a Commissioner and the DG Justice would not be accessible to most parties to the consultation. The FTC's position paper was neither nearly as extensive as the ones submitted by, for example, AmCham or Microsoft nor was it in agreement with the EDPS's submission. The duality comes from the FTC's mission to protect consumers yet at the same time promote competition. That can also entail ensuring that American companies are not overburdened by European legislation. Therefore, the goal of the FTC is to align the U.S. and EU data protection legislation – not to the extent that EU data protection legislation would be identical to U.S. legislation but to such a degree that the two would not be completely incompatible.

The FTC (Appendix 1: 2011, p. 4) supported the data minimisation principle and increased transparency and stressed that consumers need more choice mechanisms to opt-out of data processing. Furthermore, the FTC stressed that security breach notifications should be mandatory, highlighting that 45 states in the U.S. had passed legislation which requires breach notification.

Regarding access rights, the FTC was slightly more sceptical. Although generally supportive, the FTC (Appendix 1: 2011, p. 7) was 'mindful … of the significant costs associated with access'. The FTC would like to know whether companies should be able to charge for access, and while generally positive towards transparent processing, the FTC wondered whether companies should be required to inform consumers of the identity of the third parties with whom the controller has shared data and whether there should be a difference

between consumer-facing and non-consumer-facing entities. Moreover, the FTC stressed that the adequacy framework – which does not include the U.S. – has demonstrated 'significant shortcomings'. Instead, the FTC stressed the need for better enforcement cooperation globally.

Had the FTC been entirely focused on consumer protection, its submission would have been perceived as slightly odd – such an agency would not advocate for the possibility to charge users for realising their data protection rights and would not be wary of introducing more transparency requirements. Therefore, it must be stressed that the FTC has a dual purpose and that internationally, its role is not to promote the interests of American consumers but rather to make sure that American companies remain competitive also on a European market. This might also explain why the FTC has been quite reluctant to issue fines to big tech companies despite significant shortcomings in how especially Facebook has been processing data.[61]

6.3.3.4 Summary of positions: incompatible interests?

The free data lobbyists and privacy advocates have little in common in terms of how data protection legislation should be updated. One may conclude that the free data lobbyists are a much more diverse group; yet on the main topics, there is nearly full agreement. The privacy advocates are a lot more united in their approach, which can partly be explained by their similar *raison d'être*. A closer look at the positions advocated by the two camps has also revealed what a quantitative text analysis could not have – on a superficial level, privacy advocates and free data lobbyists might be in agreement, such as in their expressed support for an 'accountability principle', privacy by design, and the need to update definitions. However, closer analysis reveals that while the former expects the accountability principle to be an additional obligation and co-regulatory in nature, free data lobbyists see it as mostly self-regulatory. The same can be said of privacy by design. While both groups see an opportunity to update the main data protection definitions to their liking, there is rarely agreement on the contents of those definitions. For example, privacy advocates want consent to be explicit and are generally critical of other indicators of consent. Conversely, free data lobbyists are of the opinion that 'implicit consent' through continuing the use of a service, for example, is just as valid.

[61] In July, 2019 Facebook was finally issued a $5 billion fine due to various privacy violations (Patel 2019).

To conclude, while there is some agreement on the operational level – that a principled, technology-neutral omnibus approach is preferable to a more U.S.-oriented sectoral approach – there are fundamental disagreements on the applicational level. The disagreements are most pronounced in relation to the applications related to the procedural approach to privacy, where privacy advocates, both public and non-governmental, support more documentation and more transparency, whereas free data lobbyists would rather replace bureaucratic requirements with self-regulatory compliance measures. While updated legislation is an opportunity to lobby for more favourable legislation, it is also a risk that threatens the current ways of doing business and might entail significant compliance costs. Therefore, before turning to the question of influence, the question of what particular regulatory avenue to pursue should be addressed.

6.3.4 LOBBY POSITIONS ON CHOOSING A REGULATORY INSTRUMENT

One of the more important questions that the Commission faced when drafting the new Regulation was whether to update the regulatory framework by drafting a new Directive, drafting a Regulation, or simply relying on the existing Data Protection Directive and supplementing it with soft law measures.

It was clear from the outset that the Commission was going to update the regulatory framework and not only rely on policy instruments. The wording in the consultations was strong and the Commission does not launch public consultations unless it considers changing the law itself. However, the regulatory form it would choose was far from obvious. Although the Commission criticised the member states' divergent implementations of the original Data Protection Directive, the Commission refrained from stating what kind of legal instrument it would use in its 2010 Communication (European Commission, 2010a, p. 10).

The benefits associated with drafting a Regulation are obvious from a supranational perspective. A Regulation enters into force two years after the Parliament and the Council have agreed upon its contents, and a Regulation does not need to be transposed into the member states' national legislation. A Regulation guarantees harmonisation and is far easier to enforce than a Directive because there is no need to evaluate whether the national implementations match the original legal document. However, this also means that the drafting process of a Regulation can be protracted, as the member states want to make sure that the new law does not impede on their

sovereignty. This partially explains why it took the EU institutions four years to sign off on the new GDPR.

A Directive, on the contrary, will have to be transposed into the national legislation of each member state within one to three years, depending on the Directive. The Commission is vested with the task of ensuring that the Directive has been correctly transposed. Member states have only failed to transpose less than 1% of all Directives, which is a reasonable transposition rate according to EU goals (European Commission, 2015c). However, the original Data Protection Directive was significantly delayed in several member states (European Commission, 2016c).

Notwithstanding low non-compliance rates, Directives still grant member states a wider margin of appreciation than Regulations. Although many member states had transposed the Data Protection Directive into their legislation by 2002, closer analysis revealed significant differences between the national implementations (Korff, 2002; Löfgren & Webster, 2009). These differences led to an increasingly fragmented regulatory environment and a significant lack of harmonisation, resulting in highly bureaucratic notification schemes for multinational organisations and businesses. The choice of regulatory instrument bears with it significant consequences for data controllers. For this reason, it is imperative to examine interest representatives' positions on this issue.

6.3.4.1 A Regulation is necessary

The most avid supporters of a GDPR were international technology companies that wanted jurisdictional clarity and data privacy advocates. Although this particular overlap of interests might seem strange on the outset, global IT companies have been known to have aligned interests with some digital rights advocacy groups, most famously concerning copyright enforcement. [62] A similar tendency can be witnessed in the case of data protection. Whereas there would be wide disagreement on the actual contents of the new legislation, a Regulation would, first and foremost, harmonise the existing patchwork of national data protection frameworks so that these companies would only have to deal with one set of bureaucratic procedures.

Data privacy advocates have also realised that diverging rules within the EU in combination with transnational data flows leave citizens perplexed and confused as it is not clear which DPA one should turn to if there has been a

[62] For example, Google has frequently aligned with Internet activists in issues related to copyright enforcement, such as in the debates surrounding the controversial update to the Copyright Directive.

breach of data protection rules. Among the supporters of a Regulation, one can find the Business Software Alliance, Digital Europe, and AmCham, who all represent some of the most influential ICT companies in the world, the American pharmaceutical and medical devices multinational Johnson and Johnson, as well as the EDPS, the Bar Council of England and Wales, EDRI, and Privacy International. Although the ICT companies have the explicit goal of facilitating the free flow of personal data and the privacy advocates wish to minimise data processing and transfers, these groups can see the benefit of agreeing on a uniform standard.

The Commission would be more inclined to introduce a Regulation when politically feasible. By getting support from both the highly influential and financially important ICT industry and respectable privacy advocates, such as the EDPS and Privacy International, the Commission could argue that a Regulation had a wide basis of support that strengthened the legitimacy of their choice of legal instrument. After all, the entire purpose of introducing consultations to the legislative process is to gain legitimacy, and legitimacy cannot be gained with reference to a single interest group. By showing that parties on both sides of the spectrum can agree on a position would seem to demonstrate the deliberative character of the policy process (cf. Schmidt, 2013).

6.3.4.2 A Regulation would be counter-productive

The stakeholders who were mostly critical of proposing new legislation as a Regulation had different reasons for doing so. This group can be further divided into two factions, entities who believe that legislative reform is necessary and entities who wish to introduce light changes with soft law instruments.

The Latvian Ministry of Justice (Appendix 1: 2011) was, for example, supportive of a new Directive but concerned that a Regulation would impede on the nation's sovereignty to draft rules appropriate to the Latvian regulatory environment. The Data Protection Centre for Socio-Legal Studies at the University of Oxford (Appendix 1: 2011, p. 18) was seemingly critical of introducing 'a façade of absolute harmony' and instead favoured an updated Directive that is more concerned with establishing data protection principles rather than detailed provisions. Similarly, BEUC (Appendix 1: 2011, p. 14), otherwise supportive of radical data protection measures, advised against a Regulation because it 'would make the resulting rules less flexible, while it may compromise the legislation of those Member States where data subjects enjoy a high level of protection'.

The actors who were reluctant to admit that a new Directive was necessary can be broadly categorised as companies who have benefitted from legal uncertainty in the past. These include the BBA and AFME, national direct marketing associations, publishers and digital marketers, Axciom, one of the world's largest data brokerage companies, as well as IFPI, the global recording industry representative. The finance and banking associations were unwilling to be subjected to yet another set of limiting rules. The marketing professionals undoubtedly realised that a new Regulation would introduce more restrictive rules regarding the processing of personal data for advertising purposes, as the Commission was outspokenly critical of especially behavioural advertising in its 2010 Communication. Thus, any updated legislation would impact the advertising industry negatively. IFPI, on the contrary, feared that an updated and strengthened data protection law would make it more difficult to gather evidence for legal claims against copyright infringers.

6.3.4.3 No opinion / Neutral

Apart from these clear positions for and against a Regulation, influential actors from other sectors, such as EBF, the French retail giant Carrefour, and the European trade union UNI Europa, were fairly unconcerned with the legislative instrument but instead focused on the contents (or lack of) in the Commission's proposal. Interestingly enough, the EBF and the BBA seem to have diverging opinions on this particular issue, where the BBA is against the introduction of new legislation and the EBF welcomes increased harmonisation. Many stakeholders who participated in the consultation accepted that the data protection framework would be updated but chose not to meddle in the political issue of what type of law to put forth.

6.4 INSTITUTIONALISED DELIBERATION OR MERE LIP SERVICE?

The quantitative categorisation of the submissions to the two public consultations clearly demonstrates how formally open public consultations still lead to unequal participation. The public consultations favour resource-rich associations and firms, and although this does not preclude other actors from participating, civil society participants are in the clear minority. As the throughput legitimacy of legislative processes is reviewed based on whether interest representatives sufficiently represent different societal actors, one can conclude that the GDPR's public consultations did not fulfil this function.

Whether Schmidt's (2013) ideal throughput legitimacy is achievable on the EU level is also questionable. Business entities are directly affected by data protection regulation and will always be more attentive to regulatory change than regular citizens who adapt to the regulatory environment. Civil society organisations that operate within the sphere of communication rights will never be able to muster the same resources as businesses. Therefore, it is not plausible that civil society organisations would participate to a much higher degree than what they already have. To guarantee more balanced participation, one would instead need to restrict business entities' access to public consultations. That might also prove problematic from a democratic point of view.

If one considers the role of public consultations as a platform for deliberation rather than an avenue to increase political participation and ameliorate representation, the public consultations are perceived in a slightly more positive light. The public consultations have allowed a diverse set of actors to raise issues connected to how data protection regulation will impact practices and rights. Nevertheless, regardless of the diversity of actors, the positions are highly similar on an operational level. The position papers demonstrate that most interest representatives adhere to either of the two operational goals of data protection: free movement of data or protection of individuals. Supporting one of the two goals generally indicates what applicational instruments an interest representative is eager to support. However, whether data protection should be achieved through procedural requirements or informational self-determination set some interest representatives apart.

While free data lobbyists rarely approve of any sort of legally binding procedural obligations, they can, at times, approve of some self-managerial instruments connected to the notions of 'implicit consent' and self-regulatory transparency initiatives. It is understandable that corporations choose to advance the informational self-determination approach to privacy. Even though some aspects of the approach might make operations slightly more difficult for corporations, they can rest assured that the vast majority of people will do nothing in accordance with the so-called privacy paradox. Nevertheless, this means that business lobbyists are very wary of class-action redress and sanctions that privacy activists might use to their advantage because a few individuals could potentially cause a lot of harm. Therefore, the rights are rarely backed up by meaningful sanctions in the free data lobbyists' proposals. The interests of free data lobbyists and privacy advocates are largely incompatible and only superficially overlap.

These stark differences in the positions are not easily balanced. The public consultations clearly fall short of democratic deliberation because they do not provide any interaction between the parties (Quittkat & Kohler-Koch, 2013, p. 181). Rather, they are instrumental in increasing the diversity of opinions and concrete applications, contributing to a more diverse set of policy input. However, that input is meaningless if it does not translate into policy output. The 2010 Communication showed that some actors have been influential in introducing key concepts, but the biggest question is whether this influence has been transposed into the actual Regulation. The following chapter will examine the different versions of the EU institutions and compare the regulatory output with the regulatory applications favoured by the different interest representatives.

7 INTEREST REPRESENTATIVE'S INPUT AND POLICY OUTPUT

After presenting the way interest representatives were institutionally included in the early stages of the GDPR's legislative process and analysing how their positions differed, I now move on to the main purpose of this study: the question of influence. To what extent can the influence of interest representatives be traced down to actual regulatory initiatives in the sphere of data protection law? It is a study of how the right to privacy is operationalised and whether the codification of data protection is characterised by the suggestions made by industry lobbyists and privacy advocates. The following are the research questions presented in the introductory chapter:

3. What policy alternatives were put forth by the EU institutions in the course of the GDPR's legislative process, and how did they correspond to the ideas, issues, and frames promoted by interest representatives?

4. What does the influence of organised interests and stakeholders in GDPR decision-making reveal about the democratic legitimacy of the process?

The answer to the first research question is therefore indicative of the second. The policy output under study includes the following documents:

1. the Commission's Proposal for a General Data Protection Regulation (2012);

2. the European Parliament's first reading (2014);

3. the EU Council's adopted version (2015); and

4. the finalised Regulation (2016).

The first step is to elaborate on the contents of the Commission's original draft, on which subsequent iterations are based. This draft is compared to the interest representatives' position papers. The second step is to address how the Parliament's and the Council's versions differ from the Commission's original and whether these amendments can be traced back to the positions promoted by lobbyists and advocates during the public consultations. Finally, I will conclude by discussing the impact of the compromise, the final GDPR.

7.1 THE COMMISSION'S ONE-STOP SHOP AGENDA

7.1.1 PROBLEMS AND POLICY OPTIONS

DG Justice published its proposals for a GDPR and a Directive on the processing of data related to law enforcement on January 25, 2012. Because introducing new data protection legislation through either a Regulation or a Directive would be either politically difficult or ineffective from a supranational standpoint, the Commission settled for a dual approach. Private and public routine processing of data was to be covered by a Regulation, whereas the rules governing the protection of personal data in the realm of law enforcement would be confined to a Directive. As the above analysis demonstrates, the decision to put forth a Regulation instead of a Directive was openly supported by quite a limited group of stakeholders, but these interest representatives were also the ones who would be needed for the Commission to be able to demonstrate that the new initiative had both the industry's support and were on the side of the communication rights' activists. Through promoting two separate regulatory instruments, one for routine data processing and another for law enforcement, the Commission also managed to avoid the politically fraught issue of appeasing the governments prone to use surveillant technologies without simultaneously completely eroding the right to privacy.

The underlying political considerations are impossible to miss. Whereas it was clear that the Commission preferred a Regulation, it would have been challenging to get the member states to sign off on a Regulation that also covered law enforcement. By dividing the new law into two separate legal instruments, the Commission was thus able to steer clear of a head-on collision with the governments of the member states and yet maintain a higher level of harmonisation regarding other forms of data processing. It may be noted that while the UK Ministry of Justice (Appendix 1: 2011) did not explicitly suggest a specific legislative instrument in its position paper, it did suggest that law enforcement should be covered by a separate law.

The proposals were accompanied with a comprehensive market impact assessment report. The report outlines different policy options for addressing the two objectives of data protection: (1) enhancing the internal market dimension of data protection and (2) increasing the effectiveness of data protection rights.

In the market impact report, the Commission engages in the framing of data protection policy responses. Following van Hulst and Yanow's (2016) typology of framing, the Commission had used the public consultations and

the EU-wide study on data protection to make sense of the issue, whereas the market impact report was used to select which issues to focus on and then to name and categorise them. The market impact report lists three problems associated with data protection. The first problem relates to the internal market dimension. According to the Commission, there were '[b]arriers for business and public authorities due to fragmentation, legal uncertainty and inconsistent enforcement' (European Commission, 2012b, p. 11). The impact assessment stated that legal fragmentation costs businesses almost €3 billion per year, which is about half of the overall administrative burdens that were linked to the Directive (about €5.3 billion) (European Commission, 2012b, p. 19). Therefore, unharmonised data protection law is seen as a barrier to data trade – a very clear economic framing of the issue.

The second problem relates to the goal of protecting citizens' data protection rights. Simply put, there are '[d]ifficulties for individuals to stay in control of their personal data' (European Commission, 2012b, p. 21). The Commission noted that cloud computing and international data transfers make it increasingly difficult for citizens to stay in control. At the time, the use of software services was starting to be increasingly connected to servers as fewer of the functions were performed locally. Furthermore, the Commission justifies a new Regulation with reference to the 'privacy as control' conceptualisation, which has been influential in the privacy literature (see Nissenbaum, 2010; Westin, 1967). The Commission cited the Eurobarometer survey from 2011, according to which 'Two thirds of European citizens feel that the disclosure of personal data is a major concern for them and six in ten citizens consider that nowadays there is no alternative to disclosing personal data in order to obtain products and services' (European Commission, 2011b, p. 22). This problem is associated with both the privacy paradox (Utz & Krämer, 2009) as well as the resulting feelings of resignation (Turow, Hennessy, & Draper, 2015).

The problem description goes on to list the concerns related to the complexity of privacy notices, the difficulties associated with exercising rights, citizens' unease with behavioural advertising, data breaches, and the general aggregation of online activities and location information which can lead to the identification of individuals (European Commission, 2012b, pp. 21-28).

> *Many of the fundamental freedoms can only be fully exercised if the individual is reassured that it is not subject of permanent surveillance and observation by authorities and other powerful organisations. … Where the individual suspects that his or her interactions are subject of surveillance, collection and analysis by authorities, service operators or others, it loses partly the possibility of exercising some fundamental rights. This chilling effect can already be caused by the perception of*

> *surveillance, which may or may not exist. The lack of transparency of processing and of accessible means to effectively enforce data protection rules is therefore directly affecting individuals' fundamental rights.*
>
> (European Commission, 2012b, p. 30)

The quote shows that the Commission is highly aware of the risks associated with the increasing processing and aggregation of data from a wide variety of sources. The Commission uses public interest frames to address these concerns and refers to citizens as individuals. The 'chilling effect' that the Commission refers to is reminiscent of the disciplinary effects of Foucault's (1977) panoptic diagram. Where such an effect might be laudable for some (like the copyright industries), surveillance in the online sphere also creates uncertainty which can be an obstacle to the growth of ecommerce. The Commission states that consumers' lack of trust in service results in a slow uptake of audio-visual services and reluctance of consumers to shop online.

> *The 75% of individuals currently not feeling in complete control of their personal data on social networking sites (and 80% when shopping online) is not likely to decrease without regulatory intervention which can support the confidence of individuals. Such a development could counteract the key performance target of the Digital Agenda for Europe for 50 % of the population to buy online by 2015."*
>
> *(European Commission, 2012b, p. 37)*

It is worth noting that the main issue does not seem to be privacy concerns but the economic consequences of the uneasiness that online surveillance contributes to. The position confirms the critical accounts on data protection regulation that argue that the fundamental rights perspective is often lost (cf. Burkart & Andersson Schwarz, 2013). It also shows that the focus on the economic ramifications of policy that has dominated European media policy (Harcourt, 2005, p. 199; Hirsch & Petersen, 2007, p. 31) is equally noticeable in this policy domain.

The third problem relates to 'Gaps and inconsistencies in the protection of personal data in the field of police and judicial cooperation in criminal matters' (European Commission, 2012b, p. 31). This problem lies outside the scope of this study, but it is clear that this particular issue also impacts citizens and companies to a great extent. This problem was subsequently included in the third objective of the EU data protection legislation: 'To establish a comprehensive EU data protection framework and enhance the coherence and

consistency of EU data protection rules, including in the field of police cooperation and judicial cooperation in criminal matters' (European Commission, 2012b, p. 43).

The Commission proposed three policy options to address these problems. The first policy option was focused on strengthening self-regulatory measures, introducing technical tools, and increasing the coordination of national DPAs (European Commission, 2012b, pp. 63-64). It is clear from the outset that the Commission did not support this policy option. While it acknowledged that citizens would be slightly more aware of their rights, the Commission was sceptical of this option's positive impact on fundamental rights. Furthermore, while self-regulation could provide additional legal certainty for data controllers, national member states would still interpret rules in a divergent manner, resulting in more costs for businesses.

The second policy option contained legislative amendments that would reduce the room for the manoeuvre of member states and specify how key definitions should be interpreted (European Commission, 2012b, pp. 65-71). The Commission stated that it would be possible to draft both a Regulation and a new Directive, but a Directive could lead to 'gold-plating' by the member states, meaning that the extent of the rules and obligations under the Directive could be extended when the law is transposed into national legislation. The second option was focused on accountability in its co-regulatory sense, as the DPAs' powers are strengthened and they would be able to issue sanctions. In addition, larger organisations would be required to appoint DPOs and issue data protection risk assessments. This approach also included the creation of a 'one-stop shop', where controllers would only need to deal with one DPA despite having operations in several member states.

One important addition to this approach is the inclusion of 'delegated acts', which mean that the Commission can specify implementing measures with binding obligations. The Commission directly referred to the benefits of this approach by stating that privacy by design principles is unlikely to have a significant impact unless the Commission can draft some additional binding obligations (European Commission, 2012b, p. 70). This is partly reflective of the positions held by many privacy advocates, with the exception that these did not advocate for enforcement by the Commission but by national regulators.

According to the Commission (2012b, p. 70), the proposed measures in second policy option would lead to net savings of around '€2.3 billion per annum, arising from the elimination of legal fragmentation and the simplification of notifications'. Although the Commission only briefly mentioned the impact the clarified definitions will have on citizens, they

claimed that these measures would strengthen 'several individual fundamental rights'. While the second policy option seems to include several new obligations, the argument goes that the removal of notifications and other 'red tape' would result in significant savings for companies. Although it would seem that risk assessments and appointing DPOs would be quite expensive, the Commission's calculations in Appendix 6 seem to prove the opposite. However, these calculations are based on surmised assumptions that 90% of larger companies had already appointed DPOs.

The third policy option goes further than the second and includes more detailed rules for different sectors, new categories of sensitive data, and consent as the basis for all processing (European Commission, 2012b, p. 71). In the third option, an EU Data Protection Agency would be established and notification obligations would be completely removed. It also included a collective redress mechanism and criminal sanctions for data protection breaches. While the Commission noted that this approach would 'maximise harmonisation', it is clear that the Commission did not support it. First, too much detail in the legal document would possibly lead to more non-compliance and confusion. Second, an EU Data Protection Agency would be expensive. Third, it would be too 'inflexible' for national circumstances and possibly hinder law enforcement to complete their tasks.

The first and third policy options are purposely unrealistic versions of the policy proposals made by businesses and civil society. While the goal of introducing the first policy option is to show free data lobbyists that they have considered self-regulatory measures, they want to stress that this option would not significantly reduce administrative costs. Similarly, the third policy option is presented as something admirable yet unachievable. Thus, the only logical conclusion is to support the second policy option; however, to provide an illusion of deliberation, the Commission included some elements of the first and third options in their 'preferred policy option'. From the first policy option, the Commission included awareness-raising and new self-regulatory measures. The Commission also removed the notification requirement entirely from its preferred option, similar to the third policy option. Most of the other approaches in the third option were ignored. One of the options that were heavily supported by civil society was collective redress in the realm of data protection. The Commission acknowledged the benefits of collective redress but did not wish to include joint judicial remedy until there are general EU rules on the subject.[63]

[63] At the time of writing, in October 2019, those rules were still being debated.

Why the Commission would go to such lengths explaining different alternatives is perplexing from a legitimacy perspective based on policy output. As the Commission is free to draft laws regardless of what interest representatives say, it does not need to explain why it does not advocate for different approaches and only needs to show why the chosen approach is suitable for the problems that the new law aims to address. Therefore, the Commission knowingly departs from an output legitimacy perspective, instead acknowledging the deliberative aspects of the policy process. Therefore, the goal of presenting different policy options seems to have been to demonstrate that the public consultations are an integral part of the policy process by way of deliberation contributing to the legitimacy of the Commission's decision. To this end, Grossman's (2004) critique that the Commission merely uses stakeholders in an instrumental fashion does ring true, as very little would indicate that the preferred policy option would be a result of true deliberation.

Similarly, the calculations that serve as a basis for the market impact assessment are the products of behavioural confirmation. While legal fragmentation undoubtedly results in more red tape, the costs that the Commission associated with DPOs and DPIAs seem wildly optimistic. Nevertheless, the focus here is not to assess the feasibility of the Commission's calculations. I shall now turn to the Commission's proposal and demonstrate where there are traces of interest representatives' suggestions.

7.1.2 TRACES OF INTEREST REPRESENTATIVES' PROPOSALS IN THE COMMISSION'S DRAFT

The proposed Regulation does not depart radically from the Data Protection Directive, but rather it clarifies many unclear provisions. Provisions, which do not significantly differ from the old laws, are more a sign of path dependence than examples of influence by the actors who benefit from the status quo. Nevertheless, one significant change is the weight given to the right to data protection. The right is included both in the Lisbon Treaty[64] and in Article 8 of the Charter of Fundamental Rights of the EU. Thus, since the adoption of the Data Protection Directive, data protection has been elevated to a fundamental right. Another significant change was the added complexity of the new Regulation. Whereas the original Data Protection Directive contained 72 recitals and 34 articles, the proposed GDPR contained 139 recitals and 91 articles. While the underlying goals did not fundamentally change and one can

[64] Article 16(1) of the Treaty on the Functioning of the European Union (TFEU).

therefore view the GDPR as path-dependent, the wide-ranging additions to the GDPR suggest that path-dependence is an insufficient explanation.

Following the structure of the previous section, I will go through the proposed changes related to informational self-determination and the procedural approach to data protection. Because the scope of the proposal is much wider than what was presented in any of the position papers, it would be impossible to review the entire proposal as thoroughly as the lobby papers. Thus, my attempt is not to assess each and every article and recital in the proposal but to create an overview of its most important elements in the themes already presented above.

7.1.2.1 Informational self-determination

The Commission clearly wanted to clarify the rights of citizens and did so by introducing several explicit principles that were perhaps only tacitly recognised by the old Directive. One of the most important additions to the new Regulation was the inclusion of a requirement of 'explicit' consent. In the Commission's (2012a, p. 8) own words, 'the criterion "explicit" is added to avoid confusing parallelism with "unambiguous" consent and in order to have one single and consistent definition of consent'.

Whether consent should be explicit was one of the most important questions in the interest representatives' proposals, which clearly distinguished free data lobbyists from privacy advocates. It is important to note that there were far more lobbyists who wished to omit any reference to explicit consent and even include 'implicit consent' as a valid way of obtaining a data subject's permission. This particular amendment shows that the Commission was not swayed by the arguments of free data lobbyists.

Enshrining consent as a founding principle for the processing of personal data can be directly related to the two mechanisms that form the core of the information privacy highlighted by privacy scholars: the questions of access and control (Nissenbaum, 2010; Westin, 1967; Reiman, 1976). Through consent, citizens exercise control over their own data. In theory, the data minimisation requirement that data should only be collected for a specific purpose should strengthen the informational self-determination of citizens because access to data is then decided on a case-by-case basis. In practice, this is rarely the case, and citizens are only left with a control mechanism that allows them to determine who will act as the gatekeepers of access. In many cases, privacy policies look more like a carte blanche than meaningful consent.

The notion of explicit consent is heavily associated with informational self-determination. It presupposes that whenever an issue that is important for the

data subject arises, they should be able to make an informed decision and choose accordingly. Nevertheless, the approach is fundamentally misguided because the choice is often between accepting privacy invasive collection of personal data and complete refusal that might result in unwanted social or economic consequences (Gandy, 1989).

This inherent weakness of consent was partly recognised by the Commission (2012a) in the Recitals 32 and 34 of the draft GPDR, which state that 'consent does not provide a valid legal ground where … [there is] no genuine and free choice' and that consent is not a 'valid legal ground … where there is a clear imbalance between the data subject and the controller', for example, between an employee and an employer. This last addition is remarkable considering the trade unions' concern that data processing in the employment context was not taken into account in the Commission's 2010 Communication. More specifically, ETUC[65] was concerned by the possibility of employees being forced to consent to workplace surveillance. Under the draft GDPR, such surveillance would not be permissible with reference to consent. This paternalistic approach to consent, while slightly detached from informational self-determination, is representative of the EU's liberal market tradition (see Venturelli, 2002). Instead, such provisions require a strong public authority that can efficiently enforce the rules. Thus, the Commission's proposal has a procedural character to the consent mechanism as well, as data controllers would need to provide evidence that consent was freely given.

Although the Data Protection Directive did contain significant data subject rights related to access and rectification and the right to object, these rights were rarely respected (Norris, de Hert, L'Hoiry, & Galleta, 2017). The draft Regulation consequently detailed exactly what the right of access entailed and introduced the new right of erasure (Article 17) and right to data portability (Article 18). The right to be forgotten was later famously upheld by the European Court of Justice in Google v Costeja González, which set a precedent for requesting search engines to delete search results. Nevertheless, at the time of the draft Regulation, the right to be forgotten did not exist, and the explicit right was in fact wider in scope than what could be deduced from the court's decision. The origins of the right to be forgotten and the right to portability are all the more interesting; they were introduced in the 2010 Communication after having surfaced in the position paper by BEUC in 2009. In 2011, the right to be forgotten was addressed by over 100 interest representatives and portability by over 60, often in negative terms.

[65] The European Trade Union Confederation.

One of the more ambiguous elements of the previous Data Protection Directive was the lawfulness of processing according to the 'legitimate interests' of the data controller. What those interests might be were not clearly defined in the instrument itself, and the Article 29 Working Party (2014) did not address the question until 2014. Although the Commission strengthened the rights of users, 'legitimate interests' remained a valid ground for processing in addition to user consent in the draft Regulation. These legitimate interests may even override the right to object to processing as long as the controller can demonstrate that the interests or fundamental rights and freedoms of the data subject do not override the legitimate interests.

Although this leaves data controllers with quite a bit of leeway, the Commission introduced some safeguards regarding the protection of children and more specific transparency requirements so that the data subject would at least be aware of what these legitimate interests are (Recitals 38 and 56). Furthermore, the Commission empowered itself to introduce 'delegated acts' which would further specify acceptable legitimate interests. The validity of using legitimate interests as grounds for processing were not really questioned by the privacy advocates, but the free data proponents generally underlined their importance. The inclusion of legitimate interests as a legal ground for processing further exemplifies that the Commission's approach to privacy is very detached from the ideas of control despite what was said in the impact assessment report. Therefore, the impact assessment can be judged as primarily a rhetorical framing device, although it was also used to inform the action frames. It is equally obvious that Reiman's (1976) privacy-as-access is more reminiscent of the internal logic of the draft GDPR. That approach is easier to reconcile with the dual goal of data protection, to both share data within the Union as well as protect it. Nevertheless, a strict reading of the provision requires documentation that proves that a data controller has carefully balanced the fundamental rights of the data subjects, further underlining the importance of the procedural approach in the Commission's draft.

Much to the detriment of privacy advocates, the Commission did not include collective redress in the proposal, the reasons which were outlined in the accompanying impact assessment. This was perhaps one of the more important victories for the free data lobbyists. Judicial collective redress could be a potent tool for addressing privacy issues – questions of data protection are highly complex and require expert knowledge, and any misconduct is likely to affect a large number of people. If NGOs and other privacy advocates could lodge class action lawsuits against companies, it could carry significantly more weight than any fine or sanction issued by a DPA. In 2013, the Commission

issued non-binding recommendations on collective redress (European Commission, 2013), but the issue has not really developed since then. Some countries include collective redress mechanisms in cases that involve consumer protection, which could arguably also cover data protection issues. The Commission did, however, include the right to lodge a complaint to a DPA on behalf of a data subject, thus potentially triggering administrative fines.

7.1.2.2 The procedural approach to data protection

The most ambitious parts of the draft Regulation are concerned with the obligations and responsibilities related to data processing. While many of the principles were at least in part present in the original Directive, the draft Regulation promises stricter principles of data minimisation, a clearer purpose limitation, and more transparency. Where the Article 6(1)(c) of the Directive stated that data should be 'adequate, relevant and not excessive', the draft proposal required that it must be 'adequate, relevant, and *limited to the minimum necessary*' (emphasis added), in direct contrast to the data maximisation aspirations of free data lobbyists.

These principles were further outlined in Article 23 which lays down the provisions concerning 'Data protection by design and by default'. While the concept of privacy by design was almost universally supported as a non-binding measure by the participating stakeholders, the Commission decided to follow the recommendation by privacy advocates such as the WP29, Privacy International, the Bar Council of England and Wales, BEUC, and EDPS to make privacy by default a binding obligation. As noted above, the foundational principles of privacy by design had been introduced to the data protection policy community by the Canadian privacy commissioner of Ontario, Ann Cavoukian, and by the time of GDPR's proposal, they had received widespread recognition. Cavoukian herself submitted a position paper to the consultation, which might be perceived as a little odd: why did a regional Canadian privacy commissioner want to participate in the development of EU law? One explanation is the desire to promote a policy concept she herself had coined.

Nevertheless, strengthening the default element of privacy by design was new. The introduction of this explicit principle is in stark contrast to what the industry supported, and AmCham, Microsoft, and the World Federation of Advertisers were highly critical of the notion. These differing accounts are noticeable because the Commission did not explicitly mention the principle in its 2010 Communication. Thus, it is plausible that the privacy advocates and DPAs managed to influence the Commission.

Data protection by default extends the general data minimisation and purpose limitation principles to the realm of technical design and configuration. Whereas 'privacy by design' can mean almost anything related to technical design, processes, and user experience design, privacy by default has different connotations. Following the principles of privacy by design might mean that databases of customers should be pseudonymised, whereas privacy by default requires that the least amount of data should be collected in the first place.

This is potentially revolutionary as the opposite has often been the case. During Facebook's first five years of existence, it gradually expanded the availability of user information to a wider circle of users. In 2005, the default settings limited the availability of information such as pictures, friends, gender, and other profile data to the user's own friends. In 2010, the default settings made this information available to the entire Internet (McKeon, 2010). Facebook eventually dialled back some of these settings, but developers could still syphon a considerable amount of data from users, as was demonstrated by the Cambridge Analytica scandal (see chapter 2). The question of the importance of default settings has also surfaced in the academic literature (Shah & Sandvig, 2008), perhaps most famously by Lawrence Lessig (2006) who stated that code *is* law. Rather than giving people the tools to change privacy settings, it seems to be more important to set a standard for privacy to begin with, which is what the Commission was aiming for. Moreover, an explicit principle would limit the amount of data that the service provider itself could retain on users, possibly limiting the scope of what information a service provider can argue is within its legitimate interests.

As noted in chapter 3, a fundamental problem of privacy law is that more transparency in the form of reports and notices results in fewer people actually reading the notices (Nissenbaum, 2011, p. 36). The transparency paradox is a fundamental dilemma for EU privacy law because the whole notion of consent is based on people being informed subjects. The Commission acknowledges this problem in its impact assessment of the draft Regulation, referring to the problem of 'notification fatigue' (European Commission, 2012b, p. 100), which was raised originally by BBC, Nokia, CBI, and Microsoft in the 2011 consultation (see the previous section).

The question of 'data subject fatigue' surfaced primarily in the context of data breach notifications. It was argued that very strict thresholds for notices would result in people not knowing when to take precautions while very loose thresholds would leave them drowning in a sea of notifications and not knowing which to take seriously. Here the Commission had adopted a policy frame promoted by the lobbyists, telling a story about a flood of notices leading

to apathic citizens unable to distinguish between real danger and minor inconvenience.

The Commission's solution was to create different thresholds for notifying DPAs and the users. DPAs should be notified within 24 h on all occasions (Article 31), whereas users should be notified if the breach is 'likely to adversely affect' their privacy (Article 32). The notion of notification fatigue paints a fairly bleak picture of the security of databases. If security breaches occur on a daily basis such that users would find themselves numbed and disinterested, surely the biggest problem is not notification fatigue but the security precautions of data controllers? The Commission's willingness to accept this framing of the issue is slightly worrisome. On the contrary, the actual wording of the article detailing the obligations of controllers in case of a data breach need not result in a poorer outcome for consumers, in the sense that DPAs would have to be notified in any case, and a DPA could make the judgement that individual users should be notified as well. While contrary to the wishes of privacy proponents who prefer informational self-determination, whether this is a substantial policy loss for privacy advocates overall is questionable.

7.1.2.3 Enforcement of both approaches

The question of how the Regulation should be enforced was one of the cornerstones of the draft legislation. The lack of harmonised legislation and diverse enforcement of the Data Protection Directive's provision had resulted in an unpredictable regulatory environment. For the Commission, four goals stand out. First, the amount of 'red tape' should be cut; second, the regulation should be applied consistently across the EU; third, the data protection principles should be enforced by independent regulators with the power to issue administrative sanctions; and finally, the GDPR should have extra-territorial application.

Noting that the notification procedure emanated from the French tradition and was not applied elsewhere prior to the Data Protection Directive (Simitis, 1995), it was probably a self-evident starting point to ease the bureaucratic burden of data controllers. Some of the DPAs were already opposed of the procedure (like the Swedish Datainspektionen), virtually all companies regarded it as useless, and even some civil society organisations did not see it as contributing to the privacy of individuals. However, it did have some supporters. The UK Ministry of Justice was against abolishing the notification procedure because the fees helped fund the Information Commissioner's

Office (ICO). Removing the notification procedure would, in the view of the Ministry of Justice, challenge the independence of the ICO.

The notification procedure was replaced by a system where certain situations trigger prior consultation and authorisation with the DPA (Article 34). This system is co-regulatory by nature because the controllers themselves decide whether a DPIA is needed owing to specific risks (Article 33), but once a high risk has been identified, the DPA may prohibit the intended processing. The arrangement is partly reminiscent of the approaches advocated by free data lobbyists – more flexibility, more self-regulation, and focus on 'harms' and 'risks'. On the contrary, the Commission's draft makes privacy impact assessments obligatory in some cases (Article 33.2) and transfers the final decision to the DPAs (Article 34). Mandatory DPIAs were opposed by most free data lobbyists, including the UK Ministry of Justice, and generally approved by privacy advocates. It can be argued, then, that while some concessions were made for the industry, the draft proposal generally supported the privacy advocates' agenda. However, the proposed framework may be criticised from the point of view of privacy advocates as well because there are clear deterrents to judge a processing activity as high risk.

Arguably, the most supported of all proposals was the inclusion of the so-called one-stop shop, where a lead authority is designated in cases where processing of personal data takes place in several member states (Article 51). Therefore, the DPA of the main establishment of the controller is designated the lead authority. However, citizens may still lodge a complaint in any member state. The inconsistency of application, a common critique by both free data lobbyists and privacy advocates, is further addressed through formally recognising and requiring DPAs to co-operate and assist each other, most importantly through the establishment of a 'European Data Protection Board' (EDPB). The establishment of the Board to replace the WP29 marks an important shift in terms of transnational governance. While the WP29 was influential, its mandate was limited to an advisory function. The Commission gave the EDPB formal powers to decide whether a measure issued by a DPA should be approved according to the so-called consistency mechanism. The opinions are decided via simple majority and are jointly overseen by the Commission. This arrangement further strengthens the supranational aspect of data protection governance, to a point where one can question whether the subsidiarity principle was respected. The common grievance among free data lobbyists, that access and insight to the WP29's decision-making process is virtually non-existent, did not seem to persuade the Commission into including a formal obligation of the Board to consult with third parties.

Another enforcement-related measure worth highlighting is the level of Commission involvement in interpreting the rules and providing additional regulation. The Commission's draft empowered itself to issue delegated acts on a range of issues concerning everything from further specifying exceptions to outlining acceptable safeguards and requiring technical standards. In other words, the Commission would have been able to determine the exact contents of the provisions. These powers are an even stronger departure from the principle of subsidiarity. While delegated acts were introduced in the Lisbon Agenda in Article 290 of the TFEU, they were supposed to 'supplement or amend certain non-essential elements of the legislative act'. The Commission evidently went further in the draft GDPR, essentially giving itself the power to issue interpretations of key definitions in the law (such as legitimate interests or safeguards).

Evidently, the most significant departure from the earlier Data Protection Directive was the inclusion of administrative sanctions. While many member states had empowered DPAs to issue fines, the size of the administrative sanctions in the Commission's draft was considerably larger. While the UK's administrative sanctions amounted to a maximum of £500,000, the sanctions proposed in the Commission's draft ranged from either €250,000 or 0.5%, whichever is greater, to €1,000,000 or 2% of the global annual turnover of a company, reminiscent of the sanctions used in the competition regulation. While the scope of the sanctions raised considerable debate, an important point that is often missed is that the Commission's draft did not include a maximum figure. The fines are connected to individual incidents, which means that a fine between 0.5% and 2% of the annual turnover may be issued for each regulatory infraction. The administrative sanctions are heavily damning for infringers and set a very high standard for following the rules of the GDPR. The sanctions apply in all cases where a data controller or processor has acted either intentionally or negligently.

Given the severity of the sanctions involved, the extension of the territoriality principle is of fundamental importance. In the Commission's draft proposal, Article 3 was extended to include not only processing that takes place in the EU but also all cases where the personal data of 'data subjects residing in the Union' were processed in relation to the offering of goods or services to data subjects in the Union or 'monitoring their behaviour', clearly a reference to behavioural advertising that the Commission had criticised in its 2010 Communication. While the previous directive did contain an incentive for third countries to update data protection regulation in a fashion which imitates the EU to receive a favourable adequacy decision (Bradford, 2012), this level of extra-territoriality is unparalleled. The idea that questions of

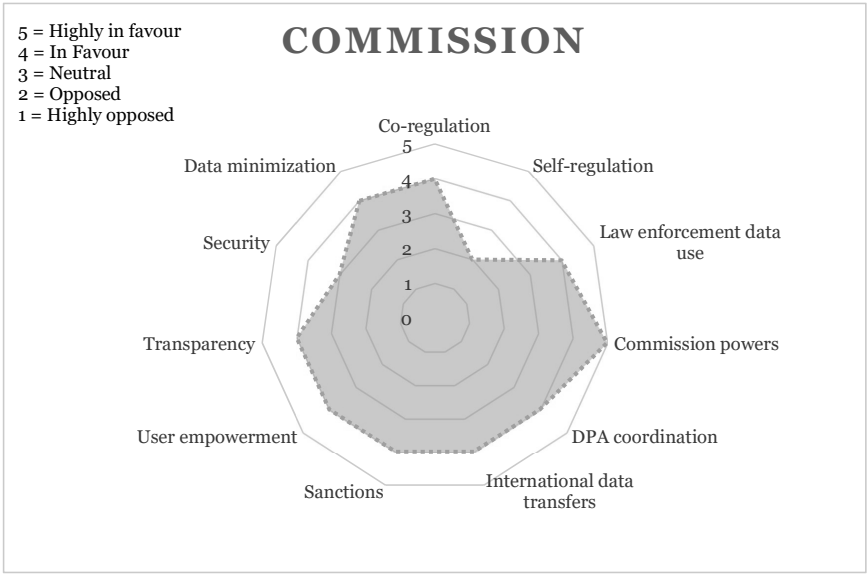
jurisdictional ambiguity can be unilaterally solved is a rather bold proposition, a proposition which was, coincidentally, strongly supported by the telecommunications companies who are in many ways in direct competition with the American IT companies.

In sum, the Commission's proposal was more aligned with the interests of privacy advocates, with one important exception, the strong role of the Commission as an arbiter of regulatory standards by way of delegated acts. Rossi (2018, p. 101) has also demonstrated that digital rights groups were pleased with the proposal, whereas many companies and trade organisations were unhappy with the result.

The proposal demonstrates significant path dependence vis-à-vis the original Data Protection Directive, the biggest departure being the inclusion of administrative sanctions. While behavioural advertising has been addressed by many updated provisions in the proposal, other potential pitfalls have been ignored, such as the broad exception to scientific research that was criticised by Simitis (1995). Despite broadly recognising the concerns associated with information privacy and trying to remedy them with the help of data protection regulation, the Commission's proposal still operated within the confines of the big data paradigm. While recognising and to some extent limiting the extent of profiling, the fundamental issues regarding such practices as raised by scholars of surveillance studies are not really addressed. The proposed solution, Article 20, rather extends the informational self-determination to profiling as well, granting natural persons 'the right not to be subject' but ignoring the more systemic problems with such systems: their opaqueness (Pasquale, 2015), the tendencies to reproduce bias (Gandy, 1993), discrimination (Turow, 1997), false positives (Brown & Korff, 2009), the inability to challenge decisions, and the fundamental question of whether there are any meaningful limits to what extent profiles may be commodified and further repurposed (Lyon, 1994). It shows that while data protection and information privacy may be used as a tool to limit some aspects of the big data paradigm, the present dominant frameworks of information privacy are incapable of fundamentally challenging the underlying framework.

Figure 7.1 provides an overview of the Commission's proposal and its approach to several key issues. The review of the proposal by Schwartz (2013) confirms the main points raised in this study's analysis: the strengthening of individual rights, the centralisation of power in terms of both DPA coordination and Commission powers, and the increased powers of the DPAs represented by the sanctions and increased focus on co-regulation.

Figure 7.1 Key applications in the Commission's draft proposal graded on a scale ranging from highly opposed (1) to highly in favour (5).



The Commission's draft GDPR was, however, merely the baseline for data protection reform. In the ordinary legislative procedure, both the Parliament and the Council have the power to suggest amendments to the final text, and the approved Regulation is undoubtedly a compromise to some degree. I will now proceed with presenting the main differences between the Parliament's and the Commission's versions, and to what extent interest representatives were able to obtain beneficial amendments to the Parliament's first reading.

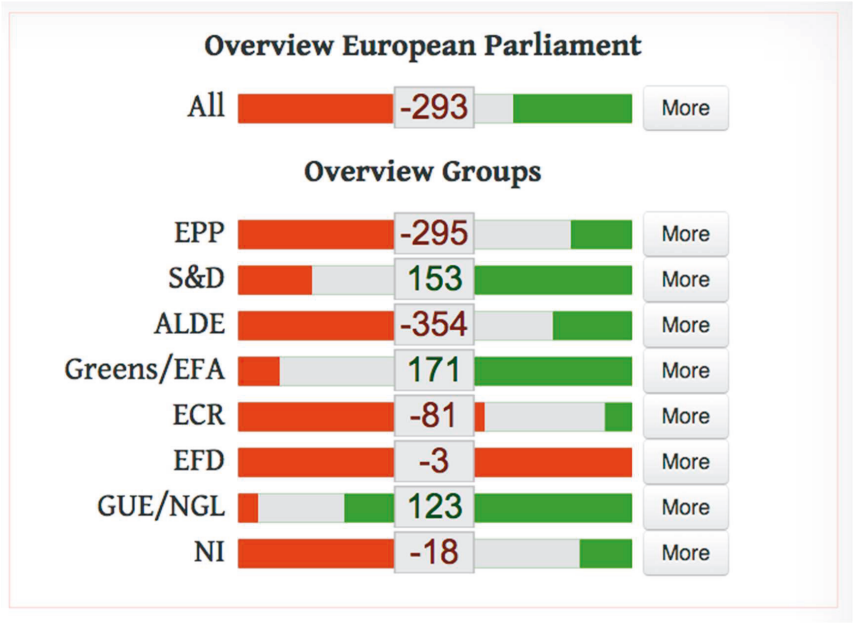
7.2 THE PARLIAMENT'S ELEGY TO SELF-DETERMINATION

Most of the reporting and research on the GDPR's legislative process focused on the influence of lobbyists during the Parliament's first reading. Rossi (2018) outlines how the Silicon Valley giants had recruited former European politicians and policy advisors to lead their lobbying campaigns and hired external lobbying firms to advance their agenda. Many MEPs have declared that the lobbying was fierce. 'I had never experienced such lobbying in my life', said Austrian MEP Josef Weidenholzer in an article in the Financial Times (Fontanella-Khan, 2013).

The process leading up to the Parliament's first reading was drawn-out, and the MEPs in the committees submitted a significant amount of amendments. It should be noted that the committee in charge of drafting the Parliament's version was not concerned with business but with civil liberties. The Rapporteur, Jan-Philipp Albrecht (Greens/EFA), is an outspoken privacy activist who affected the result to a great extent. He later described that 'the influence of the lobby of major IT businesses from Silicon Valley and the powerful advertising industry made itself felt from the outset' (Albrecht, 2016, p. 476).

The influence of lobbyists on single MEPs in the GDPR's legislative process was comprehensively documented by privacy activists. Some of the results are worth highlighting here. Lobbyplag (2013), an initiative by Austrian digital rights activists including Max Schrems, extensively analysed over 3,100 amendments proposed by the Committee on LIBE. All amendments were rated as positive, neutral, or negative in terms of their impact on the right to privacy. On an aggregate level, the results were somewhat negative: 1,263 amendments were rated as weaker, 953 as neutral, and 943 as stronger.

Figure 7.2 Aggregate scores for amendments to the General Data Protection Regulation (Lobbyplag 2014).



Lobbyplag's overview of how the political groups in the European Parliament proposed amendments shows that the green group Greens/EFA (including the Pirate party), the social democrats (S&D), and the left (GUE/NGL) submitted amendments that were predominantly stronger. The groups on the right, the centre-right European's People's Party (EPP), the Alliance of Liberals and Democrats for Europe Group (ALDE), and European Conservatives and Reformists (ECR), proposed predominantly negative amendments according to Lobbyplag's analysis (see figure 7.2).

Passages in some lobby papers ended up nearly unedited in some of the MEPs proposals. Through word-by-word comparison, Lobbyplag's (2013) analysis shows that it is not uncommon for amendments to follow the exact wording of the lobbyists' proposals (76 were leaked in total). The documents submitted to MEPs by lobbyists contained precise amendments to the Regulation, whereas the Commission consultation papers were more general in scope. While the documents from the consultations provide insight into how the Commission's proposal came into being, the documents available on Lobbyplag look at the second stage, i.e. how lobbyists attempted to encourage MEPs to add favourable amendments to the Regulation.

The following companies and NGOs were successful in influencing legislators: NGOs European Digital Rights and Bits of Freedom, telecommunications and Internet organisation EuroISPA, AmCham, the business interest association Digital Europe, the European Federation of Finance House Associations (Eurofinas), the EBF, retailers eBay and Amazon, and credit information umbrella organisation ACCIS (see table 7.1) All except Bits of Freedom, Amazon,[66] and ACCIS had participated in the earlier public consultations.

The results are revealing on a more detailed level. A comparison of the proposed amendments in the consulting committees shows that several of the MEPs had copied parts of their amendments directly from the documents the lobbyists had provided them (Lobbyplag, 2013). For example, Sajjad Karim (ECR), Klaus-Heiner Lehne (EPP), and Marielle Gallo (EPP) submitted separate amendments that added pseudonymous data to the definitions. One could argue that this was just a case of comparing notes as they were all members of the same committee (ITRE), but Michael Harbour and Adam Bielan (ECR) of the Internal Market committee also submitted the exact same definition.

[66] It is, however, likely that Amazon participated through one or several of the business interest associations such as AmCham or Digital Europe.

These amendments were identical to the proposal made by AmCham and highly similar to EuroISPA's proposal, whose membership also overlaps to some degree. It shows that strategic ad hoc coalitions were formed on specific topics. The idea behind adding pseudonymous data as separate category is to leave the door open for loosening data processing obligations. It is a textbook example of loophole lobbying (cf. Dür, Marshall, & Bernhagen, 2019, p. 85).

While pseudonymisation is usually presented as a measure that will increase the level of protection awarded to data, if pseudonymous data is awarded less strict processing requirements, the result might be the opposite. In many cases, identifying information such as names or social security numbers is replaced with pseudonyms. However, as Ohm (2010) demonstrates, the possibility to identify persons is not limited if the database is otherwise rich in information that can be compared to other datasets. If names or social security numbers are replaced with pseudonymous identifiers, two things must be considered. First, who has the keys connecting the pseudonymous data to the identified individual? Second, is there anything else in the database that will make identification possible? The concern is that by creating a weaker set of obligations for pseudonymous data, privacy rights are de facto weakened as the material difficulty to identify a data subject is not sufficiently increased by pseudonymisation.

On the contrary, Green party MEP Eva Lichtenberger and Pirate party MEPs Amelia Andersdotter and Christian Engström of the Green/EFA group also copied extensively from the proposals made by Bits for Freedom and EDRI. Although the leaked lobbyist proposals do not constitute a complete sample, the comparisons paint a clear picture: MEPs on the left copy amendments from civil rights groups and MEPs on the right copy from amendments suggested by multinational corporations (see table 7.1).[67] While there are some exceptions to this rule, they are rare.

Thus, the question of whether lobbyists exert influence over MEPs has partly been answered. The fact that several MEPs copied amendments from the lobbyists is indicative of the structural dependency of politicians on the information provided by lobbyists, as raised by Coen (2007), and it is difficult to see how Klüver's (2013) notion of 'mutual benefit' can be supported. The rapporteur, Jan-Philipp Albrecht's (2016, p. 481) testimony of the lobbying that took place in the Parliament paints a clear picture:

[67] It is of course possible to challenge the notion that Green or Pirate parties are on the 'left', as they would not be consistently in favour of policies presented by the traditional left. However, a significant part of their political agenda clearly draws of a more social liberal tradition historically associated with the left. For a more detailed discussion on contemporary Pirate politics, see Jääsaari and Hildén (2015).

> *Consumer protection organisations, with their totally inadequate resources, described consumers' interests quite differently [than industry lobbyists] – and far more accurately – often did not even succeed in reaching Members of the European Parliament with their arguments. Members' agendas were already full of meetings requested by industry lobbyists.*

These results put the legitimacy of the EU's legislative process to test. However, it is not the throughput aspect of legitimacy that is fundamentally challenged because MEP lobbying is not formally institutionalised similarly to the public consultations organised by the Commission. Therefore, it could be argued that the lack of institutionalisation is precisely what drives unequal access and influence. While civil rights organisations had considerable access to some politicians, they were mostly from fringe parties with limited political power – except for the fact that a Green had been designated special rapporteur. This also suggests that access to the politicians who are sympathetic to one's cause is an important explanation in the European Parliament as well as in the Commission. It also shows that parliamentary committee membership is less decisive than party adherence.

What is not entirely clear, however, is to what extent the amendments suggested by lobbyists were included in the Parliament's final proposal. The fact that individual MEPs have copied their amendments directly from the proposals by unelected parties does not mean that the process as a whole lacks legitimacy. In a sense, the vast number of amendments may be an indication that the process is self-correcting: even though some MEPs decide to copy-paste lobbyists' proposals, the final version will be different from the individual lobbyists' proposals. However, an unprecedented event took place during the Parliament's reading, which according to earlier research on the GDPR had a decisive influence on the legislative process: the Snowden revelations of 7 June, 2013.

Rossi (2018) and Kalyanpur and Newman (2019) highlight that prior to the Snowden revelations in 2013, MEPs were submitting amendments that were watering down the Commission's initial proposal. After Snowden, the dynamics changed. According to Kalyanpur and Newman (2019, p. 461), the Snowden revelations did not directly result in a change in attitude among the MEPs, but the activists, among them the EDPS Peter Hustinx, and privacy-oriented MEPs could capitalise on the high salience environment to push for stricter amendments. In Kalyanpur and Newman's (2019) view, MEPs were afraid to see their legitimacy questioned by their association to the IT companies that were pointed out as enablers of the NSA's PRISM programme.

Table 7.1 Influential lobbyists (Lobbyplag, 2013).

Lobbyist	Sector	Type of advocate	Influenced MEPs
Bits of Freedom	Digital rights	Privacy	Greens/EFA, S&D, EPP
EuroISPA	Telecommunications	Free data	EPP, ECR
AmCham	Business advocacy	Free data	EPP, ECR
Digital Europe	IT	Free data	ECR
Eurofinas	Finance and credit	Free data	ECR, EPP, S&D
EBF	Finance and credit	Free data	ECR, EPP, ALDE, S&D
eBay	Retail	Free data	EPP, ECR, ALDE
Amazon	Retail	Free data	EPP, ECR, ALDE
ACCIS	Data brokerage (credit data)	Free data	ALDE, EPP, ECR

According to Rossi (2018, p. 106), the debate evolved from being only about Internet privacy to becoming about the protection from American surveillance. This frustrated lobbyists, who argued that they were being unfairly associated with the spying scandal (Rossi, 2018, p. 106). A major turn was Angela Merkel's public support of the GDPR. Kalyanpur and Newman (2019) also underline that Commissioner Reding's position was remarkably hardened after the revelations. With the help of discourse network analysis of 103 actors, Laurer and Seidl (*forthcoming*) demonstrate that prior to Snowden, the coalition comprising GDPR supporters was much smaller and less dense than the group lobbying against the GDPR. After June 2013, the discourse coalitions changed, making the 'pro-GDPR' coalition stronger and denser than the coalition against the GDPR.

Earlier research has mostly focused on how the tide turned for privacy activists owing to the Snowden revelations, but they have largely overlooked to what extent the final first reading of the Parliament contained lobbyists' proposals. To assess this, I created a separate text document containing only the amendments made by the Parliament. I then used the open source plagiarism software Wcopyfind (Bloomfield, 2016) to look for similarities in the lobbyists' leaked proposals. The settings used for the study are provided in table 7.2. Some aspects of the analysis challenge the validity of the results. First, lobbyists tend to include the original Commission proposal in addition

to their amendments. This means that similarities between the Parliament's amendments and the Commission's original would be included as false positives. Second, small amendments to the text might not be included in the results owing to the sensitivity settings of the plagiarism analysis (minimum of six words, 80% accuracy). Lowering the sensitivity of the analysis would, however, result in a much higher rate of false positives. Third, the document containing Parliament proposals does not include omissions, which means that some significant amendments have not been included.[68]

Table 7.2 Wcopyfind settings used for the computerised plagiarism analysis.

Setting	**Value**
Shortest Phrase to Match	6
Fewest Matches to Report	5
Ignore Punctuation	No
Ignore Outer Punctuation	No
Ignore Numbers	No
Ignore Letter Case	Yes
Skip Non-Words	No
Skip Long Words	No
Most Imperfections to Allow	2
Minimum % of Matching Words	80

The results show a relatively low direct overlap between the Parliament's amendments and the leaked lobbyists' papers.[69] Owing to the problems associated with the validity of such a computerised analysis, individual percentages are not worth reporting. However, the results do suggest that while there are similarities, these are primarily on a conceptual level, and few longer word-by-word copied parts made it through to the final proposal.

[68] The aforementioned problems were addressed by Lobbyplag by coding all insertions and omissions separately for each article and recital in large .json files. In this way, it was possible to compare individual submissions on the website. It would be possible to copy their methodology and use their materials for a more accurate plagiarism analysis. However, this would require setting up the entire site infrastructure as Lobbyplag did. It is also as labour-intensive as a completely manual analysis, defeating the purpose the computerised analysis serves here: to provide a quick overview.

[69] The full table is provided in Appendix 2. The highest measured match was 16% between EDRI's proposal and the Parliament's amendments. There was a 12% match between the Parliament's amendments and AmCham's proposal, but many of the hits were simply phrases and terminology that had also been used in the Commission's proposal. Upon examining the two documents qualitatively, only one hit appeared to be sufficiently identical to be considered 'lobby plagiarism'.

Nevertheless, as the Lobbyplag analysis shows, the resulting document is a patchwork of amendments that both increase and decrease the data protection of citizens.

The approved version contained 207 changes to the original draft Regulation, meaning that nearly all recitals and articles were somewhat amended. Therefore, it is imperative to both analyse the Parliament's first reading in its entirety and compare it to the earlier lobbyist proposals that were of a more conceptual nature. In the next section, I will outline the main changes in the Parliament's proposal according to the operational principles of informational self-determination and bureaucratic proceduralism as well as questions of enforcement that cover both approaches. The results from this analysis will then be compared with the earlier study results of the interest representatives' positions, including some of the lobbyists who were successful in influencing individual MEPs in the Lobbyplag study.

7.2.1 TRACES OF LOBBY PROPOSALS IN THE PARLIAMENT'S DRAFT

7.2.1.1 Informational self-determination

Compared with the Commission's proposal, the Parliament's reading strengthened the rights of data subjects and was, in general, quite in line with what privacy advocates recommended in their proposals. Some of the key differences compared with the Commission's approach include the addition of more categories to the list of special categories of data, such as philosophical beliefs, sexual orientation or gender identity, trade union activities, biometric data, data on administrative sanctions, judgements, and suspected offences. Another noteworthy amendment was the addition that consent (Article 7) should be *clearly* distinguishable from other questions and 'as easy to withdraw … as to give it'. Similarly, as in the Commission's proposal, consent must be explicitly given.

In other words, the Parliament's approach was inspired by informational self-determination. Credence is given to the data subject's ability to represent their own interests and make informed choices. Some of the substantial rights related to rectification, access, right to erasure, and right to object are changed to reflect this position. For example, the right to erasure carries with it a significantly more extensive right to have data removed from third parties, essentially extending the data controller's obligations. Moreover, everyone has the right to object (instead of not be subject to as in the Commission's

proposal) to profiling and be informed of this right 'in a highly visible manner'. Profiling is also less explicitly defined than in the Commission's proposal, indicating that a wider degree of activities would be covered by the provision. The Parliament also explicitly requires that profiling that produces 'legal effects' shall only be allowed when it is authorised by law and includes a human assessment and an explanation of the decision reached. Nevertheless, an important exception to this rule was provided in Recital 58a, which explicitly states that profiling based on pseudonymous data is presumed not to significantly affect data subjects. In other words, such processing would require neither authorisation by law nor a human assessment. Pseudonymisation as a way to lower data protection requirements was an approach frequently advocated for by free data lobbyists.

The member states' mandate to limit user rights is also somewhat restricted in the Parliament's proposal. The general principles related to processing in Article 5 are not awarded any margin of appreciation in contrast to the Commission's proposal. When restrictions to user rights are introduced into member state law, these restrictions must be not only necessary and proportionate but also with a '*clearly defined* objective of public interest' (emphasis added). Furthermore, the public interest definition excludes the economic or financial interests that were present in the Commission's draft. Therefore, the supranational aspects of the proposal are strengthened.

However, not all amendments would be graded as positive from a privacy perspective. While the list of categories of sensitive data was expanded, the Parliament added that processing necessary for the performance of a contract is a permissible exception to the general prohibition. The Parliament also added the legitimate interests of third parties to the list of legal grounds of processing in Article 6, a suggestion made by free data lobby coalition Digital Europe, among others. Moreover, the Parliament's reading removed the provision stating that power imbalances should be taken into account when reviewing whether consent had been freely given, an omission specifically supported by AmCham, Eurofinas, and Insurance Europe in position papers submitted to MEPs.

Another interesting addition to the Parliament's first reading is the inclusion of collective agreements as a permissible exception to the prohibition of processing in the employment context. While this is certainly reflective of the strong role trade unions have, particularly in the Nordic countries, the inclusion of such an exception means that trade unions are granted the authority to negotiate the fundamental rights of their members. As some trade union contracts may affect non-members as well, this means that trade unions can set the standard for people who have not granted them

authority to negotiate. Nevertheless, this provision is in line with what the trade unions UNI Europa and ETUC pushed for in the 2011 consultation, wishing for increased possibilities of trade unions to represent their members. The trade unions were also successful judging by the inclusion of slightly stronger minimum employee rights, resulting in a prohibition of surveillance in private areas such as bathrooms, and that employees shall be aware of the data collection and provided with a notice of use. These questions were, to some extent, also addressed later in the 2017 Barbulescu v Romania case before the European Court of Human Rights.

7.2.1.2 The procedural approach to data protection

Many of the user rights would be largely inadequate were it not for the processing obligations of data controllers. As noted above, I choose to define the obligations that relate to transparency as processing obligations instead of data subject rights. The Parliament's take on transparency is quite revealing, as Article 14, information to the data subject, was heavily amended. The Parliament added, for example, two provisions related to information on profiling, one requiring that controllers should disclose the existence of profiling, its measures, and the envisaged effects and another requiring 'meaningful information about the logic involved in any automated processing'. Another addition was the requirement to disclose whether personal data had been provided to public authorities in the past 12 months and information on whether a data impact assessment had indicated that there may be a high risk with the processing. The risk-based approach put forth by certain lobbyists is otherwise largely absent in the Parliament's proposal.

All in all, the transparency requirements further fortify the reliance on informational self-determination, indicating that by providing sufficient information on the data processing involved, users can exercise their rights and make meaningful choices. The Parliament's proposal appears less concerned with the paradoxes of privacy (Nissenbaum, 2010; Turow, Hennessy, & Draper, 2015) and more interested in establishing mechanisms of individual control. However, the Parliament decided to add that uses of data in the realm of historical, statistical, or scientific research purposes are exempt from the transparency requirement – a decision that was undoubtedly welcomed by some of the research institutions that participated in the 2011 consultation, such as Finland's THL. The transparency requirements do not apply to persons bound by professional secrecy unless the data has been directly collected from the data subject. This is reflective of the point raised by

the European Bar Council (CCBE), who stated that 'the lawyer's professional secrecy must prevail over all data protection rules'.

The Parliament had a clear desire to introduce less formalistic and more flexible compliance measures. Increased attention is given to the role of DPOs, and the factors that trigger DPIAs are more explicit. Article 32a, a new article, introduces the concept of risk analysis. The article stipulates, among other things, that a risk analysis should be performed when data on more than 5,000 data subjects are processed, special categories of data are processed in large scale filing systems, or when profiling that produces legal effects is implemented – largely repeating what was stated as situations which are likely to trigger a DPIA. Overall, the Parliament does not grant the same exceptions that the Commission awarded to SMEs employing fewer than 250 people but instead draws the limit at processing affecting 5,000 people or more. Exactly why the Parliament introduced a separate risk analysis article instead of relying on the DPIA introduced in Article 33 is not entirely clear.[70] All in all, the DPIA and risk analysis are outlined in much more detail than in the Commission's proposal. There is a clear focus on data protection by design and by default instead of documentation, and security policy requirements are harsher than in the Commission's proposal.

For privacy advocates, the decision to include a category of pseudonymous data as well as a new definition of 'encrypted data' was less than ideal. As I have demonstrated above, the concept of pseudonymous data was not original to one specific actor, but it is clear that including a separate level of protection for pseudonymous and personal data was very much in the interest of IT companies. The Business Software Alliance and Johnson & Johnson both advocated for this two-tiered system, and a later position paper by AmCham also included this proposal.

It is possible to find a common thread in all the provisions that could be categorised as contrary to the ideals promoted by privacy advocates. The justifications provided in the Committee on LIBE's (2012, p. 64) draft report on the Parliament's amendments are especially informative and indicate that most of these exceptions to an otherwise strong privacy framework relate to processing for research purposes. The justification for including pseudonymous data states that 'there could be alleviations with regard to obligations for the data controller'. However, while research activities do benefit from less strict data protection obligations obtained through

[70] The parliament also added a separate bi-annual 'data protection compliance review', Article 33a, which stipulates that the controller or processor shall evaluate whether the results from the DPIAs have been taken into account.

pseudonymisation, this does not mean that *only* research-oriented actors would benefit from this inclusion. For example, Google uses an 'advertising ID' to gather data on users who use smartphones that employ the company's Android operating system to target ads based on app usage. In many cases, an advertising ID might be much more informative than a social security number. It shows how data protection regulation can also be instrumental in legitimising function creep, to use Lyon's (1994) terminology.

One of the more salient issues in the legislative process was the question of data transfers outside the EU, as noted above. One of the main points raised by private industries was naturally to ease the international transfers of personal data. However, the timing could not have been worse – the Snowden revelations showed how data from big American tech companies had flowed directly to the NSA. Prior to the revelations, privacy activists as well as Commissioner Reding and special rapporteur Albrecht were concerned that the proposal was being watered down (Rossi, 2018; Kalyanpur & Newman, 2019).

Therefore, a key question is to what extent the Snowden revelations had an impact on the outcome. One consequence was the overwhelming support for the tightening of transfer rules and the inclusion of whistle-blower protection. First and foremost, this is demonstrated by the Parliament's insistence on increased requirements to review the adequacy decisions and the inclusion of the EDPB in the decision-making process. The Parliament included a new article to this end, Article 43a, stating that 'No judgment of a court or tribunal and no decision of an administrative authority of a third country requiring a controller or processor to disclose personal data shall be recognised or be enforceable in any manner' unless there is a legal assistance treaty. Another major amendment was the inclusion of employee representatives when employee data transfers are drawn up in BCRs.

While the list of derogations to the transfer rules is in many respects identical to the Commission's proposal, the deletion of legitimate interests as valid grounds for derogation is a radical departure from the original. The derogations are in many ways drafted as the mirror image of the legal grounds for processing in Article 6, which explains why legitimate interests were included. Where the Commission largely uses the derogations as an instrument among the other safeguards, the Parliament seems to regard them as an instrument to be used in more exceptional circumstances. Nevertheless, such an amendment would also result in data subjects assuming more responsibility for international data transfers because consent would likely replace legitimate interests as grounds for processing abroad.

7.2.1.3 Enforcement of both approaches

One of the more significant amendments to the approach taken by the Commission was to include a specific reference to the 'accountability principle'. Exactly what the accountability principle entails has been subject to debate, as demonstrated above in section 6.2. The problem with accountability is that it can hardly be seen as one principle because there are different interpretations of what it entails. In the form advocated by the Article 29 Working Party (Appendix 1: 2010, p. 9), the accountability principle is heavily associated with the (bureaucratic) procedural approach, where compliance to rules should be demonstrated upon request. In other words, the WP29 accountability principle requires documentation and the introduction of formal policies. Crucially, the purpose of accountability is not to supplement substantive provisions.

In the Parliament's first reading, accountability was not implemented exactly as the WP29 had envisioned. While the principle is definitely present, the Parliament's reading contains fewer requirements related to the documentation associated with data processing (Article 28) than the Commission's proposal. This is slightly surprising when noting the extensive transparency obligations, but it simply shows that the Parliament relies less on the procedural approach than the Commission. While some information must be provided to data subjects so that they can make rational decisions, documentation can be replaced by other ways of demonstrating compliance. This means that the enforcement mechanisms are slightly different.

Rather than connecting administrative sanctions to specific failures to follow procedure, the Parliament focuses on the resources of DPAs, broadened mandate of the EDPB, and more limited powers of the Commission. The Parliament did not want to trust the Commission with the task of specifying the provisions more clearly and wanted to hand over the power to the EDPB instead.[71] Nonetheless, some of the concerns of lobbyists have been heard. A frequent point of concern was the opaqueness of the WP29 and the lack of industry input in its decision-making procedure. In the Parliament's version, the EDPB *must* consult with interested parties and its proceedings should be more transparent.

The administrative sanctions were also significantly amended by the Parliament. In the Parliament's reading, fines for failure to comply with the GDPR would be either €100 million or 5% of the global annual turnover, a higher level than what the Commission had proposed. Whether the total

[71] For example, the EDPB does not have to issue opinions on the Commission's request but can do so freely; the Commission has no right to give opinions or suspend the EDPB's decisions.

sanction available would be higher is somewhat unclear because the Commission's proposal had included specific sanctions for specific acts of non-compliance, whereas the Parliament simply provided a maximum level for all breaches of the GDPR. Instead, many of the softer compliance measures could have a mitigating effect on the sanctions, giving DPAs more room to manoeuvre and an incentive to data controllers to implement data protection by design and default, complete DPIAs, and designate DPOs. Moreover, the sanctions are not only reserved for intentional or negligent non-compliance, except for cases where a controller has obtained the Parliament's proposed 'data protection seal'.

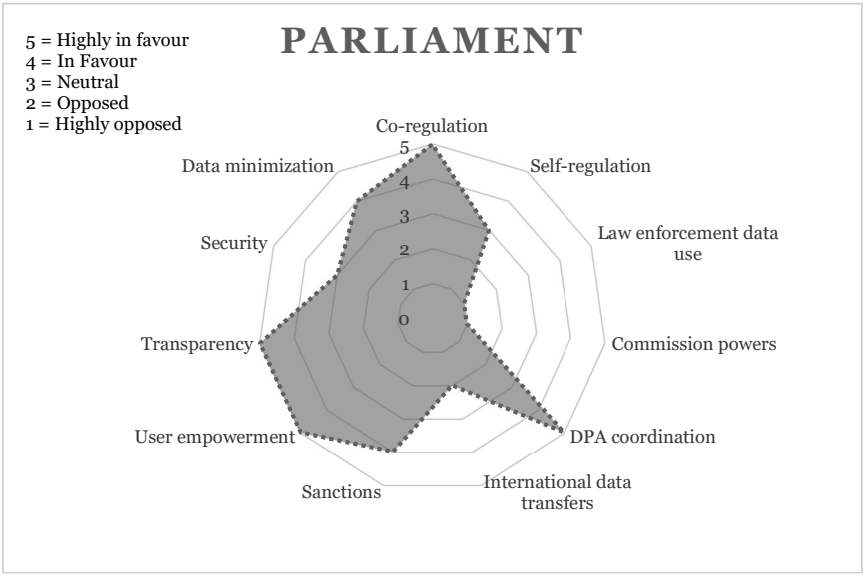
7.2.2 SELF-DETERMINATION, TO A POINT

Despite the alarming amount of lobbying activities in the Parliament, the final document was not significantly weaker than the Commission's proposal. The Parliament's position is fundamentally supportive of informational self-determination, with some important exceptions awarded to free data lobbyists. A few key differences of the Parliament's proposal to the Commission's proposal are worth pointing out. First, there is an increased focus on self-determination, clearly supporting some of the digital rights advocacy visions of how to strengthen information privacy. Second, a significant win for free data lobbyists was the inclusion of pseudonymous data as a separate category. It is not unthinkable that their success can partly be attributed to the fact that research institutions would also support such a measure. Parliamentarians could therefore be perceived as 'pro-research' while supporting data-intensive business activities.

Third, one of the most visible departures from the Commission's draft was the inclusion of extensive transparency provisions regarding whether public authorities had been provided access to personal data – the Snowden revelations serving as a clear window of opportunity for privacy activists both within and outside the Parliament to introduce stricter amendments. Fourth, the procedural and co-regulatory nature of enforcement was partly reduced and replaced by self-regulatory initiatives, but the initiatives were somewhat uneven.[72]

[72] While the mandatory consultation with DPAs as a result of certain impact assessments was removed, the requirements for how DPIAs should be conducted were much more detailed.

Figure 7.3 Key applications in the Parliament's draft proposal graded on a scale ranging from highly opposed (1) to highly in favour (5).



It is worth pointing out that while facing the choice between protecting information privacy with reference to self-managerial initiatives and procedural approaches, the former would in most cases be preferred by free data lobbyists. While user rights may add some complexity to data processing, they are in many respects less invasive than procedural approaches. This is mainly because informational self-determination does not address the paradoxes of privacy. Because people are generally not inclined to advance the protection of their privacy themselves even if they regard privacy as important (Pew Research Center, 2015a, 2015b, 2016; European Commission, 2015a; Turow, 2003; Debatin, Lovejoy, Horn, & Hughes, 2009; Halbert & Larsson, 2015; Kennedy, Elgesem, & Miguel, 2015), the initiatives that aim to increase the self-determination of data subjects are often meaningless.

Nevertheless, there is one important exception. If these rights are combined with sanctions owing to non-compliance and collective judicial redress mechanisms, they can be used very efficiently by digital rights activists. For this reason, it becomes imperative for free data lobbyists to lobby against sanctions and joint judicial redress, which were much more vehemently opposed by lobbyists than various requirements for consent and

further challenged by supporting notions such as legitimate interests and contract-based processing.

The sheer number of amendments and MEPs' propensity to use lobbyists' submitted amendments demonstrate that MEPs are dependent on their expertise and therefore a suitable target for lobbyists. Coen's (1997) depiction of lobbying as a resource dependency is therefore a more apt description of what takes place rather than Klüver's (2013) idea of mutual benefit. Lobbyplag's data also demonstrate that political allegiance is indicative of what position MEPs hold and, in extension, what lobbyists they will listen to. Owing to the diversity of the Parliament, this did not mean that the first reading was riddled with amendments from free data lobbyists but that suggestions made by civil society were also accepted to a high degree. However, as earlier research by Rossi (2018), Kalyanpur and Newman (2019), and Laurer and Seidl (*forthcoming*) have pointed out, it appears that the propensity to listen to cause groups was highly increased after the Snowden revelations. Therefore, there appears to be a dual dynamic, where interest group influence is determined partly by whether MEPs can be considered friendly and partly by the legitimacy risk politicians might bear if they follow the lobbyists' advice. This is conclusive with Dür, Marshall, and Bernhagen's (2019) research that businesses tend to be less successful than cause groups and especially so when the policy issues are highly salient.

It is also possible that the resulting public debate on online surveillance spurred what could be perceived a European public mood against surveillance. Although I argue that Zahariadis' (2008) concept of a European public mood is difficult to establish empirically, the backlash against NSA surveillance was strong and media reports on the issue were extensive in all EU member states. If one is less inclined to follow the rational choice rationale of politicians changing positions because they are afraid to be seen as the lackeys of lobbyists, it could be argued that the extensive public debate on surveillance was actual policy input from the electorate. In that regard, it would be democratically unjustified for MEPs to not amend their positions. At the same time, as Kalyanpur and Newman (2019) and Rossi (2018) highlight, policy entrepreneurs used the sudden interest in surveillance to their advantage in the policy process, actively framing the opposition to data protection as support of big American tech and surveillance companies. A window was opened, policy entrepreneurs capitalised on it, and the lobbyists' influence was largely overturned – except for a few loopholes.

However, if one accepts either of the two theses – that the Snowden revelations provided MEPs with policy input swaying their positions or policy entrepreneurs exploited a window of opportunity created by the scandal – the

result is damning for the idea of throughput legitimacy. If the diversity of viewpoints heard during the consultative stages and the representativeness of interest groups can be undone with heavy lobbying from industry insiders, the institutions in place to guarantee that such policy capture does not occur appear to be weak. Not every legislative proposal is accompanied with a scandal as remarkable as the NSA leak. Moreover, the effects of windows of opportunity tend not to last (Kingdon, 2013, p. 168), and the momentum gained by the Snowden revelations would wane.

7.3 THE COUNCIL ADHERES TO SUBSIDIARITY, STRESSES SECURITY

The Council significantly amended the Commission's proposed legislation. The final draft, signed at Brussels on 11 June, 2015, contained amendments to most articles and recitals in the Commission's draft GDPR. Lobbyplag (2016) managed to obtain 11,000 pages of classified documents containing not only the amendments but also how different member states argued for different solutions. According to their analysis, most of the member states were for limiting the scope of information privacy rights.

Although both social democrats and conservative-liberals voted for restricting modifications, the centre-right bloc was unquestionably more in favour of limiting data protection rights in Lobbyplag's analysis (2016). It may be noted that the Swedish and Czech social-democratic ministers of justice were more closely aligned with the centre-right positions. These results correspond to the earlier analysis of the Parliament's amendments, further strengthening the conclusion that party allegiance and position on the left–right scale is indicative of the position one takes towards digital rights. Regardless of the individual positions on specific amendments, the Council's position was accepted by all but Austria and Slovakia. Excluding the European Free Trade Association (EFTA) member states that also participated in the negotiations, five ministers were associated with centrist ALDE, one with centre-right to right-wing ECR, eight with centre-right EPP, one with centre-left to left-wing Greens/EFA, twelve with centre-left S&D, and one with left-wing GUE-NGL (table 7.3).

With a few exceptions, the Council representatives were the member states' ministers of justice (see table 7.3). I will not proceed with a closer analysis of the positions of the individual member states because that would require either limiting the scope of analysis to a specific issue or a specific member state. As my objective is to find evidence of lobbying influence, I am only

concerned with the text that was eventually approved by the Council, individual objections aside. That being said, many influential publishers, telecommunications companies, and broadcasters are based in Germany and the UK, and several powerful U.S.-based IT companies have their European headquarters in Ireland. The fact that these governments are prone to introduce favourable amendments to legislation that may affect these industries negatively should come as no surprise. Journalistic reports on Facebook's lobbying activity during the GDPR's legislative process highlight a very close relationship between Facebook COO Sheryl Sandberg and Irish Prime Minister Enda Kenny (Carroll, 2017). Whether the amendments that are beneficial to certain interest representatives are a direct result of successful lobbying is not always completely clear, but their very presence and the fact that these amendments required active involvement by the governments of the European member states would suggest that the results are not merely coincidental.

Table 7.3 Participating ministers and their corresponding political affiliation.

Member state (EFTA*)	**Title / Ministry**	**Politician**	**Party**	**Europarty affiliation**
Austria	Bundekanzleramt	Werner Faymann	SDP	S&D
Belgium	Secretary of State for Privacy	Bart Tommelein	Open VLD	ALDE
Bulgaria	Ministry of the Interior	Vesselin Vuchkov	GERB	EPP
Croatia	Ministry of Justice	Orsat Miljanić	SDP	S&D
Cyprus	Ministry of Justice and Public Order	Ionas Nicolaou	DISY	EPP
Czech Republic	Ministerstvo vnitra České republiky	Milan Chovanec	ČSSD	S&D
Denmark	Justitsministeriet	Mette Frederiksen	Socialdemokratiet	S&D
Estonia	Ministry of Justice	Andres Anvelt	SDE	S&D

Member state (EFTA*)	Title / Ministry	Politician	Party	Europarty affiliation
Finland	Ministry of Justice	Anna-Maja Henriksson	SFP	ALDE
France	Ministry of Justice	Christiane Taubira	Walwari (PS governmen t)	S&D[73]
Germany	Bundesministeriu m des Inneren	Thomas De Maizière	CDU	EPP
Greece	Ministry of Justice, Transparency and Human Rights	Nikos Paraskevopo ulos	Syriza	GUE/NGL
Hungary	Ministry of Public Administration and Justice	László Trócsányi	Non-partisan (Fidesz governmen t)	EPP
Iceland*	Minister of Interior	Ólöf Nordal	IP	ECR
Ireland	Minister for Justice and Equality	Frances Fitzgerald	Fine Gayl	EPP
Italy	Presidenza del Consiglio	Mateo Renzi	PD	S&D
Latvia	Minister for Justice	Dzintars Rasnačs	LNNK	ECR
Liechtenstein*	Minister of Home Affairs, Justice and Economic Affairs	Thomas Zwiefelhofer	VU	(EPP)
Lithuania	Ministry of Justice	Juozas Bernatonis	LSDP	S&D
Luxembourg	Minister for Justice	Félix Braz	Greens	Greens/EFA

[73] Since Walwari is a Guyanese party it does not have a clear Europarty affiliation. However, as Taubira was part of the socialist government, S&D was designated as the Eurogroup. It may be noted that Taubira was further on the left than the rest of the government.

Member state (EFTA*)	Title / Ministry	Politician	Party	Europarty affiliation
Malta	Minister for Justice	Owen Bonnici	PL	S&D
Netherlands	Ministerie van Veiligheid en Justitie	Ivo Opstelten	VVD	ALDE
Norway*	Ministry of Justice and Public Security	Anders Anundsen	FrP	(Right-wing)
Poland	Minister Administracji i Cyfryzacji	Andrzej Halicki	PO	EPP
Portugal	Ministry of Justice	Paula Teixeira da Cruz	PSD	EPP
Romania	Ministry of Foreign Affairs	Bogdan Aurescu	Non-partisan (PSD governmen t)	S&D
Slovakia	Ministry of Foreign Affairs	Miroslav Lajčák	Non-partisan (Smer-SD governmen t)	S&D
Slovenia	Ministry of Justice	Goran Klemenčič	SMC	ALDE
Spain	Minister of Justice	Rafael Catalá Polo	PP	EPP
Sweden	Minister of Justice	Morgan Johansson	S	S&D
Switzerland*	Minister of Justice	Simonetta Sommaruga	SP	(S&D)
United Kingdom	Minister of State for Justice and Civil Liberties	Simon Hughes	Lib Dems	ALDE

Earlier policy studies have shown that the Council is not an ideal target for lobbyists in Brussels (Eising, 2007; Coen, 2007). The relevant ministries convene to discuss certain issues and do not have a permanent presence in Brussels, which makes scheduling appointments difficult. However, even though the ministries are rarely lobbied because of their activities within the Council, this does not mean that they would not be targeted by lobbyists within their own member states (Klüver, 2013, p. 39). Representatives of digital rights NGO Bits of Freedom managed to find proof of such lobbying with the help of freedom of information requests to the Dutch government (Kreiken, 2016a). The Dutch business network VNO-NCW was the most active lobbyist in terms of messages sent. Kreiken (2016a) also points out that many corporations are included in multiple coalitions, some of which have been created specifically for the purpose of lobbying against data protection regulation. Although reluctant to address whether the lobbyists were successful, there was a significant degree of congruence between the lobbyists' positions and the Dutch governments approach (Kreiken, 2016b):

> *Although there are visible similarities between the lobby letters and the position of the Dutch government, it is difficult to produce evidence for the fact that representatives of the government have listened to lobbyists too much. We simply can't know what has been said in meetings between government representatives and lobbyists. It's also difficult to prove a causal link: maybe policymakers had already agreed on a specific position before the lobby letters arrived.*

As such, it would be fair to say that European NGOs without significant national presence in the member states would be at a disadvantage in relation to large national firms. Whether this is reflected in the Council's position is something that needs to be examined. I will now proceed with addressing how informational self-determination, the procedural approach, and questions of enforcement have been addressed by the Council. I aim to provide an overview of the key changes and how they relate to the interests of different industries and advocacy groups.

7.3.1 TRACES OF INTEREST REPRESENTATIVES' PROPOSALS IN THE COUNCIL'S DRAFT

7.3.1.1 Informational self-determination

The previous sections have demonstrated how the consent mechanism is at the core of informational self-determination, with a clear connection to the

theoretical considerations of privacy that focus on control. The consent mechanism went through significant changes in the Council's draft. While the Commission's proposal required the explicit consent of users, the Council advocates for *unambiguous* consent unless the data in question is sensitive (see Council, 2015, Article 6(1)(a)). The term unambiguous originates from the Data Protection Directive (95/46/EC) and was at that time also provided by the Council (Article 29 Working Party, 2011, p. 5). The Commission changed the definition to 'explicit' precisely for the reason that data controllers had interpreted the term 'unambiguous' in a fairly broad manner. For example, continuing to use a service has been considered unambiguous consent.

While the change in wording might seem trivial, it is in fact of great importance. The position paper of the World Federation of Advertisers (Appendix 1: 2011, p. 5) is revealing:

> *There is an important distinction between 'unambiguous' and 'explicit' consent, applicable respectively to personal and sensitive data. The distinction between two different levels of consent, with a tougher requirement for sensitive data, is therefore useful and should not be abandoned.*

The same views were echoed by all marketers in the sample, namely: IAB Europe,[74] EFAMRO and ESOMAR,[75] and the Digital Industry Platform.[76] EuroISPA[77] (Appendix 1: 2011, p. 4) even claimed 'explicit prior consent for all processing will ultimately undermine privacy'. It may also be noted that several entities advocated for the inclusion of 'implicit consent', and AmCham's and Digital Europe's submissions contained a nearly identical paragraph (see Appendix 1: AmCham, 2011,p. 19; Johnson & Johnson, 2011, p. 4; Digital Europe, 2011, p. 11; BDMA, 2011, p. 6).[78] Conversely, Privacy International (2011, p. 7) fundamentally opposed this division, arguing that

[74] The Interactive Advertising Bureau Europe is the European subsidiary of the global online advertising association.

[75] Both EFAMRO and ESOMAR can be categorised as market research associations.

[76] A lobby coalition including direct marketers and data brokers such as Acxiom.

[77] European Association of Internet Service Providers.

[78] Digital Europe company members as of 2012: Acer, Alcatel-Lucent, AMD, APC by Schneider Electric, Apple, Bang & Olufsen, BenQ Europa BV, Bose, Brother, Canon, Cassidian, Cisco, Dell, Epson, Ericsson, Fujitsu, Hitachi, HP, Huawei, IBM, Ingram Micro, Intel, JVC Kenwood Group, Kodak, Konica Minolta, Kyocera Mita, Lexmark, LG, Loewe, Microsoft, Mitsubishi Electric, Motorola Mobility, Motorola Solutions, NEC, Nokia, Nokia Siemens Networks, Océ, Oki, Optoma, Oracle, Panasonic, Philips, Pioneer, Qualcomm, Research In Motion, Ricoh International, Samsung, SAP, Sharp, Siemens, Smart Technologies, Sony, Sony Ericsson, Swatch Group, Technicolor, Texas Instruments, Toshiba, Xerox, and ZTE Corporation.

'any data can become sensitive in certain circumstances and/or if linked to other available data; we consider that all personal information should be treated equally and have strong protection'. Privacy International's framing of the issue was more in line with Ohm's (2010) illustration of how individuals in anonymised databases may be re-identified.

Furthermore, the Council significantly amended the provision stating that a power imbalance between the subject and data processor indicates that consent has not been given freely and should not be valid. The Council removed the provision from the article, and although it was mentioned in the recitals, the principle was severely weakened because recitals cannot add new rules but are merely used to help with the interpretation of the articles. The question of power imbalances is a principle that was brought to the table by the trade unions and opposed by free data lobbyists such as AmCham. The rights of employees were further undermined by the Council. Although there was no mention of it in the Commission's 2010 Communication, the Commission's proposal included a separate article on the rights of workers and the processing of data in the workplace. The article laying out the conditions for processing in the employment context was also significantly weakened in the Council's draft, citing employer property rights as a reason for discharge of obligations (Article 82). This indicates that trade unions had less traction with national governments, which should not come as a surprise noting that many of the European governments at the time were centre/right.

Another important amendment that weakened the scope of data subject rights was added to the list of restrictions in Article 21: the enforcement of civil law claims (Article 21(1)(g)). This particular amendment is remarkable in the light of the position papers submitted by the publishing audio-visual industry, represented by IFPI and a joint reply from MPA, IV, FIAD and FIAPF. In their submissions to the 2011 consultation on data protection, the representatives of the so-called copyright industries forcefully stressed that '[a]n excessively wide interpretation of data protection rules has permitted illegal operators to hide behind privacy while engaging in IPR infringement' (Appendix 1: IFPI, 2011, p. 3).[79] By including civil law claims to the list of exceptions, property rights arguably take precedence over privacy rights. It may also be noted that the other position papers made no reference to this allegedly adverse character of privacy rights.

Turning to other areas of processing in the public interest, the Council significantly strengthened the research exceptions and opened for national

[79] The wording in the FIAD, FIAPF, IVF, and MPA reply was slightly different, stressing that 'rogue' operators had been able to hide behind privacy rules.

interpretations. Whereas the Commission's proposal contained exceptions for 'historical, statistical or scientific research purposes', the Council's draft omitted the word 'research', granting even wider exceptions and also including archiving (Council, 2015, Article 6(2), Article 83). In addition, the anonymisation requirements of the Commission's proposal and most data subject rights were subjected to derogations. The Commission's proposal also contained significant exceptions to data subject rights in the realm of scientific processing but with one key difference: although several of the rights would not apply in such situations, data subjects still had the right to obtain information on whether personal data were being processed. That was no longer the case in the Council's version, with the added specification that member states must include the derogation in its own law.

The proposition is in line with research institutions' position paper, but it would arguably also support larger companies with some sort of research departments. This position can be exemplified by the position paper of Finland's THL. THL (Appendix 1: 2011), which processes large quantities of health-related data, is critical of access and rectification rights as well as expanding the role of consent.

Finally, but perhaps most importantly, civil society organisations' right to lodge complaints on behalf of data subjects was removed from Article 73. Instead, this right was limited to situations where a data subject had explicitly mandated such an organisation to represent them (Article 76), unless member state law provides otherwise.

The consequences of the Council's amendments are difficult to assess on a more general level owing to the numerous public interest clauses and other member state exceptions which the Council added. Depending on the country involved, the exceptions can be either highly restrictive or moderately disabling. Notwithstanding the national exceptions, the Council weakened the rights of citizens in many respects. The changes are numerous and often only slightly decremental, but the overall privacy rights of citizens were undoubtedly weakened. The most heavily amended principles relate to user rights, transparency, the liability of data processors and controllers, and privacy by default. These rights need to be addressed in parallel with how they would be enforced at the member state level.

7.3.1.2 The procedural approach to data protection

Noting that the Council included favourable amendments especially for public institutions and authorities by limiting the scope of data subject rights, it is

even more important to address how the Council amended the procedural safeguards in its version.

On the outset, it is worth noting that the Council deviated from the original principle of data minimisation in Article 5(c). The Commission's draft stated that data should be 'adequate, relevant, and limited to the minimum necessary', whereas the new proposal stated that data should be 'adequate, relevant, and ***not excessive*** in relation to the purposes for which they are processed'. The view that an explicit principle of data minimisation should be excluded from the law was present in most of the proposals from the advertising and data brokerage industries (see Appendix 1: WFA, 2011; Data Industry Platform, 2011; World-Check, 2011; AmCham, 2011). Somewhat surprisingly, Microsoft advocated for the principle in connection to the principle of privacy by design. Another issue directly related to the question of data minimisation was the addition of legitimate interests of third parties as suggested by the Parliament. Although citizens have the right to object to such processing, the Council (2015, Article 19(2)) deleted the provision stating that citizens may object free of charge.

One of the more conceptual innovations in the Council's draft was the so-called risk-based approach, according to which the obligations related to DPIAs, data breaches, and prior consultations are triggered by activities determined to be 'high risk' (Council, 2015, Article 31–34). High risk is defined as follows: 'discrimination, identity theft or fraud, financial loss, damage to the reputation, unauthorized reversal of pseudonymisation, loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage' (Council, 2015, Article 33).

The risk-based approach is explicitly mentioned in AmCham's and EPOF's position papers, and some of its iterations can be found in several position papers by representatives of the IT industry. As can be deduced from the definition of high risk in the Council's draft, the inclusion leads to less oversight by public authorities as the data controllers can determine the risk level themselves. Because data breaches that are not categorised as 'high risk' will not result in a data breach report to consumers, the Council is actually advocating for less transparency in their draft.

While the co-regulatory measures, such as the mandatory appointment of DPOs and the employment of DPIAs, have been weakened owing to the risk-based approach, the Council increased the importance of self-regulatory measures. The Council's draft introduced the accreditation of the bodies that oversee privacy certifications and codes of conduct. In the Commission's proposal, the Commission accepted the validity of codes of conduct and certifications. In the Council's draft, the DPAs accredit bodies to oversee the

codes of conduct and certifications. It is difficult to foresee what consequences this would have. The EDPS also supported the inclusion of accredited bodies, which suggests that such self-regulatory measures could have a positive effect on the protection of personal data. Nevertheless, the effects are highly dependent on DPAs being able to assess the accredited bodies in a credible manner, and that, in turn, is dependent on the level of funding the DPAs receive.

The Council's response can thus be categorised as fairly positive towards the retention of personal data, and although some transparency requirements are reinforced in the form of privacy notices, the weakened data breach report requirements raise some concerns. The primary concern of the Council seems to have been to lessen the administrative burdens of data controllers, but this was often done at the expense of citizens, much to the detriment of the privacy advocates.

7.3.1.3 Enforcement of both approaches

The most obvious consequence of the Council's draft is that it challenges the Commission's authority on a number of issues and limits the Commission's powers accordingly. The Commission's draft contained 26 different cases where the Commission was empowered to adopt delegated acts regarding specific processing activities and transparency requirements. All but one article related to the criteria and requirements for data protection certification mechanisms were removed from the Council's draft (Council, 2015, Article 87).

Moreover, the supranational aspects of the Regulation were severely limited, challenging the initial purpose of the Regulation to create a 'one-stop shop' for data protection. EDRI, a participant in the public consultations, counted 48 exceptions for member states and went as far to state that 'Article 21 has broadened government powers so much that they can effectively run a coach and horses through all the rights and protection in this piece of legislation and render it null and void' (EDRI, 2015).

EDRI's strongly worded analysis of the draft is not without merit. The exceptions based on public interest and law enforcement are wide-reaching and poorly defined, leaving most exact definitions to the member states. This approach seems to be central in other policy domains as well, as earlier research has shown that the Council is predominantly concerned with the domestic consequences of policies and legislation (Bouwen, 2002). From a privacy standpoint, the consequences are difficult to foresee because it would

be up to the member states to decide what level of public interest would override the rights of citizens.

By rejecting the transferral of power to the Commission and adding several exceptions to member states, the Council created an executive void, which in the draft is filled partly with the increased responsibility of the new EDPB and partly through an updated self-regulatory framework. As was the case in the legislative process of the Data Protection Directive (see Simitis, 1995), national regulators were used as a vehicle for sovereignty. However, the extension of powers is not as vast as in the Parliament's proposal. The role of DPAs is clearer and more extensive than in the Commission's proposal, yet there is more national budget control over their operations regardless of the original ambition to ensure that the authorities remain independent from the pressures of the government. The DPAs have stronger jurisdictional claims than in the Commission's version, and their investigative and corrective powers are similar. However, the threshold for issuing fines is higher, and the DPAs are no longer empowered to prohibit processing completely but can only limit processing for a certain time period.

7.3.2 FAREWELL, ONE-STOP SHOP

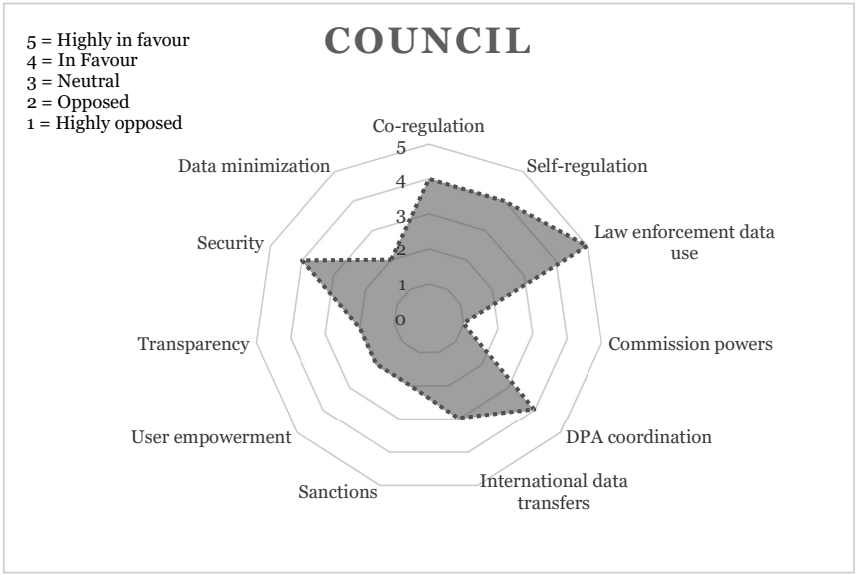
The analysis results of the influence of interest representatives on the Council's draft can be categorised as ambivalent. Drawing on the conclusions made by the positions advanced in the public consultations, neither the multinational IT corporations nor the digital rights groups were likely pleased with the Council's amended proposal. The multinational IT companies were undoubtedly unhappy because of the piecemeal character of the Regulation and the broad range of national exceptions, which effectively undermines the ambition to create a single set of rules for all controllers within the Union. The digital rights groups and trade unions, on the contrary, saw a large part of their platform get undermined because data subject rights, the principle of data minimisation, and transparency requirements regarding data breaches were significantly weakened – the largest threat being the abuse by public authorities that can refer to a number of exceptions in the public interest.

In the end, national publishers and direct marketing companies gained the most and lost the least in the Council's draft. They benefit from the explicit reference to direct marketing as a legitimate interest in the recitals as well as the addition of the legitimate interests of third parties. These companies are not as heavily affected by the lack of EU harmonisation as global IT companies because their business operations are closely tied to national environments. Market research companies could also employ the widened research

exceptions when processing data. Moreover, the copyright industries managed to persuade governments to include an important exception for the data processed in civil law claims.

It should still be noted that the Council's draft provided some clarity that the original Directive failed to deliver and that quite significant sanctions were still in place, although weaker than in the Parliament's and the Commission's versions. The Council's draft would perhaps not be seen as such a let-down for privacy advocates if the Commission would not have proposed a significantly more ambitious document in the first place. The proposed amendments and the dynamics of interest group influence reflect the Data Protection Directive's legislative process as described by Simitis (1995): whereas the early versions of the draft legislation were ambitious, the Council inserted serious loopholes, often at the suggestion of lobbyists. This is consistent with earlier studies on business groups' proficiency at loophole lobbying (cf. Dür, Marshall, & Bernhagen, 2019). Similarly, it is possible to see that many of the proposed amendments were added to protect national solutions to data protection and national uses of data that would otherwise be deemed incompatible with the GDPR. Nevertheless, some of the amendments had no relation with public administration and were close to what free data lobbyists were lobbying for.

Figure 7.4 Key applications in the Council's draft proposal graded on a scale ranging from highly opposed (1) to highly in favour (5).



Overall, the Council's draft was more aligned with the positions associated with free data lobbyists and the big data paradigm in general. What does this indicate about the realization of citizens' information privacy? The results confirm that surveillant practices within the public sector are becoming highly normalised and are definitely not limited to national security exceptions. The bureaucratic nature of surveillance is especially visible in areas of public administration (cf. Foucault, 1977; Dandeker, 1994; Lyon, 1994; Webster, 2012; Gandy, 1989), and the Council's wish to extend national exceptions to a wide variety of areas is indicative of how integral record-keeping is to the modern nation state. Moreover, the Council not only wanted to safeguard the present solutions but also made sure that public authorities would be able apply profiling technologies to sensitive data. Regardless of the original purpose of the new GDPR to strengthen the rights of citizens, the Council's draft demonstrates that the datafication of society is relatively unhindered by privacy concerns, at least on a governmental level.

7.4 THE GDPR: BUMPY HARMONIZATION OF DATA PROTECTION RULES

Burton et al. (2016) and Burri and Schär (2016) argued that the data protection regulation was impacted by three seminal decisions by the European Court of Justice(ECJ)), *Google Spain*, *Digital Rights Ireland*, and *Schrems*. However, while it can be argued that these decisions affected the salience of data protection policy, the evidence from the legislative process does not appear to support their claim in the first two cases. First, the Google Spain case set a precedent for requesting search engines to delete search results, but it referred to the previous Data Protection Directive, and a similar right had already been proposed by the Commission in its 2012 proposal. Second, the Digital Rights Ireland judgement that rendered the Data Retention Directive void was issued on 16 May, 2015. The judgement did not appear to affect the Council's position on data protection in any meaningful way – besides, many member states were inclined to continue their mass surveillance programmes regardless of the ECJ's decision.

The *Schrems* decision is different, however, because it is directly related to international transfers of data and the notion of 'adequacy'. The Schrems decision was issued in the midst of the trilogue negotiations, but I argue that its impact on the contents of the GDPR was not profound. The context is worth reviewing in more detail. As I explained in chapter three, the U.S. was never officially regarded as adequate by European standards, and the Safe Harbor

agreement was instated to circumvent this apparent shortcoming. However, the agreement was never regarded as a success. Nevertheless, it was allowed to continue until the Snowden revelations shed new light on the obvious inadequacy of the arrangement. After 15 years of concerns regarding its efficiency, the ECJ finally ruled in October 2015 that the Safe Harbor agreement was invalid.[80] In light of the Snowden revelations and the national security exceptions provided by the agreement itself, the court expressed that the Safe Harbor scheme had enabled interference of the fundamental rights of EU citizens by U.S. public authorities and could thus not be valid. The goal of the Safe Harbor agreement had been to strengthen EU citizens' information privacy, but without the agreement, data transfers to the U.S. would not have been legally permissible and the data would have to be stored in the EU. If no data had been transferred to the U.S., the mass surveillance of European communications would have been significantly more difficult.

In the months after the Safe Harbor agreement was declared invalid, in the midst of the GDPR's final negotiations, the EU Commission negotiated and then presented a new 'Privacy Shield' to replace the old agreement. The Privacy Shield contains some improvements regarding the rights of European citizens, but the same national security exception, which forced the CJEU to invalidate the Safe Harbor agreement, is still in place. According to the Commission, however, U.S. law now contains limitations on the access and use of personal data for national security purposes and should be regarded as adequate (European Commission, 2016b).[81] Whether the ECJ agrees remains to be seen.

---

[80] Judgment of 6 October 2015, Maximillian Schrems v Data Protection Commissioner, C-362/14, EU:C:2015:650. Schrems issued prior complaints to the Irish Data Protection Commissioner in 2011, but the Commissioner was reluctant to address the complaints and did not investigate the issue (Europe v. Facebook, 2014). After the Snowden revelations, Schrems filed new complaints, claiming that the new evidence clearly showed that the Safe Harbor did not constitute 'adequate protection' and that the data transfers were not permissible. The Commissioner rejected the complaint, but Schrems filed an application for judicial review in the Irish High Court that referred the question to the CJEU (Europe v. Facebook, 2015).

[81] The Commission primarily refers to Presidential Policy Directive 28 (PPD-28) on limitations on signal intelligence issued by President Obama on January 17, 2014 (Executive Office of the President, 2014). The PPD-28 extends the same level of protection to non-U.S. citizens as U.S. citizens. Before the Privacy Shield was presented, the late privacy activist Caspar Bowden pointed out that future presidents could overturn the PPD-28 at any time. The amended Foreign Intelligence Surveillance Act (FISA) still permits the surveillance of non-U.S. nationals (FISA, sec. 702). Essentially, the PPD-28 requires that the NSA should ignore the FISA provisions on foreign surveillance. The problem with presidential directives is that they are often classified, which means that the PPD-28 could be overturned at any moment without

For present purposes, it is important to acknowledge a few aspects of the Safe Harbor agreement and the Schrems decision. First, the Safe Harbor agreement was already considered a failure within the data protection policy community. Second, the Snowden revelations themselves encouraged the Parliament and the Council to strengthen the adequacy provisions in Article 45.[82] Third, the Safe Harbor agreement and its successor are both diplomatic solutions to avoid data protection rules from obstructing trade with the U.S. On the higher levels of EU politics, there was no intention to let data protection rules trump trade, which is why, despite constant critique, the Safe Harbor agreement was left in place until the court's decision. While the Schrems decision might have emboldened the privacy proponents in the trilogue agreements, it is difficult to see that it would further amplify the impact the Snowden revelations already had. A comparison of the Parliament's and the Council's draft proposals' articles on adequacy decisions and the final text supports this claim. The strengthened position on adequacy was not provoked by the CJEU but by the Snowden revelations themselves.

The final version of the GDPR was ultimately approved on April 27, 2016. As established above in sections 7.1–7.3, the three versions significantly differed in terms of the scope of consent, the data subject rights, the level of procedural obligations that apply to data controllers, the use of delegated acts, and the scope of member state exceptions. The final draft expanded the number of recitals from the original 139 to 173 and articles from 91 to 99, adding further complexity to an already intricate piece of legislation. While some of the additions were mere subparagraphs elevated to separate articles, some entirely new concepts were also introduced. It is worth highlighting Article 48, a suggestion by the Parliament that was clearly inspired by the Snowden revelations outlining the NSA's access to personal data held by American IT companies (cf. Greenwald, 2014).[83] According to Article 48, transfers that are not authorised by Union law have to be based on international agreements such as mutual legal assistance treaties. Another addition worth emphasising is the Council's suggestion to allow data protection certification by independent certification bodies (Article 43), further strengthening the self-regulatory elements of the GDPR.

European legislators being informed. Even if the PPD-28 would be allowed to stay in force, it still endorses the mass collection of data. By its very nature, bulk collection means that all data is retained and accessible by the intelligence community, and there is no effective oversight on how that data is used. It is thus likely that the CJEU will invalidate the Privacy Shield as well.

[82] Article 41 in the draft proposals.

[83] See chapter two, section 2.1.

The introduction of new articles suggests that Boräng and Naurin's (2015) position that it is difficult to introduce new concepts in the later stages of the policy process is not completely unassailable. The signalling significance of new articles is by itself noteworthy, but at the same time, it is also true that the fundamental structure of the Commission's draft did not change. While this proves the importance of the Commission's agenda-setting capabilities (cf. Eising, 2007), nearly all substantial provisions were amended in the GDPR. Taking into account that both the Parliament and the Council amended nearly all articles of the Commission's draft, it should not come as a surprise that the final GDPR was manifestly different from the original on which it was based. While the Snowden revelations caused an exogenous shock that somewhat shaped the contents of the GDPR, other changes cannot be attributed to clear windows of opportunity.

While the primary focus of this study has been to highlight to what extent interest representatives exert influence over the EU institutions, the question of the power relations between the EU institutions is worth addressing. As noted in chapter four, the EU's democratic deficit has been addressed by the introduction of the ordinary legislative procedure. While the Parliament is at least formally on equal standing with the Council, a closer comparison of the GDPR with the different versions put forth by the Commission, the Council, and the Parliament reveal that the Council was far more successful in introducing significant amendments to the Commission's proposal.

Where the Council and the Parliament had suggested different amendments to a provision, in most cases, the Council's suggestion would be the one ultimately approved. There might be several explanations as to why a single article ended up looking the way it did, but the overall tendency is abundantly clear. As previous research on lobbying in the Parliament has pointed out, MEPs are, to a higher degree, dependent on the information provided by lobbyists owing to their comparably more moderate resources than the other EU institutions (Kohler-Koch, 1997; Coen, 2007; Klüver, 2013). The informational disadvantage of MEPs versus the justice ministries of the member states is evident, and it is formally reflected by the approved amendments by the GDPR. The question is important because of the tendencies of the different EU institutions to adhere to the wishes expressed by lobbyists. The previous sections outlined how the Council was more likely to advance the positions associated with the free data lobbyist approach. The Council was able to advance its position to a higher degree than the Parliament, meaning that the end result was more in line with what many free data lobbyists wished for. However, owing to the wide range of member state

exceptions required by the Council, the GDPR is far more fragmented than what companies operating on a global scale would have hoped for.

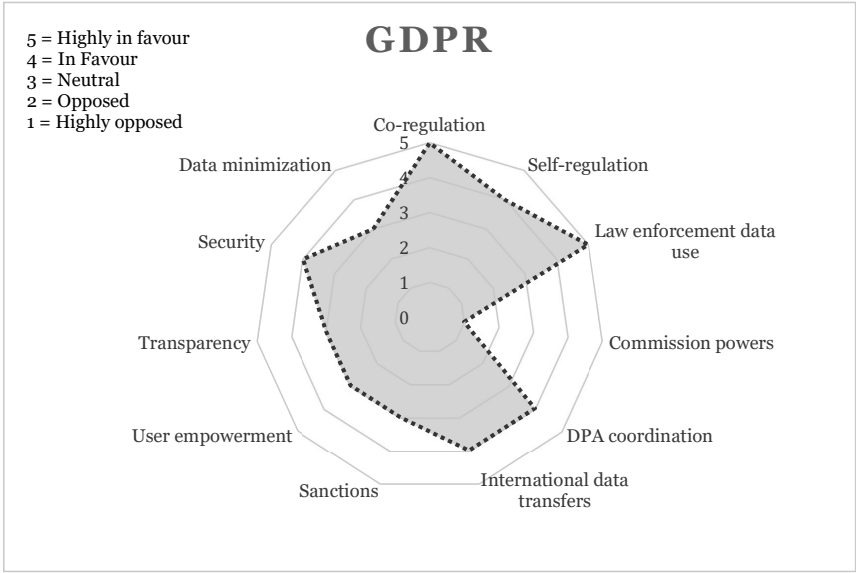
Turning to some of the material changes to the GDPR, Recital 6 is worth quoting at length:

> *Technology has transformed both the economy and social life, and should further facilitate the free flow of personal data within the Union and the transfer to third countries and international organisations, while ensuring a high level of the protection of personal data.*

This particular recital was originally provided by the Commission, never challenged, and ultimately strengthened by the Council, replacing 'requires that' with 'should further facilitate', thus transforming data sharing from a necessary evil for the information society to a function to a desirable feature. While the legal status of recitals is secondary, they denote in what light the binding articles should be interpreted. The wish to extend data sharing beyond the EU is reflected by how more instruments were added to enable such distribution than were available in the Commission's draft.

These amendments also increased the self-regulatory aspects of how such transfers are regulated by allowing codes of conduct and certification mechanisms to function as safeguards for data sharing. While the GDPR generally requires that the safeguards, whether they are inscribed in codes of conduct, BCRs, or other contracts, should grant the same rights as in the Regulation, these are only enforceable between parties. Importantly, this means that any national security exceptions that provide authorities access to data in third countries are unfettered by them. The safeguards may thus guarantee, for example, that data subjects have access to their data, but the security provisions or breach reporting requirements are undermined in practice. Per Council's amendment, such actors have a duty to report the legal obligations that might undermine the rights of data subjects. Nevertheless, such a requirement can hardly be seen as an adequate safeguard and the consequence is, regardless of such disclosures, that the privacy of data subjects is undermined.

Figure 7.5 Key applications in the final General Data Protection Regulation graded on a scale ranging from highly opposed (1) to highly in favour (5).



On a schematic level, the GDPR resembles the Council's draft with slightly stronger user rights and procedural obligations (see figure 7.5). While the supranational elements are less pronounced than in the Commission's original draft, the role of national regulators is elevated through the new, legally binding decision-making powers of the EDPB. From an enforcement perspective, the change is remarkable and demonstrates how the EU is moving towards formalising transnational cooperation between regulatory authorities.

While the EU has a long history of institutionalised enforcement networks (Slaughter, 2005, p. 56), granting such networks binding decision-making powers elevates the governance structures to another level, evolving from mere information networks to enforcement networks. As such, the move further solidifies the importance of DPAs that had a strong impact on the legislative process of the Data Protection Directive (Newman, 2008b; Simitis, 1995). The decisions of the EDPB may also be challenged in court, which raises interesting jurisdictional questions. While the GDPR stipulates that the Board's binding decisions may be challenged in national court, Article 263 of the Treaty of the Functioning of the European Union provides that any binding decisions by an EU body can be challenged in the CJEU. Therefore, it is possible that disdained controllers may seek redress in the General Court

directly, although it is far more likely that most will choose the speedier national courts. The role of national courts in enforcing data protection regulation is therefore elevated in practice.

Owing to the large number of member state exceptions available for research, public health, and employment, the GDPR more closely resembles the U.S. sectoral approach. The differences between the omnibus and sectoral approach as noted by American legal scholars such as Nissenbaum (2010), Ohm (2010), and Schwartz (2013) are more theoretical. The difference is rather that the GDPR provides a principled baseline that is partly replaced by national solutions.[84] On the one hand, the contextual integrity framework might be easier to apply by regulating on a sectoral basis (Nissenbaum, 2010); on the other hand, it means that the consistency and predictability of the principle-based approach is challenged to a point where only experts in data protection law can draw meaningful conclusions about the contents of the law.

The GPDR correspondingly draws on both informational self-determination and procedural approaches. While the Commission's initial proposal did provide individuals with relatively strong user rights, the draft similarly expressed concerns with the various paradoxes associated with people's disconnected (and often disillusioned) approaches to online privacy. To that end, the procedural approach with its co-regulatory elements was used to counter the drawbacks of the self-managerial approach. The Parliament, on the contrary, often replaced the requirements to communicate with DPAs with the requirements to communicate with data subjects, further strengthening the self-managerial approach. The GDPR is, however, more reminiscent of the Council's approach, with stronger self-regulatory elements and relatively weaker user rights. While Recital 7 provides that 'natural persons should have control of their own personal data', a clear reference to the information-privacy-as-control paradigm advocated especially by earlier privacy scholars such as Westin (1967), the articles in the Regulation more closely resemble Reiman's (1976) conceptualisation of information-privacy-as-access, where individuals can sometimes restrict access to some personal information but control resides with other societal actors.

For example, the notion that all consent should be 'explicit' was removed upon the Council's request, a sign of both path dependence from the Data Protection Directive and the influence of free data lobbyists. Moreover, the ability of privacy organisations to act on behalf of data subjects was further

[84] See, for example, Recital 10 which provides that 'this Regulation does not exclude Member State law that sets out the circumstances for specific processing situations, including determining more precisely the conditions under which the processing of personal data is lawful'.

restricted to situations where they have been mandated to do so. While the Commission was clear in why joint judicial redress could not be provided for in the GDPR, neither the Commission nor the Parliament saw reason to restrict activists from making complaints to DPAs on behalf of data subjects. Nevertheless, the Council did open for the possibility of allowing member states to allow for collective action. Bearing in mind that the GDPR already provides for a number of national exceptions, the possibility of joint judicial redress in some member states would entail a clear deterrent to set up shop in such countries.

While some important changes were made that somewhat undermined the informational self-determination of data subjects, the biggest changes compared with the Commission's draft were undeniably associated with the procedural approach that has often been perceived as bureaucratic by industry lobbyists. First, the data minimisation requirements were weakened; second, the legitimate interests of third parties were recognised; and third, further processing was enabled to a greater extent, greatly reminiscent of the position advanced by the Council and clearly favoured by free data lobbyists. Moreover, the most demonstrably visible aspect of lobbyist influence was the inclusion of the so-called risk-based approach, visible in the Council's draft, according to which different levels of perceived risk merit different action (see e.g. Recitals 73–77). The risk-based approach was clearly advocated for by lobbyists such as AmCham, EPOF, and CIPL. Importantly, the risk-based approach heightens the threshold for DPA involvement and data breach reporting. Table 7.4 demonstrates how some concepts that were introduced by lobbyists in the early stages of the legislative process can be found in the different versions of the GDPR.

However, not all procedural aspects of the Commission's draft were weakened. One notable addition was the legally binding obligation to introduce 'privacy by default', an obligation highly supported by privacy activists and first mentioned by the WP29 and BEUC. Another was the Parliament's amendment requiring that profilers demonstrate 'the meaningful logic involved'.

Table 7.4 Lobby concepts in the different versions of the GDPR.

Concept	Promoted by	Commission?	Parliament?	Council?	GDPR?
"notification fatigue" caused by data breach reports	CBI, Microsoft, Nokia, BBC, EDRI[1]	Yes (impact assessment)	Yes (found in justifications)	Yes (leaked documents)	(Indirectly in Art. 34)
Risk-based approach	AmCham, EPOF	No	No	Yes	Article 33, 34
Unambiguous consent	Microsoft, EFAMRO, AmCham etc.	No	No	Yes	Recital 32
Privacy by default	Art. 29 WP, BEUC[2]	Yes	Yes	Yes	Article 25
"Pseudonymous data" as separate category	BSA, AmCham, Yahoo[3]	No	Yes	No	No
Employee codetermination	ETUC, UNI Europa	No	Yes	No	No[4]
"Reasonable expectations" test for secondary processing	Microsoft	No	Yes	No	Recital 50

[1] EDRI mentioned 'breach fatigue' in its proposal submitted to the MEPs and proposed that the breach notification deadline should be extended to 72 h. Curiously, no free data lobbyists proposed extending the deadline but rather preferred removing the hard deadline altogether.

[2] Several others mentioned privacy by default after it was mentioned in the Commission's 2010 Communication. A Google (2019) trends search reveals that the concept did not surface until 2011.

[3] Proposed in a leaked lobby proposal.

[4] Could be allowed for by national exceptions.

In the end, the Commission's goal to restrict the online advertising ecosystem endured, although slightly weakened by a Council amendment specifying that legitimate interests could be used as a legal basis for direct marketing.

Nevertheless, the tracking and targeting of consumers online are subject to the updated consent rules that were backed up with new sanctions. However, whether the self-managerial approach will be sufficient to restrict the online advertising economy is debatable. Although the sanctions definitely caused a scare, whether the GDPR has been able to challenge the surveillance logic on a more profound level is questionable. Scholars such as Bermejo (2009), Turow (2011), Webster (2014), Schneier (2015), and Pasquale (2015) have shown how the media advertising system has evolved from a fairly simple two-sided market comprising audiences and advertisers into a complex web of middlemen. Nothing in the GDPR inherently challenges this model of online surveillance, but it does create an added strain for the consumer-facing entry to obtain verifiable consent to online targeting. For this reason, the industry's largest players with the most targeting power in the form of consumer-facing platforms are at an advantage because they can target their users directly through multiple avenues of communication.

When the GDPR entered into force on May 25, 2018, the consequences of the updated transparency and consent requirements were felt in practice. People received dozens of emails requesting their consent to various newsletters, and sites expanded their cookie notices with minute preferences that regular users had difficulties understanding. Many of these requests were highly deceptive, popularly called 'dark patterns'[85] that nudge users into making choices that are privacy invasive. These include making privacy settings difficult to find, enticing users into consenting, making it easier to accept than to refuse, obscuring the dissenting choice while highlighting the affirmative one, or requesting sign-in when such action is not needed. Some of these practices have been tested by the European DPAs.

On the day the GDPR entered into force, Max Schrems' digital rights organisation NOYB cooperated with other NGOs to lodge complaints with four European DPAs regarding so-called forced consent mechanisms. The complaints initiated a French investigation into the consent practices of Google, resulting in a €50 million fine. As some commentators have noted, the fine amounts to about four hours of Google's revenue, but the more wide-reaching consequences are the invalidation of the ways Google solicits consent to tracking. Some of the early sanctions issued by DPAs indicate that the GDPR has created hurdles for behavioural targeting by way of its detailed consent and transparency requirements. At the same time, however, it is possible that bigger actors will leverage their position to shift liability on smaller ones. For

[85] The term was coined by Brignull (2019). Brignull maintains a 'hall of shame' on his twitter handle @darkpatterns.

example, Google has strong-handed publishers into bearing the burden of soliciting consent to data collection and bearing the responsibility for doing so while Google reaps the benefits, an approach which publishers criticised in a public letter to Google CEO Sundar Pichai (Kint, Mills Wade, Chavern, & Newell, 2018).

A key underlying logic that underpins the GDPR is that while there are reasons behind granting individuals more control over their personal data and some procedural obligations support these goals, there are always other, more important societal goals that are perceived as legitimate exceptions to the right to privacy. Turning to the conceptual notions and fundamental rights origins of privacy, it is easy to see how the big data paradigm has clearly expanded the range of acceptable exceptions. While regulating the processing of data in a separate legal instrument with far more restricted rights for individuals is compatible with a rights-based approach to privacy, the security creep into the GDPR goes further, meaning that essentially any data collected for legitimate purposes within a private enterprise can be accessed by the security agencies, provided such an option exists in national law. The participatory turn in surveillance thus feeds additional data into the surveillant diagram (Cohen, 2012). To a lesser extent, such exceptions are also granted for the enforcement of lower-level crimes and breaches of contract, as demonstrated by the exceptions that were added for the 'establishment, exercise or defence of legal claims', reminiscent of the copyright lobby's critique of bad actors 'hiding behind privacy laws'.

Moreover, the rationale of extending the bureaucratisation of society by introducing more data points is not only a mere requirement to fulfil welfare programmes (Giddens, 1985) but also used for more experimental societal control (Gandy, 1989). Perhaps most evident in the sphere of employment, the GDPR gives equal possibilities to disregard data protection rights for uses that advance the rights of the individual as well as those that are to their detriment. Finally, the big data paradigm is nowhere as present as in the provisions that lay out broad exceptions for scientific research. The broad exceptions, already criticised under the Data Protection Directive (Simitis, 1995), seem to indicate that while privacy rights are worthy of protection in the regular course of business, they cannot be used to hinder innovation. The surveillance-innovation complex, as denoted by Cohen (2016), can only partially be restricted by reference to fundamental rights.

8 CONCLUSION

The GDPR could not have been more aptly timed. During the years leading up to the Commission's draft Regulation, the online advertising economy took off, smartphones became ubiquitous, several ICT giants began offering cloud services, and social networking sites became an integral part of how people communicate. In 2013, a year after the Commission submitted its draft Regulation, Edward Snowden revealed that millions of Europeans had been affected by the NSA's and GCHQ's surveillance programmes. In March 2018, two months before the GDPR entered into force, Facebook was discovered to have allowed third party developers, including Cambridge Analytica, access to millions of Facebook users' personal data. Data protection moved from the fringes of information society policy to its very centre.

From the perspective of EU decision-making, the GDPR was drafted at a time when the lobbying efforts in the EU were becoming more pronounced. An integral aspect of this trend is that the Silicon Valley IT giants, many of which are regarded as the most valuable companies on the planet, brought the full range of Washington lobbying strategies to Brussels.

The GDPR is about more than a new set of data protection rules: it is about privacy, datafication, and power. This study has sought to examine how these trends were reflected in the regulatory output of the EU institutions. In particular, I have attempted to answer the following research questions:

1. What policy alternatives were put forth by the EU institutions in the course of the GDPR's legislative process, and how did they correspond to the ideas, issues, and frames promoted by interest representatives?

2. What does the influence of organised interests and stakeholders in GDPR decision-making reveal about the democratic legitimacy of the process?

This final chapter is devoted to distilling the main findings of this study and providing some suggestions for further research. I will address the first question by looking at how the different regulatory drafts were shaped by earlier events, the influence of interest representatives, and the paradigms structuring and constraining the EU's data protection reform. Based on the answers to the first research question, the second question addresses whether the GDPR can be perceived as democratically legitimate. Finally, I will

conclude by elevating the main contributions of this study and discussing what this means for the legitimacy of EU decision-making in general and for future policy within this domain.

8.1 THE POLITICS OF DATAFICATION

What does the process leading up to the GDPR say of media and communication regulation in the 21st century? In some respects, the regulation of data transfers is reminiscent of the problems associated with transnational television – how can sovereign states remain in control when communication technologies do not respect geographical borders? The EU's answer has always been part fantasy and part geopolitics: within the single market, there are no borders, but to breach the outer border as an outsider, one must adjust to the EU's rules. The fantasy of the single market fractured in the events leading up to the original Data Protection Directive. As Newman (2008a, 2008b) and Simitis (1995) demonstrated, DPAs in member states with data protection laws in place obstructed data transfers to the member states that lacked legislation and forced the Commission to act.

Through this intervention, the level of data protection regulation in the EU became more consistent. Nevertheless, while there was agreement on the level of principle, a closer examination of how the Directive was implemented would soon reveal that the national solutions were wildly different (Korff, 2002) and the level of privacy protections not quite comparable. The idea that the EU favours a principle-based approach while the U.S. employs a sectoral approach to data protection does not quite hold upon closer scrutiny. While the reason to draft a new law, whether a directive or a regulation, was motivated with reference to the diverging implementations of the previous Directive, the GDPR fell short of both the Commission's and the multinational corporations' expectations to harmonise European data protection law. For the governments of member states, such an ambition might never have existed to begin with.

Apart from the differences between the EU institutions' approaches to data protection, this study has mainly been focused on the role of interest representatives in the legislative process. Intergovernmentalists such as Moravcsik (2002) argue that national ways for assessing legitimacy are not applicable in the EU context, but the legitimacy of EU-policy-making should instead be the efficiency of supranational decision-making. While output legitimacy is not sufficient to deal with the EU's democratic deficit for reasons

outlined in chapter four, whether the GDPR achieved what it was set to do and why it came to look like it did is worth considering. In particular, drawing on new institutionalists such as Campbell (2004) and Schmidt (2008), to what extent is the GDPR path-dependent of the earlier Data Protection Directive, what was the role of interest representatives in shaping its contents, and what paradigms shaped and constrained the policy options available?

The path dependence of the GDPR is adamantly clear. As was highlighted in chapter three, the Data Protection Directive was in many ways a more revolutionary piece of legislation than the GDPR. The GDPR draws on many of the key principles from the Data Protection Directive, but the differences lie in the level of detail and in the GDPR's extra-territorial application. Whereas the Data Protection Directive mostly operated on a level of principle, the GDPR further evolves both the bureaucratic proceduralism and informational self-determination approaches to information privacy legislation. The extent to which the GDPR can be traced to its antecedent is worth addressing. First, the data protection reform was unlikely to depart radically from the omnibus approach to data protection regulation. Stakeholder and DPA reviews of the Directive in 2002 did not focus on upending the logic of the regulatory intervention but focused on clarifying and harmonising provisions. True to form, business networks were not advocating for major overhaul; nonetheless, they were not proponents of the status quo but wanted to see regulatory change. There were no positive feedback loops for companies in a situation where data protection regulation was interpreted inconsistently in the different member states. In sum, there were clear calls for complexity to provide further certainty but no radical departure from the original.

Second, as with the Data Protection Directive, the role of national DPAs was pronounced. Although they did not use their powers to coerce the Commission to act, they did provide commentary and expertise, which were taken into consideration by DG Justice. The decision to make DG Justice the secretariat of the WP29 appears to have had a profound impact on the legislative process, as Laurer and Seidl (*forthcoming*) argue. The institutionalised cooperation made DG Justice the likely lead DG for the data protection reform, despite DG INFSO (now Connect) and DG Internal Market (now Growth) being serious contenders. The WP29 had been providing authoritative opinions on data protection legislation for years, and the traces of these opinions can be seen in the Commission's draft GDPR. However, the GDPR's legislative process is different from that of the Data Protection Directive in one important regard. In the drafting of the Directive, the DPAs had a pronounced role from the beginning, whereas other stakeholders were largely excluded from the agenda-setting stage. Therefore, the lobbying did

not really commence until the draft Data Protection Directive had been submitted. When the data protection reform was initiated in 2009, the Commission had a different perspective on stakeholder participation. Stakeholders were included from the very beginning, providing their positions on everything from specific provisions to the general approach. Nevertheless, the influence of interest representatives looked very different at different stages of the process.

As pointed out by earlier research on interest group participation and the effects of lobbying, separately addressing each EU institution is necessary. Based on how susceptible the different EU institutions have been to the influence of interest representatives, a few observations can be made. First, conclusive with earlier research on interest group participation (Klüver, 2013; Dür, Bernhagen, & Marshall, 2019), it is possible to conclude that while the resources of interest representatives certainly impact their ability to participate in the legislative process, the Commission was less swayed by actors with significant resources than the Council and the Parliament. This does not mean, in my view, contrary to what Dür, Bernhagen, and Marshall (2019) argue, that businesses 'lose'. It means that businesses are comparatively successful in shaping EU policy, even though they might not be able to shape the agenda of a DG that can be perceived as, if not hostile, at least not friendly.

The GDPR did include important changes to the preceding Data Protection Directive that have a deterring effect on data maximisation, but I argue that this is mainly because DG Justice had aligned interests with privacy advocates. Nonetheless, the scope of powers awarded to the national regulators is testimony of the influence of national regulators and privacy advocates. Because the level of enforcement is considerably dependent on the national setting, the most important victories for the privacy advocates are, in my opinion, the introduction of 'privacy by default', as first promoted by the WP29 and BEUC, the codification of the right to be forgotten and the right to data portability, and a stronger data minimisation principle. These were all, however, included in the Commission's draft Regulation. While many of the provisions that privacy advocates supported were eventually included in the Commission's draft, most were partly weakened in the final GDPR according to the Council's wishes. This suggests that participating in the early stages of policy formulation is more important for cause groups than for large firms that can pursue their agenda and influence the Council's amendments through national avenues of lobbying.

My analysis of the legislative process shows that the MEPs were more inclined to accept the reasoning of lobbyists than the Commission's officials

and that the Council's draft included most suggestions made by free data lobbyists. This supports earlier research by Klüver (2013, p. 39) that the Council tends to listen to lobbyists from corporations with a strong presence in the member states. Lobbyists were perceivably able to water down the draft GDPR in the Parliament, especially prior to the Snowden revelations. If, as the evidence presented in chapter seven suggests, the Snowden revelations provided privacy activists a window of opportunity to counter the influence of industry lobbyists, this indicates not only that the legislative process in the EU is open for policy capture by industry lobbyists but also that the deliberative aspects of the early stages of the legislative process can be completely undone.

While the final text did include suggestions made by the Parliament, a comparison of all amendments to the respective drafts of the EU institutions reveals that most amendments to the Commission's text were, in fact, suggested by the Council. This matters not only because of the lack of insight into how lobbying takes place on the national level when EU legislation is drafted but also because the power relations between the Council and the Parliament are clearly tilted in favour of the former, at least in the case of the GDPR. Given that many significant changes were introduced by the Council, it shows that the Council does not appear to be a sub-optimal target for lobbyists, contrary to what is suggested in some of the literature (cf. Hayes-Renshaw, 2009; Eising, 2007; Coen, 2007).

Whether lobbyists primarily contacted the Council in the member states or when the Council was convening has not appeared in the documents used for this analysis; however, the Council's overwhelming support for industry amendments indicates that the Council is not a sub-optimal target for lobbyists. Some of the Council's amendments include exceptions to data subject rights, weakened procedural requirements, and advanced exceptions to public authorities.

Many of these changes were highly reminiscent of lobbyists' suggestions (see section 7.4). For example, the Council's suggestions weakened the consent mechanism, restricted privacy organisations' ability to act on behalf of data subjects and made it possible for data controllers to limit data portability requests with reference to intellectual property rights. While the individual positions of the member states were not included in the primary sources of this study, it should still be stressed that Lobbyplag (2016) had ranked the German, British, and Irish representatives' draft amendments predominantly negative and that Facebook COO Sheryl Sandberg had congratulated Irish Prime Minister Enda Kenny on Ireland's position in the negotiations of the GDPR (Carroll, 2017). Moreover, freedom of information requests to the Dutch government revealed that the Dutch negotiators were overwhelmed

with lobbyists' requests, and nearly all of the communication was from parties engaged in watering down data protection provisions. It is absolutely clear that the existence of influential publishers, telecommunications companies, and broadcasters in especially Germany and the UK had an impact on their respective government's positions and that Ireland's strategic position as home to the European headquarters of many Silicon Valley companies was decisive.

Finally, following the arguments of intergovernmentalists that the EU's legitimacy stems from its capacity to draft efficient policy, the GDPR must also be evaluated based on the Commission's own ambition. The problems that the Commission identified based on its meetings with stakeholders were the lack of harmonisation, people's perceived lack of control of their personal data, and the inconsistencies in personal data protection in the field of police and judicial cooperation. Because the purpose of the GDPR was mainly to address the first two problems, I will focus on them.

The first problem was superficially dealt with by drafting a Regulation instead of a Directive. Regulations do not need to be transposed into national legislation, and evaluating whether member states interpret the same law consistently is easier rather than examining whether national laws and their enforcement uphold the spirit of a directive. From a supranational enforcement perspective, the benefits are unquestionable, but regulations undoubtedly encroach on the sovereignty of member states to draft laws which are consistent with their national legal tradition. In a policy domain such as data protection, where the transnational flow of data is a matter of fact, it can be argued that some degrees of sovereignty have already been lost. Following Slaughter's (2005) work on the role of transnational networks, the increased cooperation of national regulators is a necessity for efficient enforcement action. While having a regulation without national derogations within this policy domain would be unfeasible, the Council's added derogations poked several holes in what was supposed to harmonise legislation in the member states.

One of the biggest differences between the final GDPR and the Commission's proposal is evidently the broad range of exceptions available for services in the public interest. These are dependent on national exceptions and pave the way for data-driven bureaucratisation in the public sector and private suppliers of public services. Moreover, they enable researchers of artificial intelligence and automated decision-making to experiment freely. For these uses of data, informational self-determination is toothless, and bureaucratic proceduralism is heavily constrained. Few governments are willing to outlaw

privacy invasive practices that can potentially have a broader impact on employment, welfare, taxation, or security.

This explains why data protection regulation and privacy cannot alone address issues connected with societal datafication. The GDPR challenges the big data paradigm in areas which are perceived as less innovative but does not profoundly challenge the role of data and automated decisions. Regulatory affordances provided for the development of artificial intelligence, such as facial recognition technology, are fundamentally different from the rules that limit online tracking. Even though the former may be used to inform the latter – for example, facial recognition in physical stores to identify subjects of online advertising – the degree of acceptability of data processing is ultimately decided by what is perceived as scientific and, by extension, innovative. The exceptions to Article 22 on automatic decision-making are especially informative in this regard, as it is blatantly obvious that industries most reliant on automatic processing, such as the financial and insurance industries, are exempt based on contractual necessity.

Regarding the second problem, control of personal data, whether the GDPR has managed to curtail behavioural targeting which was cited as a key concern in the Commission's 2010 Communication needs to be addressed. Did the EU succeed in drafting an efficient response to this perceived policy problem? In chapter two, I defined targeting power as the combination of 1) the collection of data from primary and secondary sources (tracking), 2) the search for patterns and inferences in the data (mining), 3) the association of these patterns with individuals (profiling), and 4) access to audiences. Based on the different applications in the GDPR, it can be concluded that the targeting power of advertising intermediaries that have little-to-no consumer facing activity has been somewhat limited because the collection of data is subject to purpose limitation and data minimisation principles, making transfers to third parties slightly more restricted. Facebook and Google, who have consumer facing interfaces, have embraced the consent-based approach, although the methods used to obtain consent can be criticised. Other advertising intermediaries are dependent on online publishers, whose different transparency policies and ways to verify consent have resulted in mixed results and questionable levels of compliance. Therefore, the GDPR's potential rests partly on the shoulders of privacy activists such as Max Schrems or Privacy International who are willing to use the new data subject rights to encourage DPAs to enforce and ultimately sanction actors that engage in practices that could be categorised as noncompliant.

However, owing to the structure of the online advertising ecosystem, advertising networks are in a strong position to place the burden of providing

a legal ground for processing on publishers. The biggest ad exchanges in the world are operated by Google, AT&T, Microsoft, and AOL that provide access to users on most of the world's most visited websites. Facebook has its own ad exchange with access to over 2 billion users. Many publishers are financially dependent on ad exchanges for a significant portion of their income and this has consequences for data collection practices as well.

In other words, the GDPR has not been able to challenge the ecosystem itself but has forced publishers dependent on it to be clearer about their advertising partnerships. If one ignores the economic ramifications, it would be simpler for publishers to revert to the old model of contextual advertising. However, owing to the rise of behavioural advertising and the targeting power of especially Google and Facebook, advertisers are not dependent on the reach of publishers, resulting in the diminishing demand for the advertising products of traditional publishers. The trust that publishers have built up with their readership is of secondary importance compared with the promises of microtargeted ads. Data protection regulation cannot efficiently regulate online behavioural advertising unless behavioural targeting is completely decoupled from access to services and content. The problem is that behavioural targeting can never be decoupled from the economic incentive to encourage users into consenting. Therefore, the solution on the table is for privacy activists to challenge whether consent has been given in a way which is consistent with the law.

Given how the influence of organised interests has been established at different stages of the GDPR's legislative process, I now analyse whether this also impacts the legitimacy of the EU's data protection reform. As was outlined in chapter four, the inclusion of stakeholders in decision-making is a response to the EU's democratic deficit. To demonstrate that interest representatives' views were taken into consideration in the legislative process does not necessarily mean that the democratic legitimacy of the process is questionable. Instead, the assessment must be made with reference to how successful different interest representatives were in getting favourable policy applications in place and whether their influence was proportionate if one considers the goals with the data protection reform.

8.2 THE LEGITIMACY OF THE EU'S DATA PROTECTION REFORM

From a legitimacy perspective, the GDPR's legislative process highlights several aspects connected to the question of democratic deficit. The discussion

in chapter four explored how the different aspects of legitimacy, input, output, and throughput interact with the notion of democratic decision-making. While sceptics such as Scharpf (1999) and Coen (2007) have been unconvinced by the efforts to make the legislative process more inclusive and thus more democratic, Schmidt (2013), Kohler-Koch (2010), and Klüver (2013) have been more optimistic.

Before addressing whether stakeholder inclusion in policy processes can contribute to a higher degree of legitimacy, another aspect of the GDPR's legislative process is worth examining. Following Scharpf's (1999; see also Zahariadis, 2008) idea that input legitimacy emanates from a European policy discourse on privacy, how does one identify such a discourse, and how could it be translated to actual data protection regulation? One could argue that the two EU-wide Eurobarometer surveys on privacy and data protection (2011 and 2015) were used to identify the building blocks of an EU-wide notion of privacy and data protection. In lack of a collective identity and an EU-wide policy discourse, the two surveys reconstructed the main opinions of the European constituency via a representative sample in each member state. While it is obvious that a survey cannot be equated with public discourse, representative samples can serve as a proxy for a 'European mood' (Zahariadis, 2008) or public sentiments (Campbell, 2004, pp. 96-98).

The obvious problem with this notion of legitimacy is that the GDPR does not fully correspond to the answers given in the surveys. For example, a clear majority of the respondents believed consent should be required before personal information is collected and processed (European Commission, 2015a, p. 59). A few replied affirmatively concerning personal information on the Internet. Approximately one in ten thought that consent should be required only for sensitive information. Only 5% replied 'no'. While especially the Commission made some efforts to strengthen the consent mechanism, it has always been clear that several other legal bases for processing would be made available. Furthermore, the unpopularity of the ePrivacy Directive and its cookie notifications indicates that while people say that they want to control their personal information, they do not want to be informed of the intricacies of the online advertising economy but simply wish that controllers of personal information respect their privacy. Therefore, contrary to Utz and Krämer (2009), I would argue that the real privacy paradox is not that people's views on privacy contrast their actions but that people believe they want control when in reality they just want their reasonable expectations of privacy to be fulfilled.

Noting that this type of input only appeared to have a limited effect on the draft proposal, the idea of including stakeholders in the legislative process

needs to be connected to the other notions of legitimacy. To begin with, it is worth distinguishing between the two approaches to interest representative inclusion in the legislative process. First, are stakeholders included to represent populations to compensate for a lacking Europe-wide policy discourse (Scharpf, 1999) or to deliver a diversity of arguments in a deliberative process (Kohler-Koch, 2010; Quittkat & Kohler-Koch, 2013)? The legitimacy of the GDPR's legislative process is completely dependent on whether one accepts the former or the latter notion of policy input. Schmidt's (2013) concept of throughput legitimacy would be more inclined to accept the second view rather than the first.

I will address the legitimacy of the GDPR by considering both notions of legitimacy, looking at the representativeness of interest groups as well as the diversity of arguments. On the outset, it is easy to concede to Scharpf's critique of the EU's lack of legitimacy when looking at the GDPR. The results from chapter six revealed that a majority of the participants to the public consultations represented private interests rather than the public interest, and in the first consultation, most of them did not even bother to dress up their arguments in more general terms or public interest frames. The later stages of the legislative process, outlined in chapter seven, were even more dominated by industry lobbyists because these had better means to access decision-makers.

The presence of industry lobbyists is especially problematic when actors that are primarily engaged in profit and data extraction from the EU have a very limited local presence but still seek to influence the contents of legislation. The public consultations showed that companies headquartered in the U.S. participated to a very high degree. Many of these companies have a European presence, and it would obviously not be possible to exclude them from the public consultations simply because of where their headquarters are based. Nevertheless, the lack of participation from many of the Eastern member states combined with the fact that the U.S.-based companies mainly seek to advance the flow of personal data from the EU leads to a situation wherein the suggested proposals that undermine the privacy rights of EU residents heavily outnumber the ones that are more focused on the protection of privacy.

If the outstated goal with an updated piece of legislation is to counter the challenges associated with the globalisation of data flows and the risks involved (European Commission, 2010a), including the lobbyists that participate in these activities is questionable. Moreover, including stakeholders whose very activities one seeks to harmonise with the public interest is problematic (Bellamy, 2010). Their participation cannot be motivated by deliberative ideals but must instead be based on ideas of

representation: as these actors will be regulated by the new law, it is only reasonable that they should have a say in the process, regardless of how counterintuitive it is for the goals of the legislation.

Nevertheless, how far should one enable such participation? Is the automotive industry fit to suggest amendments to regulation on petrol tax? Should actors that provide offshore letter-box companies be able to weigh in on tax reform? Are the corporations that benefit from the privatisation of healthcare the right actors to suggest how public procurements should be conducted? While it is reasonable to consult with affected parties to avoid completely unfeasible solutions, institutionalising their participation does not contribute to a higher level of legitimacy.

Even if one accepts the view that interest representatives are granted access to the legislative process not because of their ability to represent large swaths of the population but because of their ability to bring forth interesting arguments and a diversity to the discussions (Kohler-Koch, 2010; Quittkat & Kohler-Koch, 2013), it begs the question of whether the actors engaged in the exploitation and export of personal data should be equally able to shape the contents of an instrument that has an outstated goal to enhance the protection of privacy as cause groups whose very missions are to advance fundamental rights. An obvious argument against this critique is that the free movement of data is *also* the stated goal of the original Data Protection Directive and subsequently the GDPR. However, the free movement of data was added to the title by the Council on recommendation by industry lobbyists (Bennett & Raab, 1997). This shows the importance of symbolic victories on the operational level, providing a framework for more concrete applications that do not seek to advance the protection of privacy rights but rather enable data processing and exchange.

Nevertheless, as many policy researchers are keen to point out, access does not always correspond with influence (Dür & Mateo, 2012). If one looks not only at access and participation but also at the policy output, the results look slightly different. A comparison between the output of the interest representatives and the output of the EU institutions shows that both business networks and civil society organisations appear to have been quite successful. A closer look at the Commission's proposed regulation and the Parliament's and Council's amendments to the same reveal that while civil society was clearly not as well represented as business interests in the consultations, their input seems to have been taken into account to a high degree. Therefore, the way DG Justice handled the input from interest representatives appears to be consistent with throughput legitimacy – regardless of the unevenness of participation, the policy output was quite balanced.

To some extent, civil society appears to have represented a supranational public interest that was also accepted by the EU legislature. As the respective membership bases of different cause groups are somewhat limited in scope, it can be deduced that their main contribution was deliberative and discursive rather than representative. Therefore, the unevenness of participation was counteracted by the quality of the policy proposals, at least to some degree. While it would be overconfident to argue that this is indicative of the deliberative function of the public consultations – I argue that no compromise can be reached with such incompatible interests – it does mitigate the effects of heavily one-sided lobbying.

However, the examination of the legitimacy of a legislative process does not end with the Commission's proposal. The role of outside influence is notably very different in the three EU institutions. This has consequences for the throughput aspect of legitimacy. While stakeholders can be formally included by the Commission, the later stages of the legislative process are rather unfettered by these procedural innovations to introduce more deliberation to the decision-making process.

Upon closer analysis, it is more accurate to say that the *lack of* institutional inclusion of interest representatives in the later stages of the GDPR's process proved to be more detrimental to its legitimacy. For example, how individual MEPs had copied extensively from lobbyists' proposals was only possible to see through leaked proposals. These cases revealed that party adherence was highly indicative of the position an MEP might hold. Furthermore, the question of influence can be answered affirmatively on the individual level, but as a collective, the Parliament's first reading can be perceived as overly supportive of neither industry interests nor privacy advocates but rather a mix of the two.

The Parliament's position was also affected by two factors: that the rapporteur, Jan-Philipp Albrecht, was an outspoken privacy activist and that the Snowden revelations surfaced at the time of drafting. This result is consistent with institutionalist arguments that both the role of policy entrepreneurs and windows of opportunity need to be considered (Peters, 2012; Zahariadis, 1995, 2008; Kingdon, 2013). Nevertheless, it challenges Pierson's (2000) and Mahoney's (2000) notion that events early in the process would be more important than later events: the Snowden revelations came quite late in the process. Moreover, it appears that no window of opportunity was needed to water down the legislation, which would be consistent with earlier research on lobbying that stresses lack of salience as a contributing factor to business success (Dür, Marshall, & Bernhagen, 2019, p. 106; Culpepper, 2010; Rasmussen, 2015). From a legitimacy perspective, it is

unsatisfactory that balanced policy output is dependent on such pivotal windows of opportunity.

While the lobbying of MEPs was made more transparent owing to the MEPs that actively leaked lobby position papers, it is blatantly obvious that the full force of lobbying that took place after the Commission had submitted its draft proposal has little to do with deliberation and a lot to do with the access goods that interest groups provide (Bouwen, 2002): money, policy expertise, and the support of politicians' constituencies. Moreover, there is little-to-no public insight into how interest representatives engaged with the Council.

The Council's role is the most apparent challenge to the legislative process's legitimacy. No lobby proposals provided to the Council were leaked to the public, but a closer examination of the Council's positions revealed that its suggested amendments were highly reminiscent of the positions held by free data lobbyists – with some exceptions. Overall, very little information is available on the interactions of the ministers of the Council and lobbyists. Moreover, the Council's draft contained a wide variety of exceptions and weakened safeguards with reference to national laws, largely undermining the effort of creating a unitary data protection framework across the EU.

Therefore, whether the throughput legitimacy of the legislative process can be increased as long as the initiatives are restricted to the agenda-setting stage of policy-making is doubtful. Making access to EU politicians conditional on registering to the Transparency Register (2019) is an important step that has not yet materialised.

Thus, it is important to not only document meetings with interest representatives but also make the actual policy proposals that they put forth accessible to the general public. Estimating to what extent lobbyists and advocates are successful in influencing decision-makers is only possible by comparing the input of interest representatives with the output of the EU institutions (cf. Dür, Bernhagen, & Marshall, 2019; Klüver, 2013).

Although the methodological approach taken here, process tracing with the help of qualitative document analysis and automated text searches, has proven to be efficient for determining how concepts and frames find their way into the policy output of the EU institutions, it is possible that some connections go unnoticed. Furthermore, the approach is cumbersome and requires policy expertise – in other words, it does not scale, and applying it to evaluate the influence of all possible lobbyists in all possible policy domains is not realistic. This approach could perhaps be automated using calibrated antiplagiarism software, but as noted in chapter five, automated approaches are less apt at finding conceptual similarities and do not differentiate between meaningless

stylistic amendments and important changes. Nevertheless, regardless of the methodology one uses to assess influence, the informal open consultation procedure where interest representatives can provide open-ended solutions to their perceived policy problems is highly valuable from a transparency perspective, and it makes tracing the positions of interest representatives possible.

8.3 DISCUSSION

This purpose of this study has been to delve into the GDPR's legislative process to gain deeper understanding of the politics of datafication and how the contents of data protection policy is shaped by the actors involved, external events, and the institutionalisation of stakeholder involvement in EU decision-making. This study has both theoretically and empirically addressed the two research questions related to the (1) policy congruence between the applications and their ideational underpinnings put forth by interest representatives and the EU institutions and the (2) legitimacy of the legislative process and the influence of interest representatives.

The contribution to the literature on EU studies can be summarised as follows. First, this study has proved that the interest group studies that exclude the examination of how national regulators influence regulatory proposals ignore a critical element of policy-making in the EU. Having a broader perspective that also includes public authorities is absolutely necessary. Slaughter's (2005) emphasis on the role of regulators in transnational regulatory reform is a good starting point. Second, I have provided additional nuance for understanding the comparative successes of business networks and cause groups. I argue that cause groups are much more dependent on both a friendly DG and public salience than business groups. This is demonstrated by the relative success that privacy advocates had in introducing policy applications in the Commission's proposal despite being visibly outnumbered in the public consultations. Moreover, the industry lobbyists were successful in watering down the GDPR in the Parliament prior to the Snowden revelations. The privacy proponents in the Parliament did not manage to turn the tide until then. While this confirms Dür, Marshall, and Bernhagen's (2019) results that businesses tend to lose when an issue enjoys high salience, it also demonstrates that cause groups are much more dependent on salience than what Dür, Marshall, and Bernhagen seem to suggest, consistent with Culpepper's (2010) approach to explaining influence.

Third, the party affiliation of the MEPs and the ministers in the Council is highly indicative of which type of lobbyists the politicians listen to. Politicians on the centre/right end of the spectrum are much more likely to be influenced by business networks than cause groups, at least in the f data protection policy domain.

Fourth, as this study has suggested that the Council and the governments of member states are the most susceptible to the influence of free data lobbyists, attention should be devoted to examining how Internet policy lobbyists operate and engage with the national representations and whether increasing the transparency of this aspect of the EU's legislative process would be possible. Future work should focus on these issues, and a natural continuation of this study would be to explore the composition of lobbying networks within the Internet policy domain. Using freedom of information requests, assessing the interactions between leading politicians and lobbyists within these countries would be possible.

The practical implications for this dissertation are that further attention is devoted to the conversation on the transparency of the Council, that the studies on how national lobbying of Internet policy contributes to EU reform enrich the picture sketched here, and that my contribution highlights the urgent need for a compulsory Transparency Register.

While I have demonstrated that the deliberative ideals of participatory democracy failed to materialise, it appears that the institutional inclusion of powerful actors in the early stages of the policy formulation process did not overly upset the balance of interests and disproportionally favour free data lobbyists. Rather, legitimacy issues emerged at later stages of the process. There are several explanations for this.

First, the entrepreneurial role of data protection regulators needs to be considered. They steered the legislative process of the Data Protection Directive (Newman, 2008a, 2008b), and their opinions were taken into account to a high degree in the Commission's draft GDPR – both collectively, as the WP29, and individually, as consulted parties in the 2002 review of the Data Protection Directive as well as individual contributors to the public consultations in 2009 and 2011. Second, the outstated agenda of DG Justice and Commissioner Reding was to advance the rights and interests of citizens related to the fundamental right of data protection. The outcome would have been very different had DG Internal Market or DG Connect been given the responsibility to draft the new proposal. Evidently, the fact that DG Justice provided the secretariat of the WP29 had an impact on this outcome. Finally, notwithstanding the superior resources of industry lobbyists, privacy

advocates with a presence in the EU could still participate in targeted consultations and were generally well received by the friendly Commission.

Taking into consideration the disproportionate influence of the Council on the final GDPR and the Council's tendency to promote free data lobbyists' suggestions, the most worrisome is not the institutional inclusion of interest representatives in the agenda-setting stage but the lack of institutionalised access in the last steps of the process. By way of national representation, governments are to a certain extent perceived as legitimate from an input perspective; however, as Follesdal and Hix (2006) note, such a position does not adequately consider that governments are rarely elected because of their stance on EU issues – or if they are, as the Brexit negotiations have demonstrated, the political campaigns have little to do with the realities and consequences of EU policy. To alleviate this apparent lack of input legitimacy, more focus could be devoted towards achieving throughput legitimacy by making the Transparency Register mandatory. Moreover, the register should include a database on all submitted proposals by lobbyists and proper documentation on Council ministers' meetings with lobbyists.

Ultimately, the strong attempt to counter the negative effects of societal datafication that materialised in the Commission's proposal was largely undone by the Council, although the Snowden revelations managed to at least shift the Parliament's position and slightly improve their bargaining position. While the GDPR may in many respects be perceived as path-dependent of earlier data protection policy in the EU, it did not succeed in fundamentally upending privacy-invasive practices. Moreover, while expanding bureaucratic proceduralism compared with the Data Protection Directive can be instrumental in achieving incremental change, it does not appear to have caused a systematic overhaul of data handling practices. The lack of radical policy change, despite windows of opportunity, knowledgeable policy entrepreneurs in the form of DPAs, a friendly DG, and an even friendlier Parliamentary rapporteur, is telling. These factors did not lead to significantly stronger data protection, with a few exceptions: the extra-territorial application of EU data protection regulation, stronger sanctions, and more powers to regulators. Therefore, the lack of change cannot be attributed to lack of involvement of a wide degree of actors but the resistance represented by European governments and their propensity to align their position with those of business lobbyists.

Looking at the broader societal context sheds light on why the Council would favour such an approach. In addition to testing the legitimacy claims for including interest representatives in the EU's legislative process, the goal of this study has been to explore the role of paradigms in the discursive

intuitionalist tradition, aiming to demonstrate how they shape, structure, and constrain the available policy options.

From the late 1980s onwards, surveillance scholars have highlighted how society has evolved from the panoptic diagram described by Foucault (1977) into a surveillance society focused on data collection (De Landa, 1991), profiling (Gandy, 1989), and prediction (Lyon, 1994; Andrejevic, 2012). The rationale has undoubtedly changed, where the psychological awareness of surveillance appears to be less important than the information one can mine from the data. One of the theoretical ambitions of this study has been to demonstrate that surveillance, big data, and the bureaucratisation of both private and public organisations are inherently interconnected and that their infrastructures overlap. While the concept of datafication is useful in describing the ways in which social relations are datafied and commodified and the uses of personal data are normalised (cf. van Dijck, 2014), I argue that the current technological landscape encapsulates a paradigm shift that is connected to the earlier aspirations to increase the bureaucratisation of societal institutions.

The rationales are mutually supportive. Datafication is instrumental in explaining the online advertising economy and the surveillance innovation complex. However, the rationale for processing personal data is equally connected to a discourse most commonly associated with the resource efficiency that is integral for understanding the role of personal data in bureaucratic power and control (Weber, 1978; Dandeker, 1994). After all, the surveillant aspects of personalisation technologies and behavioural targeting are seen as inherent necessities for achieving the functional goals of relevancy, rationality, and efficiency, whereas the parties that engage in these practices argue that the information, and by extension the individual, is of no functional interest to the entity engaged in processing personal data. This is also why data protection regulation, although instrumental in providing people with the rights associated with data concerning them, will ultimately be insufficient in challenging the big data paradigm because other strong societal interests are at play.

While, as I argue in chapter three, the development of privacy legislation is connected to countering the negative aspects of societal datafication, it is fundamentally reactive in nature. Technological change, not the gradual shifts in attitudes to privacy, has forced legislators to act. Notions of privacy have been quite stable the past few years (Pew Research Center, 2015a, 2015b, 2016; European Commission, 2015a; Turow, 2003; Debatin, Lovejoy, Horn, & Hughes, 2009; Halbert & Larsson, 2015; Kennedy, Elgesem, & Miguel, 2015), yet the chasm between what is perceived as permissible uses of personal

information and what is actually being collected appears to only grow wider. Data protection legislation has not tried to fully reflect people's notions of privacy owing to economic and security interests. The twin goal of data protection is a case in point. The fact that the twin goal also rests on ideas of deepening European integration means that not only does the right to privacy face significant obstacles in the form of innovation and security discourse but also that it is challenged by one of the core norms of the European project.

Informational self-determination appears to be in line with what people want, but the policies exclusively focused on such an approach might not be efficient. Owing to the nature of personal data as a right rather than property, consent mechanisms alone will never be sufficient for the vast array of services that rely on the supply of at least some personal information. Taxation, welfare benefits, and health care cannot, by definition, rely on consent, but neither can telecommunications services. The idea of limiting certain types of personal data to specific contexts that are perceived as socially acceptable according to Nissenbaum's (2010) contextual integrity framework is a fruitful starting point when looking at other legitimate grounds for processing. To some extent, such 'appropriate information flows' have been included in the GDPR by way of data minimisation and purpose limitation requirements, but the list of exceptions is long. For example, owing to the carte blanche given to scientific research, any pictures uploaded to cloud services, even private albums, could be used for training facial recognition algorithms. Moreover, in practice, controllers are heavily incentivised to solicit consent for their processing: once consent has been given, it is possible to go further than when one relies on the other legal grounds.

The situation is further complicated by the fact that software is increasingly connected to remote servers and consumer products are connected to the Internet to a high degree. Actions that previously took place locally are now processed in the cloud, which enables interception while the information is being communicated as well as access to the data being processed on remote servers. This not only raises security concerns for the public authorities that use cloud-powered software in their daily operations but also can have consequences for private individuals. Cloud services prompt a convenience dilemma because many of their functions are undoubtedly useful and disabling them will impair the functionality of the software. From the perspective of data protection regulation, data associated with such software use also trigger the 'expanding gas' issue raised by Ohm (2010) and other American privacy scholars, namely that the way personal data is defined in the GDPR will include all kinds of technical data, a concern voiced in the data protection public consultations by computer security firm Symantec.

Nevertheless, although a wider category of data types is regarded as personal data in contrast with how personally identifiable information is defined in the U.S., the GDPR simultaneously enables their use with reference to other legal grounds than consent.

This leads back to one of the most fundamental observations of this study: addressing the issue of data protection by simply contrasting the 'citizen rights' with 'business interests' or the 'public interest' with 'private interests' is impossible. The same arguments for sharing information across borders are put forth by the UK Ministry of Justice and Acxiom; it is only the underlying goal that changes. Interests overlap even when purposes do not. Public and private bureaucracies share the same ambitions to collect, share, and process data, which undoubtedly resulted in weaker provisions in the final GDPR. A fundamental challenge to privacy legislation is that exceptions granted with one situation in mind apply more broadly than perhaps first intended. For example, the right to data portability is limited by intellectual property rights to avoid corporate espionage with the help of data subject rights, but it is much more likely that the exceptions can be used in other circumstances to prevent access to personal data. The same issue applies to the broad research exception in general. Therefore, the question of how the GDPR should be enforced will be of utmost importance, especially considering the increased powers of DPAs and the new EDPB. Their interpretation of data protection regulation will impact practical applications to a very high degree.

In the first eight months of the GDPR's entry into force, 95,000 complaints were lodged with the European regulators. [86] The outcomes of these complaints will not only determine the effectiveness of the GDPR but also reveal significant differences between national DPAs. This should be jointly assessed with an examination of how the EDPB operates and whether the EU member state power relations are translated into the power dynamics of the Board. Owing to their strategic positions within the online economy, special attention should be devoted to the DPAs in Ireland, Germany, France, and the UK.

As I have demonstrated, the global dimensions of Internet policy lobbying materialised in practice in the GDPR's legislative process, and there is little indication that it was an exception but rather a demonstration of how future regulatory proposals within this domain will be met with global interest. The lobbying surrounding the new ePrivacy Regulation is testimony to this. The Corporate Europe Observatory (2017) quoted a Parliamentary insider stating

[86] The number was quoted in a Joint Statement by First Vice-President Timmermans, Vice-President Ansip, and Commissioners Jourová and Gabriel (European Commission, 2019).

that it was 'one of the worst lobby campaigns I have ever seen'. By focusing on the GDPR's legislative process, the ambition has been to demonstrate how Internet policy lobbying shapes regulation in practice, a conversation which has been more widespread within civil society than academia. Further attention needs to be devoted towards looking at how competition regulation impacts datafication, the role of discrimination regulation in examining how social or economic disadvantages overlap with data protection policy, and analysing whether the principles of accountability, fairness, and due process can withstand the efficiency arguments of datafication.

REFERENCES

Albrecht, J. P. (2016). Regaining Control and Sovereignty in the Digital Age. In D. Wright & P. De Hert (Eds.), *Enforcing Privacy: Regulatory, Legal and Technological Approaches* (pp. 473-488). Cham: Springer International Publishing. Retrieved from https://doi.org/10.1007/978-3-319-25047-2_20

Alexandrova, P., & Carammia, M. (2017). Agenda-setting in the European Union. In N. Zahariadis & L. Buonanno (Eds.), *Routledge handbook of European public policy* (pp. 288-298). Florence: Routledge.

Andrejevic, M. (2002). The work of being watched: interactive media and the exploitation of self-disclosure. *Critical Studies in Media Communication, 19*(2), 230-248. https://doi.org/10.1080/07393180216561

Andrejevic, M. (2012). Ubiquitous surveillance. In K. Ball, K. D. Haggerty, & D. Lyon (Eds.), *Routledge handbook of surveillance studies* (pp. 91-98). London: Routledge.

Andreou, A., Venkatadri, G., Goga, O., Gummadi, K. P., Loiseau, P., & Mislove, A. (2018). Investigating Ad Transparency Mechanisms in Social Media: A Case Study of Facebook's Explanations. In *Proceedings 2018 Network and Distributed System Security Symposium*. San Diego, CA: Internet Society. Retrieved from https://doi.org/10.14722/ndss.2018.23191

Armstrong, K. A., & Bulmer, S. (1998). *The Governance of the Single European Market*. Manchester: Manchester University Press.

Arthur, W. B. (1994). *Increasing returns and path dependence in the economy*. University of Michigan Press.

Article 29 Working Party. (2003). Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, WP 74. Retrieved 20 Feb, 2019, from https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp74_en.pdf

Article 29 Working Party. (2007). Opinion Nº 4/2007 on the concept of personal data, WP 136. Retrieved 2 March, 2015, from http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf

Article 29 Working Party (2008). Working Document setting up a framework for the structure of Binding Corporate Rules. Retrieved 11 October, 2016, from https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2008/wp154_en.pdf

Article 29 Working Party. (2010). Opinion 3/2010 on the principle of accountability, WP 173.

Article 29 Working Party. (2011). Opinion 15/2011 on the definition of consent, WP 187. Retrieved 24 January, 2016, from http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf

Article 29 Working Party. (2014). Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC. Retrieved 19 January, 2016, from http://ec.europa.eu/justice/data-

protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf

Athique, A. (2018). The dynamics and potentials of big data for audience research. *Media, Culture & Society, 40*(1), 59-74. https://doi.org/10.1177/0163443717693681

Auletta, K. (2009). *Googled – The End of the World as We Know It*. New York: The Penguin Press.

Baines, J. (2018, August 16). Via LinkedIn - @ICOnews has revealed in an #FOI response that it has spent £1.34m so far on its data analytics investigations. *Twitter.com*. Retrieved 21 August, 2018, from https://twitter.com/bainesy1969/status/1030063026051923970

Barocas, S., & Nissenbaum, H. (2014). Big Data's End Run around Anonymity and Consent. In J. Lane, V. Stodden, S. Bender, & H. Nissenbaum (Eds.), *Privacy, Big Data, and the Public Good: Frameworks for Engagement* (pp. 44-75). Cambridge: Cambridge University Press. Retrieved from doi:10.1017/CBO9781107590205.004

Baumgartner, F. R., & Mahoney, C. (2008). The two faces of framing: individual-level framing and collective issue-definition in the EU. *European Union Politics*, 9(3), 435–49.

Bellamy, R. (2010). Democracy without democracy? Can the EU's democratic 'outputs' be separated from the democratic 'inputs' provided by competitive parties and majority rule? *Journal of European Public Policy, 17*(1), 2-19. https://doi.org/10.1080/13501760903465256

Benford, R. D., & Snow, D. A. (2000). Frame processes and social movements. *Annual Review of Sociology, 26*(1), 611-639.

Bennett, A., & Checkel, J. T. (2014). Process tracing. In A. Bennett & J. T. Checkel (Eds.), *Process Tracing* (pp. 3-38). Cambridge: Cambridge University Press.

Bennett, A., & Elman, C. (2006). Complex Causal Relations and Case Study Methods: The Example of Path Dependence. *Political Analysis, 14*(3), 250-267. Retrieved from JSTOR.

Bennett, C. J., & Raab, C. D. (1997). The Adequacy of Privacy: The European Union Data Protection Directive and the North American Response. *The Information Society, 13*(3), 245-264. https://doi.org/10.1080/019722497129124

Bermejo, F. (2007). *The Internet Audience: Constitution and Measurement*. New York: Peter Lang Inc., International Academic Publishers.

Bermejo, F. (2009). Audience manufacture in historical perspective: from broadcasting to Google. *New Media & Society, 11*(1-2), 133-154. https://doi.org/10.1177/1461444808099579

Bernhagen, P. (2012). Who Gets What in British Politics – and How? An Analysis of Media Reports on Lobbying around Government Policies, 2001–7. *Political Studies, 60*(3), 557-577. https://doi.org/10.1111/j.1467-9248.2011.00916.x

Bernhagen, P., Dür, A., & Marshall, D. (2015). Information or context: What accounts for positional proximity between the European Commission and lobbyists? *Journal of European Public Policy, 22*(4), 570-587. https://doi.org/10.1080/13501763.2015.1008556

Beyers, J. (2002). Gaining and Seeking Access. The European Adaptation of Domestic Interest Associations. *European Journal of Political Research, 41*(5), 585-612.

Beyers, J., Eising, R., & Maloney, W. (2008). Researching Interest Group Politics in Europe and Elsewhere: Much We Study, Little We Know? *West European Politics*, *31*(6), 1103-1128. https://doi.org/10.1080/01402380802370443

Bitonti, A. (2017). The Role of Lobbying in Modern Democracy: A Theoretical Framework. In A. Bitonti & P. Harris (Eds.), *Lobbying in Europe* (pp.17-30). London: Palgrave Macmillan.

Bloomfield, L. (2016). Wcopyfind 4.1.5. Retrieved 12 March, 2017, from https://plagiarism.bloomfieldmedia.com/software/wcopyfind/

Boerman, S. C., Kruikemeier, S., & Borgesius, F. J. Z. (2017). Online Behavioral Advertising: A Literature Review and Research Agenda. *Journal of Advertising, 46*(3), 363-376. https://doi.org/10.1080/00913367.2017.1339368

Bogard, W. (2012). Simulation and post-panopticism. In K. Ball, K. D. Haggerty, & D. Lyon (Eds.), *Routledge handbook of surveillance studies* (pp. 30-45). London: Routledge.

Bolin, G. (2012). The Labour of Media Use. *Information, Communication & Society, 15*(6), 796-814. https://doi.org/10.1080/1369118X.2012.677052

Bolin, G., & Andersson Schwarz, J. (2015). Heuristics of the algorithm: Big Data, user interpretation and institutional translation. *Big Data & Society, 2*(2), 2053951715608406. https://doi.org/10.1177/2053951715608406

Boräng, F., & Naurin, D. (2015). 'Try to see it my way!' Frame congruence between lobbyists and European Commission officials. *Journal of European Public Policy, 22*(4), 499-515.

Botsman, R. (2017, October 21). Big data meets Big Brother as China moves to rate its citizens. *Wired UK*. Retrieved 11 March, 2018, from https://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion

Bouk, D. (2018). *How Our Days Became Numbered: Risk and the Rise of the Statistical Individual (Reprint edition)*. Chicago: University of Chicago Press.

Bouwen, P. (2002). Corporate lobbying in the European Union: the logic of access. *Journal of European Public Policy, 9*(3), 365-390. https://doi.org/10.1080/13501760210138796

Bouwen, P. (2004). Exchanging access goods for access: a comparative study of business lobbying in the European Union institutions. *European Journal of Political Research, 43*(3), 337-369.

boyd, d., & Crawford, K. (2012). Critical Questions for Big Data. *Information, Communication & Society, 15*(5), 662-679. https://doi.org/10.1080/1369118X.2012.678878

Bradford, A. (2012). The Brussels Effect. *Northwestern University Law Review, 107*(1). Retrieved 19 July, 2016, from https://scholarship.law.columbia.edu/faculty_scholarship/271

Braman, S. (2006). *Change of State*. Cambridge, MA: MIT Press.

Brignull, H. (2019). What are dark patterns? Retrieved 5 February, 2019, from https://darkpatterns.org

Brown, I., & Korff, D. (2009). Terrorism and the Proportionality of Internet Surveillance. *European Journal of Criminology, 6*(2), 119-134. https://doi.org/10.1177/1477370808100541

Bucher, T. (2016). Neither black nor box: Ways of knowing algorithms. In S. Kubitschko Sebastian & A. Kaun (Eds.), *Innovative Methods in Media and Communication Studies* (pp. 81-98). London: Palgrave.

Bug, M. (2013). Societal Divisions Regarding Attitudes towards Digitized Security Measures? British versus German Perspectives. In M. Löblich & S. Pfaff-Rüdinger (Eds.), *Communication and Media Policy in the Era of the Internet* (pp. 159-174). Berlin: Nomos publishers.

Bunea, A. (2017). Designing stakeholder consultations: Reinforcing or alleviating bias in the European Union system of governance? *European Journal of Political Research, 56*(1), 46-69. https://doi.org/10.1111/1475-6765.12165

Burkart, P., & Andersson Schwarz, J. (2013). Post-privacy and ideology: a question of doxa and praxis. In A. Jansson & M. Christiansen (Eds.), *Media, Surveillance and Identity: A Social Perspective* (pp. 218-237). New York, NY: Peter Lang.

Burri, M., & Schär, R. (2016). The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy. *Journal of Information Policy, 6*, 479-511.

Burton, C., De Boel, L., Kuner, C., Pateraki, A., Cadiot, S., & Hoffman, S. G. (2016). The Final European Union General Data Protection Regulation. *BNA Privacy & Security Law Report, 15*, 153.

Campbell, J. L. (2004). *Institutional change and globalization*. Princeton: Princeton University Press.

Canhoto, A. I. (2013). Critical examination of the role of private actors in the fight against money laundering: the case of the UK retail banking industry. In K. Ball & L. Snider (Eds.), *The surveillance-industrial complex: A political economy of surveillance* (pp. 95-108). Routledge: London.

Carroll, B. (2017, May 29). Revealed: How Facebook chief, Sheryl Sandberg, lobbied Taoiseach Enda Kenny over data protection role and taxation. *The Independent*. Retrieved 6 March, 2019 from https://www.independent.ie/irish-news/revealed-how-facebook-chief-sheryl-sandberg-lobbied-taoiseach-enda-kenny-over-data-protection-role-and-taxation-35765139.html

Castelluccia, C. (2012). Behavioural Tracking on the Internet: A Technical Perspective. In S. Gutwirth, R. Leenes, P. De Hert, & Y. Poullet (Eds.), *European Data Protection: In Good Health?* (pp. 21-33). Dordrecht: Springer Netherlands. Retrieved from https://doi.org/10.1007/978-94-007-2903-2_2

Cavoukian, A. (2009). Privacy by Design: The 7 foundational principles. Retrieved 21 September, 2015, from https://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples.pdf

Cengiz, F. (2018). Bringing the citizen back into EU democracy: against the input-output model and why deliberative democracy might be the answer.

European Politics and Society, 19(5), 577-594. https://doi.org/10.1080/23745118.2018.1469236

Charlesworth, A. (2012). Data Protection, Freedom of Information and Ethical Review Committees. *Information, Communication & Society, 15*(1), 85-103. doi:10.1080/1369118X.2011.637572

Cheneval, F., Lavenex, S., & Schimmelfennig, F. (2015). *Demoi -cracy* in the European Union: principles, institutions, policies. *Journal of European Public Policy, 22*(1), 1-18. https://doi.org/10.1080/13501763.2014.886902

Christl, W. (2017). Corporate Surveillance in Everyday Life: How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions. *Vienna: Cracked Labs*. Retrieved from http://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf

Cisco. (2018). Cisco Global Cloud Index. Retrieved 29 January, 2019, from https://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/white-paper-c11-738085.html

Clarke, R. A. (1988). Information technology and dataveillance. *Communications of the ACM, 31*(5), 498-512.

CNIL. (2019). Data protection around the world. Retrieved 27 August, 2019, from https://www.cnil.fr/en/data-protection-around-the-world

Coen, D. (1997). The evolution of the large firm as a political actor in the European Union. *Journal of European Public Policy, 4*(1), 91-108.

Coen, D. (2007). Empirical and theoretical studies in EU lobbying. *Journal of European Public Policy, 14*(3), 333-345. doi:10.1080/13501760701243731

Coen, D., & Richardson, J. (2009). *Lobbying the European Union: Institutions, Actors, and Issues*. Oxford: Oxford University Press.

Cohen, J. (2011). [1989] Deliberation and democratic legitimacy. In J. Gripsrud, J. H. Moe, A. Molander et al. (Eds.), *The Public Sphere* (pp. 31-50). New York: Sage.

Cohen, J. E. (2012). *Configuring the Networked Self*. Yale University Press.

Cohen, J. E. (2016). The Surveillance-Innovation Complex: The Irony of the Participatory Turn. In D. Barney, G. Coleman, C. Ross, J. Sterne & T. Tembeck (Eds.), *The participatory condition in the digital age* (pp. 207-226). Minneapolis: University of Minnesota Press.

Coleman, J. S. (1990). *Foundations of Social Theory*. Cambridge, MA: Belknap Press.

Collier, D. (2011). Understanding Process Tracing. *PS: Political Science & Politics, 44*(04), 823-830. https://doi.org/10.1017/S1049096511001429

Committee on Civil Liberties, Justice and Home Affairs. (2012). Draft report on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011– C7-0025/2012– 2012/0011(COD)). Retrieved 28 November, 2015, from http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/922/922387/922387en.pdf

Connolly, C., & Van Dijk, P. (2016). Enforcement and Reform of the EU-US Safe Harbor Agreement. In D. Wright & P. De Hert, P. (Eds.), *Enforcing Privacy* (pp. 261-283). Cham: Springer International Publishing. Retrieved from https://doi.org/10.1007/978-3-319-25047-2

Corbett, A. (2005). *Universities and the Europe of Knowledge: Ideas, Institutions and Policy Entrepreneurship in European Union Higher Education Policy, 1955- 2005*. New York: Palgrave Macmillan.

Corporate Europe Observatory. (2019). Big Data is watching you. Retrieved 8 February, 2019, from https://corporateeurope.org/power-lobbies/2017/10/big-data-watching-you

Couldry, N., & Hepp, A. (2018). The continuing lure of the mediated centre in times of deep mediatization: Media Events and its enduring legacy. *Media, Culture & Society, 40*(1), 114-117.

Council of Europe. (2018). Chart of signatures and ratifications of Treaty 108. Retrieved 10 January, 2019, from https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=8Uysz6kT

Council of the European Union. (2015). Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (Preparation of a general approach 9565/15).

Council of the European Union (2016). Position of the Council at first reading with a view to the adoption of a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) - Statement of the Council's reasons – Adopted by the Council on 8 April 2016. ST 5419 2016 REV 1 ADD 1 - 2012/011 (OLP). Retrieved 12 September, 2019, from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=consil:ST_5419_2016_REV_1_ADD_1 .

Cram, L. (1997). *Policy-making in the EU*. London and New York: Routledge.

Culpepper, P. D. (2010). *Quiet Politics and Business Power: Corporate Control in Europe and Japan*. Cambridge: Cambridge University Press.

Dandeker, C. (1994). *Surveillance, Power and Modernity: Bureaucracy and Discipline from 1700 to the Present Day*. Cambridge: Polity.

De Bruycker, I. (2017). Framing and advocacy: A research agenda for interest group studies. *Journal of European Public Policy, 24*(5), 775-787. https://doi.org/10.1080/13501763.2016.1149208

De Landa, M. (1991). *War in the Age of Intelligent Machines*. New York: Zone.

Debatin, B., Lovejoy, J. P., Horn, A.-K., & Hughes, B. N. (2009). Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences. *Journal of Computer-Mediated Communication, 15*(1), 83-108. https://doi.org/10.1111/j.1083-6101.2009.01494.x

Dehousse, R. (1997). Regulation by Networks in the European Community: The Roleof European Agencies. *Journal of European Public Policy, 4*(2), 246-61.

Dehousse, R. (2003). The Open Method of Coordination: A New Policy Paradigm?. *Cahiers Européens de Sciences Po, 3*.

Deleuze, G. (1992). Postscript on the Societies of Control. *October, 59*, 3-7.

Democracy-film. (2018). Democracy – im Rausch der Daten. Retrieved 27 August, 2019, from http://www.democracy-film.de/

Deters, H. (2013). Process tracing in the development and validation of theoretical explanations: the example of environmental policy-making in the EU. *European Political Science, 12*(1), 75-85. https://doi.org/10.1057/eps.2012.11

Diamandouros, N. (2008). Openness and access to documents. *European State Aid Law Quarterly, 7*(4), 654-658.

Donders, K., Pauwels, C., & Loisen, J. (Eds.). (2014). *The Palgrave Handbook of European Media Policy*. Retrieved from https://doi.org/10.1057/9781137032195

Downs, A. (1957). *An Economic Theory of Democracy*. New York: Harper.

Duhigg, C. (2009, May 12). What Does Your Credit-Card Company Know About You? *The New York Times*. Retrieved 10 June, 2015, from https://www.nytimes.com/2009/05/17/magazine/17credit-t.html

Dunin-Wasowicz, J. K. (2009). The Transparency Regulation in Context: A Proxy for Legitimacy or an Instrument of Regulatory Practice. *Columbia Journal of European Law, 16*, 465.

Dür, A. (2008). Measuring Interest Group Influence in the EU: A Note on Methodology. *European Union Politics*, 9(4), 559–576. https://doi.org/10.1177/1465116508095151

Dür, A. (2009). Interest Groups in the European Union: How Powerful Are They? *West European Politics, 31*(6), 1212-1230. https://doi.org/10.1080/01402380802372662

Dür, A., & Mateo, G. (2012). Who lobbies the European Union? National interest groups in a multilevel polity. *Journal of European Public Policy, 19*(7), 969-987.

Dür, A., Marshall, D., & Bernhagen, P. (2019). *The Political Influence of Business in the European Union*. Ann Arbor: University of Michigan Press.

EDRI. (2015). Press Release: Privacy and Data Protection under threat from EU Council agreement. Retrieved 15 June, 2015, from https://edri.org/press-release-privacy-and-data-protection-under-threat-from-eu-council-agreement/

Egdell, J. M., & Thomson, K. J. (1999). The Influence of UK NGOs on the Common Agricultural Policy. *Journal of Common Market Studies, 37*(1), 121-131. https://doi.org/10.1111/1468-5965.00153

Eising, R. (2007). The access of business interests to EU institutions: towards élite pluralism?. *Journal of European Public Policy, 14*(3), 384-403. doi:10.1080/13501760701243772

Eising, R., Rasch, D., & Rozbicka, P. (2015). Institutions, policies, and arguments: Context and strategy in EU policy framing. *Journal of European Public Policy, 22*(4), 516-533. https://doi.org/10.1080/13501763.2015.1008552

Englehardt, S., Han, J., & Narayanan, A. (2018). I never signed up for this! Privacy implications of email tracking. *Proceedings on Privacy Enhancing Technologies, 2018*(1), 109-126. https://doi.org/10.1515/popets-2018-0006

Entman, R. M. (1993). Framing: Toward clarification of a fractured paradigm. *Journal of Communication, 43*(4), 51-58.

Essers, L. (2014, September 30). Germany orders Google to stop illegal user data processing. *PC World*. Retrieved 16 March, 2019, from https://www.pcworld.com/article/2689672/germany-orders-google-to-stop-illegal-user-data-processing.html.

Eur-lex. (2016). Procedure 2012/0011/COD. Retrieved 10 January, 2017, from http://eur-lex.europa.eu/procedure/EN/2012_11?qid=1526045053961&rid=1

Europe v. Facebook. (2014). Legal Procedure against "Facebook Ireland Limited". Retrieved 4 March, 2019, from http://www.europe-v-facebook.org/EN/Complaints/complaints.html

Europe v. Facebook. (2015). "PRISM" Complaints against Facebook, Apple, Skype, Microsoft and Yahoo!. Retrieved 4 March, 2019, from http://www.europe-v-facebook.org/EN/Complaints/Safe_Harbor/safe_harbor.html

European Commission. (2000). Proposal for a Regulation of the European Parliament and of the Council regarding public access to European Parliament, Council and Commission documents (Proposal for an act 52000PC0030). *Official Journal* C 177 E, 27.06.2000: 70-73.

European Commission. (2001). European governance (White Paper 52001DC0428). *Official Journal C* 287, 12.10.2001: 1-29.

European Commission. (2002). Towards a reinforced culture of consultation and dialogue - Proposal for general principles and minimum standards for consultation of interested parties by the Commission (Communication 52002DC0704).Retrieved 19 March, 2019, from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52002DC0704

European Commission. (2003a). Answers to the questionnaire addressed to the Supervisory Authority. (no longer accessible).

European Commission. (2003b). Answers to the questionnaire addressed to the Member States. (no longer accessible).

European Commission. (2003c). Your Views on Data Protection. Questionnaire for on the implementation of the Data Protection Directive (95/46/EC) Results of on-line consultation 20 June - 15 Sept. 2002. (no longer accessible).

European Commission. (2003d). Questionnaire for Data Controllers on the implementation of the Data Protection Directive (95/46/EC) Results of on-line consultation 20 June - 15 Sept. 2002. (no longer accessible).

European Commission. (2009). Legal framework: Consultation on the legal framework for the fundamental right to protection of personal data. Retrieved 22 October, 2014, from https://web.archive.org/web/20171026105125/http://ec.europa.eu/justice/newsroom/data-protection/opinion/090709_en.htm

European Commission. (2010a). Communication From the Commission to the European Parliament, the Council, the Economic And Social Committee and the Committee of the Regions: A comprehensive approach on personal data protection in the European Union (Brussels: 4.11.2010) (Communication 52010DC0609). Retrieved 19 March, 2019, from

https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:52010DC0609.

European Commission. (2010b). Summary of replies to the public consultation about the future legal framework for protecting personal data. (no longer accessible).

European Commission. (2011a). European Commission's comprehensive approach. Retrieved 19 March, 2019, from https://web.archive.org/web/20120228103631/http://ec.europa.eu/justice/newsroom/data-protection/opinion/101104_en.htm

European Commission. (2011b). Flash Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union. Retrieved 14 November, 2014, from http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf

European Commission. (2012a). Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (Proposal for an act 52012PC0011). Retrieved 14 March, 2014, from https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1552556267691&uri=CELEX:52012PC0011

European Commission. (2012b). Impact Assessment Accompanying the document Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) and Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data (Commission staff working paper SEC/2012/72).

European Commission. (2012c). Annexes to the impact assessment SEC/2012/72.

European Commission. (2013). Towards a European Horizontal Framework for Collective Redress (Communication 52013DC0401). Retrieved 30 November, 2018, from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52013DC0401

European Commission. (2014, March 12). Progress on EU data protection reform now irreversible following European Parliament vote. MEMO/14/186. Retrieved 14 November, 2014, from http://europa.eu/rapid/press-release_MEMO-14-186_en.htm

European Commission. (2015a). Special Eurobarometer 431: Data protection. Retrieved from doi:10.2838/552336

European Commission. (2015b). Better regulation for better results - An EU agenda (Communication 52015DC0215). Retrieved 14 March, 2019, from https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52015DC0215

European Commission. (2015c). Single Market Scoreboard. Retrieved 29 July, 2016, from http://ec.europa.eu/internal_market/scoreboard/performance_by_governance_tool/transposition/index_en.htm

European Commission. (2016a). Proposal for a Interinstitutional Agreement on a mandatory Transparency Register (Proposal for an act 52016PC0627). Retrieved 30 September, 2018, from https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1553004130005&uri=CELEX:52016PC0627

European Commission. (2016b). Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (notified under document C(2016) 4176) (Implementing decision 32016D1250). *OJ L 207*, 1.8.2016: 1-112.

European Commission. (2016c). Status of implementation of Directive 95/46 on the Protection of Individuals with regard to the Processing of Personal Data. Retrieved 29 July, 2016, from http://ec.europa.eu/justice/data-protection/law/status-implementation/index_en.htm

European Commission. (2018). Consultations. Retrieved 20 November, 2018, from https://ec.europa.eu/info/consultations_en?order_by_status=All&field_core_topics_target_id_entityreference_filter=All&page=49

European Commission. (2019, January 25). Joint Statement by First Vice-President Timmermans, Vice-President Ansip, Commissioners Jourová and Gabriel ahead of Data Protection Day. Retrieved 11 February, 2019, from http://europa.eu/rapid/press-release_STATEMENT-19-662_en.htm

European Data Protection Supervisor (2015). Annex to Opinion 3/2015: Comparative table of GDPR texts with EDPS recommendations. Retrieved 12 August, 2017, from https://edps.europa.eu/sites/edp/files/publication/15-07-27_gdpr_recommendations_annex_en_1.pdf.

European Parliament. (2013). Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (Report A7-0402/2013).

European Parliament. (2015). New EU rules on data protection put the citizen back in the driving seat (press release). Retrieved 12 September, 2019, from http://www.europarl.europa.eu/news/en/press-room/20151217IPR08112/new-eu-rules-on-data-protection-put-the-citizen-back-in-the-driving-seat

European Parliament. (2019). The Ordinary Legislative Procedure. Retrieved 12 September, 2019, from http://www2.europarl.europa.eu/ordinary-legislative-procedure/en/ordinary-legislative-procedure.html

Facebook. (2018a). Replies to the Senate Committee on the Judiciary. Retrieved from https://www.commerce.senate.gov/public/_cache/files/ed0185fb-615a-4fd5-818b-5ce050825a9b/62027BC70720678CBC934C93214B0871.senate-judiciary-combined-7-.pdf

Facebook. (2018b). Replies to the Senate Committee on Commerce, Science, and Transportation. Retrieved from https://www.commerce.senate.gov/public/_cache/files/9d8e069d-2670-4530-bcdc-

d3a63a8831c4/7C8DE61421D13E86FC6855CC2EA7AEA7.senate-commerce-committee-combined-qfrs-06.11.2018.pdf

Farrell, H., & Newman, A. L. (2019). *Of Privacy and Power: The Transatlantic Struggle over Freedom and Security*. Princeton, NJ: Princeton University Press.

Federal Trade Commission. (2014). Data brokers: a call for transparency and accountability. Retrieved 14 November, 2014, from https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf

Federal Trade Commission. (2018, March 26). Statement by the Acting Director of FTC's Bureau of Consumer Protection Regarding Reported Concerns about Facebook Privacy Practices. Retrieved 19 April, 2018, from https://www.ftc.gov/news-events/press-releases/2018/03/statement-acting-director-ftcs-bureau-consumer-protection

Ferretti, F. (2015). *Credit bureaus between risk-management, creditworthiness assessment and prudential supervision*. EUI Department of Law Research Paper No. 2015/20. Available from https://ssrn.com/abstract=2610142

Fischer-Hübner, S. (1998). Privacy and security at risk in the global information society, *Information, Communication & Society, 1*(4), 420-441. doi:10.1080/13691189809358981

Follesdal, A., & Hix, S. (2006). Why There is a Democratic Deficit in the EU: A Response to Majone and Moravcsik. *Journal of Common Market Studies, 44*(3), 533-562. https://doi.org/10.1111/j.1468-5965.2006.00650.x

Fontanella-Khan, J. (2013, June 26). Brussels: Astroturfing takes root. *Financial Times*. Retrieved 29 August, 2019, from https://www.ft.com/content/74271926-dd9f-11e2-a756-00144feab7de#axzz2XLjof7HR

Foucault, M. (1977). *Discipline and punish: the birth of the prison*. Translated from French by Alan Sheridan. London: Penguin Books.

Franks, B. (2015). What Is Big Data and Why Does It Matter? In B. Franks (Ed.), *Taming the Big Data Tidal Wave* (pp. 1-27). Hoboken: John Wiley & Sons, Ltd. Retrieved from https://doi.org/10.1002/9781119204275.ch1

Freedman, D. (2008). *The politics of media policy*. Cambridge: Polity.

Fuchs, C. (2012). Dallas Smythe Today - The Audience Commodity, the Digital Labour Debate, Marxist Political Economy and Critical Theory. *TripleC: Communication, Capitalism & Critique. Open Access Journal for a Global Sustainable Information Society, 10*(2), 692-740. https://doi.org/10.31269/triplec.v10i2.443

Fuchs, C. (2013). Political Economy and Surveillance Theory. *Critical Sociology, 39*(5), 671-687. https://doi.org/10.1177/0896920511435710

Gandy, O. H., Jr. (1989). The Surveillance Society: Information Technology and Bureaucratic Social Control. *Journal of Communication, 39*(3), 61-76. https://doi.org/10.1111/j.1460-2466.1989.tb01040.x

Gandy, O. H., Jr. (1993). *The Panoptic Sort: A Political Economy of Personal Information*. Boulder, CO: Westview Press.

Gandy, O. H., Jr. (2009). *Coming to Terms with Chance: Engaging Rational Discrimination and Cumulative Disadvantage.* London: Routledge.

Gandy, O. H., Jr. (2011). The Political Economy of Personal Information. In J. Wasko, G. Murdock & H. Sousa (Eds.), *The Handbook of Political Economy of Communications* (pp. 436-457). Oxford: Wiley-Blackwell.

Gandy, O. H., Jr. (2012). Remote sensing in the digital age. In K. Ball, K. D. Haggerty & D. Lyon (Eds.), *Routledge handbook of surveillance studies* (pp. 125-132). London: Routledge.

Giddens, A. (1985). *The Nation-State and Violence* (1st edn.). Berkeley: University of California Press.

Goldfarb, A., & Tucker, C. E. (2010). Privacy Regulation and Online Advertising. *Management Science, 57*(1), 57-71. https://doi.org/10.1287/mnsc.1100.1246

González Fuster G., & Gutwirth, S. (2013). Opening up personal data protection: A conceptual controversy. *Computer Law & Security Review*, 29(5), 531-539.

González Fuster, G. (2014). *The Emergence of Personal Data Protection as a Fundamental Right of the EU*. New York: Springer.

Greener, I. (2005). The Potential of Path Dependence in Political Studies. *Politics, 25*(1), 62-72. https://doi.org/10.1111/j.1467-9256.2005.00230.x

Greenwald, G. (2014). *No place to hide. Edward Snowden, the NSA and the Surveillance State.* London: Hamish Hamilton.

Greenwood, J. (2011a). The lobby regulation element of the European Transparency Initiative: Between liberal and deliberative models of democracy. *Comparative European Politics, 9*(3), 317-343. https://doi.org/10.1057/cep.2010.18

Greenwood, J. (2011b). Actors of the common interest? The Brussels offices of the regions. *Journal of European Integration, 33*(4), 437-451.

Greenwood, J. (2017). *Interest Representation in the European Union* (4th edn.). London: Red Globe Press.

Grossman, E. (2004). Bringing politics back in: rethinking the role of economic interest groups in European integration. *Journal of European Public Policy, 11*(4), 637-654. doi:10.1080/1350176042000248061

Habermas, J. (1999). *The Inclusion of the Other: Studies in Political Theory*. C. P. Cronin & P. D. Greiff (Eds.) (Reprint edition). Cambridge: The MIT Press.

Haggerty, K. D., & Ericson, R. V. (2000). The surveillant assemblage. *The British Journal of Sociology, 51*(4), 605-622. https://doi.org/10.1080/00071310020015280

Halbert, D., & Larsson, S. (2015). By Policy or Design? Privacy in the US in a Post-Snowden World. *Journal of Law, Technology and Public Policy, 1*(2), 1-17.

Harcourt, A. J. (1998). EU Media Ownership Regulation: Conflict over the Definition of Alternatives. *JCMS: Journal of Common Market Studies, 36*(3), 369-389. https://doi.org/10.1111/1468-5965.00115

Harcourt, A. J. (2005). *The EU and the Regulation of Media Markets*. Manchester: Manchester University Press.

Harlow, C. (2006). Global Administrative Law: The Quest for Principles and Values. *European Journal of International Law, 17*(1), 187-214. https://doi.org/10.1093/ejil/chi158

Hartzog, W. (2018). *Privacy's blueprint: the battle to control the design of new technologies*. Cambridge, MA: Harvard University Press.

Hayes-Renshaw, F. (2009). Least accessible but not inaccessible: Lobbying the Council and the European Council. In D. Coen and J. Richardson (Eds.), *Lobbying the European Union: institutions, actors, and issues* (pp. 70-88). Oxford: Oxford University Press.

Heinz, J. P., Laumann, E. O., Nelson, R. L., & Salisbury, R. H. (1993). *The Hollow Core: Private Interests in National Policy Making*. Cambridge, MA: Harvard University Press.

Hern, A., & Cadwalladr, C. (2018, April 13). Revealed: Aleksandr Kogan collected Facebook users' direct messages. *The Guardian*. Retrieved 1 March, 2019, from https://www.theguardian.com/uk-news/2018/apr/13/revealed-aleksandr-kogan-collected-facebook-users-direct-messages

Hesmondhalgh, D. (2012). *The Cultural Industries* (3rd edn.). London: Sage Publications Ltd.

Hildebrandt, M. (2006). Profiling: From data to knowledge: The challenges of a crucial technology. *Datenschutz Und Datensicherheit - DuD, 30*(9), 548-552. https://doi.org/10.1007/s11623-006-0140-3

Hildebrandt, M., & Gutwirth, S. (Eds.). (2008). Profiling the European Citizen. Dordrecht: Springer Netherlands. Retrieved from https://doi.org/10.1007/978-1-4020-6914-7

Hildén, J. (2017). Am I my IP address's keeper? Revisiting the boundaries of information privacy. *The Information Society, 33*(3), 159-171.

Hintz, A., Dencik, L., & Wahl-Jorgensen, K. (2018). *Digital Citizenship in a Datafied Society*. Cambridge: Polity.

Hirsch, M., & Petersen, V. G. (2007). Enlargement of the Arena: European Media Policy. In W. A. Meier and J. Trappel (Eds.), *Power, Performance and Politics* (pp. 21-39). Baden-Baden: Nomos Publishers.

Hoofnagle, C. J. (2018). Designing for Consent. *Journal of European Consumer and Market Law, 7*(4), 162-171.

Innis, H. A. (1951). *The Bias of Communication*. Toronto: University of Toronto Press.

Jääsaari, J., & Hildén, J. (2015). Piracy & Social Change: From File Sharing to Free Culture: The Evolving Agenda of European Pirate Parties. *International Journal of Communication*, 9, 870–889.

Järvinen, H. (2015). EU Data Protection Package – Lacking ambition but saving the basics. *EDRi.org*. Retrieved 12 September, 2019, from https://edri.org/eu-data-protection-package-lacking-ambition-but-saving-the-basics/

Jin, D. Y., & Feenberg, A. (2015). Commodity and Community in Social Networking: Marx and the Monetization of User-Generated Content. *The Information Society, 31*(1), 52-60. https://doi.org/10.1080/01972243.2015.977635

Kaltheuner, F. (2018, May 24). Privacy is power. *Politico*. Retrieved 26 May, 2018, from http://edition.pagesuite-professional.co.uk/html5/reader/production/default.aspx?pubname=&pubid=926f0c8c-7f9b-4c0c-a74d-25af040856bf, 14-15

Kalyanpur, N., & Newman, A. L. (2019). The MNC-Coalition Paradox: Issue Salience, Foreign Firms and the General Data Protection Regulation. *JCMS: Journal of Common Market Studies*, 57(3), 448-467.

Kennedy, H., Elgesem, D., & Miguel, C. (2015). On fairness: User perspectives on social media data mining. *Convergence: The International Journal of Research into New Media Technologies, 23*(3), 270-288. https://doi.org/10.1177/1354856515592507

Kim, T., Barasz, K., & John, L. K. (2019). Why Am I Seeing This Ad? The Effect of Ad Transparency on Ad Effectiveness. *Journal of Consumer Research, 45*(5), 906-932. https://doi.org/10.1093/jcr/ucy039

Kingdon, J. W. (2013). Agendas, Alternatives, and Public Policies, Update Edition, with an Epilogue on Health Care: Pearson New International Edition (2nd edn.). Harlow, United Kingdom: Pearson.

Kint, J., Mills Wade, A., Chavern, D., & Newell, D. (2018). Publisher Letter to Google re GDPR Terms. Retrieved 5 February, 2019, from https://digitalcontentnext.org/wp-content/uploads/2018/04/Publisher-Letter-to-Google-re-GDPR-Terms-042918.pdf

Kitchin, R. (2014). Big Data, new epistemologies and paradigm shifts. *Big Data & Society, 1*(1), 2053951714528481. https://doi.org/10.1177/2053951714528481

Klüver, H. (2013). *Lobbying in the European Union: Interest Groups, Lobbying Coalitions, and Policy Change*. Oxford: Oxford University Press. Retrieved from https://doi.org/10.1093/acprof:oso/9780199657445.001.0001

Klüver, H., & Mahoney, C. (2015). Measuring interest group framing strategies in public policy debates. *Journal of Public Policy, 35*(2), 223-244. https://doi.org/10.1017/S0143814X14000294

Klüver, H., Braun, C., & Beyers, J. (2015). Legislative lobbying in context: towards a conceptual framework of interest group lobbying in the European Union. *Journal of European Public Policy*, 22(4), 447–461, DOI: 10.1080/13501763.2015.1008792

Klüver, H., Mahoney, C., & Opper, M. (2015). Framing in context: how interest groups employ framing to lobby the European Commission. *Journal of European Public Policy, 22*(4), 481-498. doi:10.1080/13501763.2015.1008550

Kohler-Koch, B. (1997). Organized Interests in the EC and the European Parliament. *European Integration Online Papers, 1*(9).

Kohler-Koch, B. (2010). Civil society and EU democracy: "astroturf" representation?. *Journal of European Public Policy, 17*(1), 100-116. https://doi.org/10.1080/13501760903464986

Kokott, J., & Sobotta, C. (2013). The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR. *International Data Privacy Law, 3*(4), 222-228. https://doi.org/10.1093/idpl/ipt017

Koops, B.-J. (2014). The trouble with European data protection law. *International Data Privacy Law, 4*(4), 250-261. https://doi.org/10.1093/idpl/ipu023

Korff, D. (2002). EC Study on Implementation of Data Protection Directive (Study Contract ETD/2001/B5-3001/A/49). Retrieved 29 July, 2016, from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1287667

Kosinski, M., Stillwell, D., & Graepel, T. (2013). Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences, 110*(15), 5802-5805. https://doi.org/10.1073/pnas.1218772110

Koskenniemi, M. (2004). International law and hegemony: a reconfiguration. *Cambridge Review of International Affairs, 17*(2), 197-218. https://doi.org/10.1080/0955757042000245852

Kreiken, F. (2016a). The lobby-tomy 3: who are lobbying? *Edri.org*. Retrieved 23 September, 2018, from https://edri.org/the-lobby-tomy-3-who-are-lobbying/

Kreiken, F. (2016b). The lobby-tomy 9: Lessons of the lobby. *Edri.org*. Retrieved 23 September, 2018, from https://edri.org/lobby-tomy-9-lessons-of-the-lobby/

Laney, D. (2001, February 6). 3D Data Management: Controlling Data Volume, Velocity and Variety. *Meta Group / Gartner*. Retrieved 14 November, 2014, from http://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf

Lauer, J. (2017). *Creditworthy: A History of Consumer Surveillance and Financial Identity in America.* New York: Columbia University Press. Retrieved from https://doi.org/10.7312/laue16808

Laurer, M. & Seidl, T. (*forthcoming*). Regulating the European Data-Driven Economy: A Case Study on the General Data Protection Regulation. Unpublished.

Lehmann, W. (2009). The European Parliament. In D. Coen & J. Richardson (Eds.), *Lobbying the European Union: institutions, actors, and issues* (pp. 39-69). Oxford: Oxford University Press.

Lessig, L. (2006). *Code (Version 2.0)*. New York: Basic Books.

Levin, A. (2018). Privacy by Design by Regulation: The Case Study of Ontario. *Canadian Journal of Comparative and Contemporary Law,* 115-160.

Lobbyplag.eu. (2013). Influence. Retrieved 10 October, 2013, from http://lobbyplag.eu/influence

Lobbyplag.eu. (2014). Transparency for the EU. Retrieved 14 November, 2014, from http://lobbyplag.eu/lp

Lobbyplag.eu. (2016). Governments. Retrieved 24 November, 2017, from http://lobbyplag.eu/governments

Löfgren, K., & Webster, C. W. R. (2009). Policy Innovation, Convergence and Divergence: Considering the Policy Transfer Regulating Privacy and Data Protection in Three European Countries. *Information Polity, 14*(4), pp. 279-298. doi:10.3233/IP-2009-0188

Lupton, D., & Williamson, B. (2017). The datafied child: The dataveillance of children and implications for their rights. *New Media & Society, 19*(5), 780-794. https://doi.org/10.1177/1461444816686328

Lyon, D. (1994). *The electronic eye: The rise of surveillance society*. Minneapolis: University of Minnesota Press.

Mahoney, C. (2007). Networking vs. allying: the decision of interest groups to join coalitions in the US and the EU. *Journal of European Public Policy, 14*(3), 366-383. doi:10.1080/13501760701243764

Mahoney, J. (2000). Path Dependence in Historical Sociology. *Theory and Society, 29*(4), 507-548.

Majone, G. (2005). *Dilemmas of European Integration*. Oxford: Oxford University Press. Retrieved from https://doi.org/10.1093/0199274304.001.0001

Majone, G. (2014a). From Regulatory State to a Democratic Default: From regulatory state to a democratic default. *Journal of Common Market Studies, 52*(6), 1216-1223. https://doi.org/10.1111/jcms.12190

Majone, G. (2014b). Rethinking the Union of Europe Post-Crisis: Has Integration Gone Too Far? Retrieved from https://doi.org/10.1017/CBO9781107477766

Marsden, C. T. (2011). *Internet co-regulation: European law, regulatory governance and legitimacy in cyberspace*. Cambridge: Cambridge University Press.

Marx, K. (1867/1984). *Capital. A Critique of Political Economy*. *Volume 1*. New York: New World. Retrieved from http://www.marxists.org/archive/marx/works/download/Marx_Capital_Vol_1.pdf

Mayer-Schönberger, V., & Cukier, K. (2013). *Big Data: A Revolution That Will Transform How We Live, Work and Think*. London: John Murray.

McKay, A. (2012). Buying Policy? The Effects of Lobbyists' Resources on Their Policy Success. *Political Research Quarterly, 65*(4), 908-923. Retrieved from JSTOR.

McKeon, M. (2010). The Evolution of Privacy on Facebook. Retrieved 29 November, 2016, from http://mattmckeon.com/facebook-privacy/.

McQuail, D., & Sinue, K. (Eds.) (1998). *Media Policy: Convergence, Concentration and Commerce*. London: SAGE.

Meehan, E. R. (2002). Gendering the commodity audience: Critical media research, feminism, and political economy. In E. Meehan, & E. Riordan (Eds.), *Sex and Money: Feminism and Political Economy in the Media* (pp. 209-222). Minneapolis: University of Minnesota Press.

Meehan, E. R. (2005). Watching television: A political economic approach. In J. Wasko (Ed.), *A Companion to Television* (pp. 238-55). Malden, MA: Blackwell.

Michalis, M. (2007). *Governing European Communications*. Lanham, MD: Lexington.

Michalowitz, I. (2007). What determines influence? Assessing conditions for decision-making influence of interest groups in the EU. *Journal of European Public Policy, 14*(1), 132-151.

Mistreanu, S. (2018, April 3). Life Inside China's Social Credit Laboratory. *Foreign Policy*. Retrieved 15 March, 2019, from http://foreignpolicy.com/2018/04/03/life-inside-chinas-social-credit-laboratory/

Moravcsik, A. (2002). Reassessing legitimacy in the European Union. *Journal of Common Market Studies, 40*(4), 603-624.

Morth, U. (2000). Competing frames in the European Commission—The case of the defence industry and equipment issue. *Journal of European Public Policy, 7*(2), 173-189. https://doi.org/10.1080/135017600343151

Mosco, V. (2009). *The Political Economy of Communication* (2nd edn.). London: SAGE Publications Ltd. Retrieved from https://doi.org/10.4135/9781446279946

Napoli, P. M. (2001). *Foundations of Communications Policy. Principles and Process in the Regulation of Electronic Media*. Cresskill, NJ: Hampton Press.

Napoli, P. M. (2010). *Audience Evolution: New Technologies and the Transformation of Media Audiences*. New York: Columbia University Press.

Napoli, P. M. (2016). The Audience as Product, Consumer, and Producer in the Contemporary Media Marketplace. In G. F. Lowe & C. Brown (Eds.), *Managing Media Firms and Industries* (pp. 261-275). Berlin: Springer.

Narayanan, A., & Reisman, D. (2017). The Princeton Web Transparency and Accountability Project. In T. Cerquitelli, D. Quercia & F. Pasquale (Eds.), *Transparent Data Mining for Big and Small Data* (Vol. 32, pp. 45-67). Cham: Springer International Publishing. Retrieved from https://doi.org/10.1007/978-3-319-54024-5_3

Neuvonen, R. (2014). *Yksityisyyden suoja Suomessa*. Helsinki: Lakimiesliiton kustannus.

Newman, A. L. (2008a). Building Transnational Civil Liberties: Transgovernmental Entrepreneurs and the European Data Privacy Directive. *International Organization, 62*(1), 103-130.

Newman, A. L. (2008b). *Protectors of Privacy: Regulating Personal Data in the Global Economy*. Ithaca: Cornell University Press.

Nicolaïdis, K. (2013). European Demoicracy and Its Crisis: European demoicracy and its crisis. *Journal of Common Market Studies, 51*(2), 351-369. https://doi.org/10.1111/jcms.12006

Nissenbaum, H. (2010). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, CA: Stanford Law Books.

Nissenbaum, H. (2011). A Contextual Approach to Privacy Online. *Daedalus, 140*(4), 32-48.

Norris, C., de Hert, P., L'Hoiry, X., & Galleta, A. (Eds.) (2017). *The unaccountable state of surveillance: Exercising access rights in Europe*. (Law, Governance and Technology Series; Vol. 34). Cham (Switzerland): Springer International.

North, D. C. (1990). *Institutions, Institutional Change and Economic Performance*. Cambridge: Cambridge University Press. Retrieved from https://doi.org/10.1017/CBO9780511808678

Obar, J. A. (2015). Big Data and The Phantom Public: Walter Lippmann and the fallacy of data privacy self-management. *Big Data & Society, 2*(2), 2053951715608876. https://doi.org/10.1177/2053951715608876

Ohm, P. (2010). Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. *UCLA Law Review, 57*(2010), 1701-1778.

O'Neil, C. (2016). *Weapons of math destruction: How big data increases inequality and threatens democracy*. New York: Broadway Books.

Online Etymology Dictionary. (2014). *Surveillance*. Retrieved 8 January, 2015, from http://www.etymonline.com/index.php?term=surveillance&allowed_in_frame=0

Organization for Economic Co-operation & Development [OECD]. (1980). Council Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, OECD Doc.C(80)(58) final (Oct. 1, 1980).

Palmås, K. (2011). Predicting what you'll do tomorrow: Panspectric surveillance and the contemporary corporation. *Surveillance & Society, 8*(3), 338-354. https://doi.org/10.24908/ss.v8i3.4168

Panizza, F., & Miorelli, R. (2013). Taking Discourse Seriously: Discursive Institutionalism and Post-structuralist Discourse Theory. *Political Studies, 61*(2), 301-318. https://doi.org/10.1111/j.1467-9248.2012.00967.x

Papacharissi, Z. A. (2010). *A Private Sphere: Democracy in a Digital Age* (1st edn.). Cambridge: Polity.

Pappi, F. U., & Henning, C. H. C. A. (1999). The organization of influence on the EC's common agricultural policy: A network approach. *European Journal of Political Research, 36*(2), 257-281. https://doi.org/10.1111/1475-6765.00470

Parltrack (2016). 2012/0011(COD). Retrieved 3 February, 2017, from http://parltrack.euwiki.org/dossier/2012/0011%28COD%29

Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Cambridge, MA: Harvard University Press.

Patel, N. (2019, July 12). Facebook's $5 billion FTC fine is an embarrassing joke. *The Verge*. Retrieved 3 October, 2019, from https://www.theverge.com/2019/7/12/20692524/facebook-five-billion-ftc-fine-embarrassing-joke.

Peters, B. G. (1994). Agenda-setting in the European community. *Journal of European Public Policy, 1*(1), 9-26. https://doi.org/10.1080/13501769408406945

Peters, B. G. (2012). *Institutional theory in political science: The new institutionalism* (3rd edn.). New York, NY: The Continuum International Publishing Group.

Peters, B. G., Pierre, J., & King, D. S. (2005). The Politics of Path Dependency: Political Conflict in Historical Institutionalism. *Journal of Politics, 67*(4), 1275-1300. https://doi.org/10.1111/j.1468-2508.2005.00360.x

Pew Research Center. (2015a). *Americans' Attitudes About Privacy, Security and Surveillance*. Retrieved 25 April, 2017, from http://www.pewinternet.org/files/2015/05/Privacy-and-Security-Attitudes-5.19.15_FINAL.pdf

Pew Research Center. (2015b). *Americans' Privacy Strategies Post-Snowden*. Retrieved 25 April, 2017, from http://www.pewinternet.org/files/2015/03/PI_AmericansPrivacyStrategies_0316151.pdf

Pew Research Center. (2016). *Privacy and Information Sharing*. Retrieved 25 April, 2017, from http://assets.pewresearch.org/wp-content/uploads/sites/14/2016/01/PI_2016.01.14_Privacy-and-Info-Sharing_FINAL.pdf

Pierson, P. (2000). Increasing returns, path dependence, and the study of politics. *The American Political Science Review, 94*(2), 251-267. https://doi.org/10.2307/2586011

Poster, M. (1990). *The Mode of Information: Poststructuralism and Social Context* (1st edn.). Chicago: University of Chicago Press.

Pridmore, J., & Zwick, D. (2011). Editorial - Marketing and the Rise of Commercial Consumer Surveillance. *Surveillance & Society, 8*(3), 269-277. https://doi.org/10.24908/ss.v8i3.4163

Quittkat, C. (2011). The European Commission's online consultations: a success story?. *Journal of Common Market Studies, 49*(3), 653-674.

Quittkat, C., & Kohler-Koch, B. (2013). *De-Mystification of Participatory Democracy: EU-Governance and Civil Society*. Oxford: Oxford University Press.

Raab, C. D. (2010). Information Privacy: Networks of Regulation at the Subglobal level. *Global Policy, 1*(3), 291-302.

Rasmussen, M. K. (2015). The Battle for Influence: The Politics of Business Lobbying in the European Parliament. *Journal of Common Market Studies, 53*(2), 365-382.

Reiman, J. H. (1976). Privacy, Intimacy, and Personhood. *Philosophy and Public Affairs, 6*(1), 26-44.

Rein, M., & Schön, D. (1994). *Frame reflection: Toward the resolution of intractable policy controversies*. New York: Basic Book.

Reuters. (2017, July 28). Why Google and Facebook Prove the Digital Ad Market Is a Duopoly. *Fortune*. Retrieved 30 July, 2017, from http://fortune.com/2017/07/28/google-facebook-digital-advertising/

Richardson, J. (2000). Government, interest and policy change. *Political Studies, 48*(5), 1006-28.

Rittberger, B. (2007). *Building Europe's Parliament: Democratic Representation Beyond the Nation-State*. Oxford: Oxford University Press.

Rossi, A. (2018). How the Snowden Revelations Saved the EU General Data Protection Regulation, *The International Spectator*, 53(4), 95–111, DOI: 10.1080/03932729.2018.1532705

Rule, J. B. (1974). *Private Lives and Public Surveillance: Social Control in the Computer Age*. New York: Shocken Books.

Ryan, J. (2019, February 20). New evidence filed in RTB complaint. *Fixadtech*. Retrieved 3 March, 2019, from https://fixad.tech/wp-content/uploads/2019/02/4-appendix-on-market-saturation-of-the-systems.pdf

Sabatier, P. A. (1998). The advocacy coalition framework: revisions and relevance for Europe. *Journal of European Public Policy, 5*(1), 98-130. doi:10.1080/13501768880000051

Scharpf, F. W. (1997). *Games real actors play: actor-centered institutionalism in policy research*. Boulder, Colorado: Westview Press.

Scharpf, F. W. (1999). *Governing in Europe: Effective and Democratic?* Oxford: Oxford University Press. Retrieved from https://doi.org/10.1093/acprof:oso/9780198295457.001.0001

Schmidt, V. A. (2006). *Democracy in Europe*. Oxford: Oxford University Press. Retrieved from https://doi.org/10.1093/acprof:oso/9780199266975.001.0001

Schmidt, V. A. (2008). Discursive institutionalism: The explanatory power of ideas and discourse. *Annual Review of Political Science, 11*, 303-326.

Schmidt, V. A. (2010). Taking ideas and discourse seriously: explaining change through discursive institutionalism as the fourth 'new institutionalism'. *European Political Science Review, 2*(1), 1-25.

Schmidt, V. A. (2013). Democracy and Legitimacy in the European Union Revisited: Input, Output and 'Throughput.' *Political Studies, 61*(1), 2-22. https://doi.org/10.1111/j.1467-9248.2012.00962.x

Schneier, B. (2015). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* (1st edn.). New York, N.Y: W. W. Norton & Company.

Schwartz, P. M. (2013). The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures. *Harvard Law Review, 126*(7), 1966-2013.

Scott, W. R. (2014). *Institutions and organizations: Ideas, interests and identities*. Thousand Oaks, California: SAGE.

Searls, D. "Doc". (2018a, March 23). Facebook's Cambridge Analytica problems are nothing compared to what's coming for all of online publishing [*Doc Searls Weblog*]. Retrieved 24 April, 2018, from https://blogs.harvard.edu/doc/2018/03/23/nothing/

Searls, D. "Doc". (2018b, May 12). GDPR will pop the adtech bubble. [*Doc Searls Weblog*]. Retrieved 24 April, 2018, from http://blogs.harvard.edu/doc/2018/05/12/gdpr/

Shah, R. C., & Sandvig, C. (2008). Software defaults as de facto regulation: The case of the wireless internet. *Information, Communication & Society, 11*(1), 25-46. https://doi.org/10.1080/13691180701858836

Simitis, S. (1995). From the market to the polis: The EU Data Protection Directive on the protection of personal data. *Iowa Law Review, 80*(3), 445-469.

Simitis, S. (2010). Privacy—An Endless Debate. *California Law Review*, 98, 1989–2006.

Simpson, S., Puppis, M., & Van den Bulck, H. (Eds.) (2016). *European Media Policy for the 21st Century: Assessing the Past, Setting Agendas for the Future*. New York/London: Routledge.

Slaughter, A-M. (2005). *A New World Order*. Princeton, NJ: Princeton University Press.

Smismans, S. (2014). Regulating interest group participation in the European Union: Changing paradigms between transparency and representation. *European Law Review, 39*(4), 470-492.

Smythe, D. W. (1977). Communications: blindspot of western Marxism. *CTheory*, *1*(3), 1-27.

Teinowitz, I. (2007, September 27). Microsoft: DoubleClick Deal Will Bring New Meaning to "Being Googled". *AdAge*. Retrieved 16 March, 2019, from https://adage.com/article/digital/microsoft-doubleclick-deal-bring-meaning-googled/120800/

Tene, O., & Polonetsky, J. (2013). A theory of creepy: technology, privacy and shifting social norms. *Yale Journal of Law and Technology, 16*, 59.

Thelen, K. (2009). Institutional Change in Advanced Political Economies. *British Journal of Industrial Relations, 47*(3), 471-498. https://doi.org/10.1111/j.1467-8543.2009.00746.x

Thomas, R., & Turnbull, P. (2017). Talking up a storm? Using language to activate adherents and demobilize detractors of European Commission policy frames. *Journal of European Public Policy, 24*(7), 931-950. https://doi.org/10.1080/13501763.2016.1162831

Transparency Register. (2019). Transparency and the EU. Retrieved 28 August, 2019, from http://ec.europa.eu/transparencyregister

Turow, J. (1997). *Breaking Up America: Advertisers and the New Media World* (1st edn.). Chicago: University of Chicago Press.

Turow, J. (2003). *Americans Online Privacy: The System Is Broken*. A report from The Annenberg Public Policy Center of the University of Pennsylvania.

Turow, J. (2006). *Niche Envy: Marketing Discrimination in the Digital Age*. Cambridge, MA: MIT Press.

Turow, J. (2011). *The Daily You: How the New Advertising Industry Is Defining Your Identity and Your Worth*. New Haven: Yale University Press.

Turow, J., Hennessy, M., & Draper, N. (2015). The Tradeoff Fallacy: How Marketers Are Misrepresenting American Consumers and Opening Them Up to Exploitation. *Annenberg School for Communication*. Retrieved from https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf

Utz, S., & Krämer, N. C. (2009). The privacy paradox on social network sites revisited: The role of individual characteristics and group norms. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 3*(2). https://cyberpsychology.eu/article/view/4223

Van Dijck, J. (2013). *The Culture of Connectivity: A Critical History of Social Media*. New York: Oxford University Press.

Van Dijck, J. (2014). Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveillance & Society, 12*(2), 197-208. https://doi.org/10.24908/ss.v12i2.4776

Van Dijck, J., Poell, T., & De Waal, M. (2018). The platform society: Public values in a connective world. Oxford University Press.

van Hulst, M., & Yanow, D. (2016). From Policy "Frames" to "Framing": Theorizing a More Dynamic, Political Approach. *The American Review of*

Public Administration, 46(1), 92-112. https://doi.org/10.1177/0275074014533142

Venturelli, S. (2002). Inventing e-regulation in the US, EU and East Asia: conflicting social visions of the Information Society. *Telematics and Informatics, 19*(2), 69-90. https://doi.org/10.1016/S0736-5853(01)00007-7

Voltolini, B., & Eising, R. (2017). Framing processes and lobbying in EU foreign policy: case study and process-tracing methods. *European Political Science, 16*(3), 354-368. https://doi.org/10.1057/eps.2016.18

Warren, S. D., & Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review, 4*(5), 193-220.

Weber, M. (1978). *Economy and Society: An Outline of Interpretive Sociology*. Berkeley: University of California Press.

Webster, C. W. R. (2012). Public administration as surveillance. In K. Ball, K.D. Haggerty & D. Lyon (Eds.), *Routledge handbook of surveillance studies* (pp. 313-320). London: Routledge.

Webster, J. G. (2014). *The Marketplace of Attention: How Audiences Take Shape in a Digital Age*. Cambridge, MA: MIT Press.

Weiler, J. H. H., Haltern, U. R., & Mayer, F. C. (1995). European democracy and its critique. *West European Politics, 18*(3), 4-39. https://doi.org/10.1080/01402389508425089

Westin, A. F. (1967). *Privacy and freedom* (1st edn.). New York: Atheneum.

Whiteley, P. F., & Winyard, S. J. (1987). *Pressure for the Poor: The Poverty Lobby and Policy Making*. London: Routledge.

Whitman, J. Q. (2004). The Two Western Cultures of Privacy: Dignity versus Liberty. *The Yale Law Journal, 73*, 1151-1222.

Woll, C. (2006). Lobbying in the European Union: From sui generis to a comparative perspective. *Journal of European Public Policy, 13*(3), 456-469.

Wong, J. C. (2018, April 11). Congress grills Facebook CEO over data misuse – as it happened. *The Guardian*. Retrieved 12 April, 2018, from https://www.theguardian.com/technology/live/2018/apr/10/mark-zuckerberg-testimony-live-congress-facebook-cambridge-analytica

WPP. (2016). WPP's Data Alliance and Spotify announce global data partnership. Retrieved 1 April, 2017, from http://www.thedataalliance.com/blog/wpps-data-alliance-and-spotify-announce-global-data-partnership/

Wright, D. (2016). Enforcing Privacy. In D. Wright & P. De Hert (Eds.), *Enforcing Privacy: Regulatory, Legal and Technological Approaches* (pp. 13-49). Cham: Springer International Publishing. Retrieved from https://doi.org/10.1007/978-3-319-25047-2_2

Zahariadis, N. (1995). *Markets, states, and public policy: Privatization in Britain and France*. Ann Arbor: University of Michigan Press.

Zahariadis, N. (2008). Ambiguity and choice in European public policy. *Journal of European Public Policy, 15*(4), 514-530. https://doi.org/10.1080/13501760801996717

Zuboff, S. (2018). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. Campus: Berlin.

Zwick, D., & Denegri Knott, J. (2009). Manufacturing Customers: The database as new means of production. *Journal of Consumer Culture, 9*(2), 221-247. https://doi.org/10.1177/1469540509104375

LEGAL SOURCES

INTERNATIONAL TREATIES

Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5.

Council of Europe, Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data, 28 January 1981, ETS 108.

UN General Assembly, *International Covenant on Civil and Political Rights*, 16 December 1966, United Nations, Treaty Series, vol. 999, p. 171.

UNITED STATES

U.S. Const. amend. IV.

Foreign Intelligence Surveillance Act of 1978 ("FISA" Pub.L. 95–511, 92 Stat. 1783, 50 U.S.C. ch. 36)

EUROPEAN UNION

Charter of Fundamental Rights of the European Union, *Official Journal C 326, 26.10.2012, 391–407*.

Consolidated version of the Treaty on the Functioning of the European Union. *Official Journal C 326, 26.10.2012, 47–390*.

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, *Official Journal* L 281 *23.11.1995: 31–50*.

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), *Official Journal* L 178, 17.7.2000: 1–16.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), *Official Journal* L 201, *Official Journal L 201, 31.7.2002, 37–47*.

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services

or of public communications networks and amending Directive 2002/58/EC. *Official Journal* L 105, 13.4.2006: 54–63.

Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 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 (Text with EEA relevance). *Official Journal* L 337, 18.12.2009: 11–36.

Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents. *Official Journal* L 145, 31.5.2001: 43–48.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). *Official Journal* L 119, 4.5.2016: 1–88.

ECTHR CASE-LAW

Bărbulescu v. Romania, App. No. 61496/08, Eur. Ct. H.R. (Grand Chamber, 2017). Available at http://hudoc.echr.coe.int/eng?i=001-177082.

EU CASE-LAW

Judgment of 20 February 1979, Rewe-Zentral v Bundesmonopolverwaltung für Branntwein ("Cassis de Dijon"), Case 120/78, EU:C:1979:42.

Judgement of 8 April 2014, Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Ireland and the Attorney General, C-293/12, EU:C:2014:238.

Judgment of 13 May 2014, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, C-131/12, EU:C:2014:317.

Judgment of 6 October 2015, Maximillian Schrems v Data Protection Commissioner, C-362/14, EU:C:2015:650.

APPENDIX

Appendix 1 Position papers chosen for qualitative analysis.[87]

2009 consultation (n=23)	2011 consultation (n=44)
RESEARCH	
	Data Protection Centre for Socio-Legal Studies at the University of Oxford
BUSINESS LOBBYING	
United States Chamber of Commerce (AmCham)	United States Chamber of Commerce (AmCham)
Confederation of British Industry (CBI)	Data Security Council of India (DSCI)
	Japan Business Council in Europe
	General Electric Company (US)
CONSUMER / CITIZEN INTERESTS NGOS	
The European Consumer Organisation (BEUC)	The European Consumer Organisation (BEUC)
European Digital Rights (EDRI)	European Digital Rights Initiative (EDRI)
Privacy International (UK)	Privacy International (UK)
INSURANCE	
	Comité Européen des Assurances (CEA) (Insurance Europe from 2012)
MARKETING	
IAB Europe	IAB Europe
	World Federation of Advertisers (WFA)
	Data Industry Platform
	EFAMRO and ESOMAR (joint reply)
DATA BROKERAGE	
Acxiom (US)	World-Check, acquired by Thomson Reuters in 2011
Centre for Information Policy Leadership (CIPL), Hunton & Williams LLP	Centre for Information Policy Leadership (CIPL), Hunton & Williams LLP

[87] The topics are instructive and do not fully correspond to the categorisation in the full position paper tables in chapter 6. Some of the categories in this table are made up of several sectors.

European Privacy Officers Forum (EPOF), Hunton & Williams LLP	European Association of Directory and Database Publishers (EADP)
IT	
Business Software Alliance (BSA) Digital Europe	Business Software Alliance (BSA) Digital Europe Symantec (US) European Game Developers' Forum (EGDF) Microsoft (US)
SOCIAL MEDIA	
	Facebook (US)
PUBLIC AUTHORITES & GOVERNMENTS	
Ministry of Justice (UK) Dutch Government (NL) Article 29 Working Party & Working Party on Police and Justice	Ministry of Justice (UK) Ministry of Justice (LV) Datainspektionen (SE) Federal Trade Commission (FTC) (US) European Data Protection Supervisor (EDPS)
TRADE UNIONS AND TRADE ASSOCIATIONS	
	European Trade Union Confederation (ETUC) UNI Europa Le Conseil Des Barreaux Europeens (CCBE) Bar Council of England And Wales
COPYRIGHT INDUSTRIES	
Joint reply by the European Newspaper Publishers Association (ENPA) and the European Federation of Magazine Publishers (FAEP)	International Federation of the Phonographic Industry (IFPI)
Joint reply by the Motion Picture Association (MPA),the International Video Federation (IVF), the International Federation of Film Distributors Associations (FIAD) and the International Federation of Film Producers Associations (FIAPF)	MPA, IVF, FIAD, and FIAPF (joint response)

	Association of Commercial Television (ACT) European Broadcasting Union (EBU) BBC (UK)
HEALTHCARE	
National Information Governance Board for Health and Social Care (NIGB) (UK)	Finnish National Welfare Authority THL (FIN)
Association of Clinical Research Organizations (ACRO) (US)	Johnson & Johnson (US)
INTERNET SERVICE PROVIDERS	
European Telecommunications Network Operators' Association (ETNO)	European Telecommunications Network Operators' Association (ETNO)
EuroISPA Telefonica SA (ES)	EuroISPA
FINANCE AND CREDIT INSTITUTIONS	
Visa (US)	British Bankers' Association (BBA) and Association for Financial Markets in Europe (AFME)
European Banking Federation (EBF)	European Banking Federation (EBF)
AVIATION	
	International Air Transport Association (IATA)
RETAIL	
	Carrefour (FR)

Appendix 2 File Comparison Report

Produced by WCopyfind.4.1.5 with the following settings:

Shortest Phrase to Match: 6
Fewest Matches to Report: 5
Ignore Punctuation: No
Ignore Outer Punctuation: No
Ignore Numbers: No
Ignore Letter Case: Yes
Skip Non-Words: No

Skip Long Words: No
Most Imperfections to Allow: 2
Minimum % of Matching Words: 80

WCopyfind.4.1.5 found 51 matching pairs out of 73 documents.

Perfect Match	Overall Match	File L	File R
521 (4% L, 5% R)	545 (5%) L; 539 (5%) R	Parl only amendments_2all.docx	1212_EuroISPA_contribution.pdf
865 (8% L, 4% R)	902 (8%) L; 909 (4%) R	Parl only amendments_2all.docx	20121026_Drafting-recommendations_IMCO-draft-opinion_final.pdf
453 (4% L, 2% R)	479 (4%) L; 476 (2%) R	Parl only amendments_2all.docx	ACCIS_Position%20Paper%20on%20Proposed%20Data%20Protection%20Regulation%20May%202012.pdf
133 (1% L, 3% R)	143 (1%) L; 141 (3%) R	Parl only amendments_2all.docx	ACCIS-DP-Amendments-Position-Paper_FINAL.pdf
244 (2% L, 5% R)	253 (2%) L; 253 (5%) R	Parl only amendments_2all.docx	Agoria_Stellungnahme%20zu%20Delegated%20Acts_02102012.pdf
634 (6% L, 4% R)	669 (6%) L; 657 (4%) R	Parl only amendments_2all.docx	amazon_letter_26_1.pdf
634 (6% L, 4% R)	669 (6%) L; 657 (4%) R	Parl only amendments_2all.docx	AMAZON-amendments.pdf
1198 (11% L, 3% R)	1263 (12%) L; 1260 (3%) R	Parl only amendments_2all.docx	AmCham_EU_Proposed_Amendments_on_Data_Protection.pdf

347 (3% L, 6% R)	361 (3%) L; 354 (6%) R	Parl only amendments_2all.docx	BITKOM%20Amendments.docx
56 (0% L, 2% R)	56 (0%) L; 56 (2%) R	Parl only amendments_2all.docx	BITKOM%20Self%20regulation.docx
334 (3% L, 6% R)	351 (3%) L; 342 (6%) R	Parl only amendments_2all.docx	BITKOM_Amendments%20GDPR_final.pdf
334 (3% L, 6% R)	351 (3%) L; 342 (6%) R	Parl only amendments_2all.docx	bmi_auskunft.pdf
400 (3% L, 7% R)	421 (4%) L; 430 (7%) R	Parl only amendments_2all.docx	BT-Amendments-DP-Regulation-08112012-FIN.pdf
233 (2% L, 6% R)	242 (2%) L; 241 (6%) R	Parl only amendments_2all.docx	CLOUD-Amendments-Telefo%CC%81nica-Nov.pdf
550 (5% L, 7% R)	581 (5%) L; 576 (8%) R	Parl only amendments_2all.docx	COCIR-Amendments-on-the-General-Data-Protection-Regulation-_-Final_25-October-2012.pdf
706 (6% L, 10% R)	736 (7%) L; 736 (10%) R	Parl only amendments_2all.docx	COM-Rapporteur-Bits%20of%20Freedom.pdf
1107 (10% L, 3% R)	1153 (11%) L; 1154 (4%) R	Parl only amendments_2all.docx	D1391E-2012-EBF-Amendments-to-EC-Proposal-for-a-Regulation-on-Data-Protection-31.10.12.pdf
205 (1% L, 3% R)	214 (2%) L; 216 (3%) R	Parl only amendments_2all.docx	D2153B-2012-EBF%20position%20on JURI%20draft%20opinion%20on%20EC%20Pro

			posal%20for%20a%20Regulation%20on%20Data%20Protection.pdf
1265 (12% L, 3% R)	1325 (12%) L; 1320 (3%) R	Parl only amendments_2all.docx	DIGITALEUROPE_Amendments-to-Data-Protection-Regulation_final.pdf
172 (1% L, 9% R)	184 (1%) L; 178 (9%) R	Parl only amendments_2all.docx	eBay-recommendation-ahead-of-IMCO-vote.pdf
1699 (16% L, 4% R)	1771 (16%) L; 1773 (4%) R	Parl only amendments_2all.docx	edris-suggested-amendments-general-data-protection-regulationv3a.pdf
156 (1% L, 4% R)	169 (1%) L; 168 (5%) R	Parl only amendments_2all.docx	Equifax_kontaktdaten.pdf
156 (1% L, 4% R)	169 (1%) L; 168 (5%) R	Parl only amendments_2all.docx	Equifax_Proposed%20Amendments.pdf
488 (4% L, 7% R)	509 (4%) L; 512 (8%) R	Parl only amendments_2all.docx	ESBA%20-%20ACT%20Amendments.pdf
38 (0% L, 3% R)	38 (0%) L; 39 (3%) R	Parl only amendments_2all.docx	ESBA%20-%20ACT%20Position%20Paper.pdf
717 (6% L, 3% R)	751 (7%) L; 751 (3%) R	Parl only amendments_2all.docx	Eurofinas-amendments-final.pdf
64 (0% L, 2% R)	69 (0%) L; 68 (2%) R	Parl only amendments_2all.docx	Eurofinas-position-on-ITRE-draft-opinion.pdf
50 (0% L, 0% R)	51 (0%) L; 51 (1%) R	Parl only amendments_2all.docx	Facebook.pdf

909 (8% L, 4% R)	952 (9%) L; 959 (4%) R	Parl only amendments_2all.docx	facebook_imco.pdf
121 (1% L, 3% R)	125 (1%) L; 123 (4%) R	Parl only amendments_2all.docx	FEAM-proposed-amendments-on-the-EC-Data-Protection-Regulation.pdf
132 (1% L, 3% R)	141 (1%) L; 138 (3%) R	Parl only amendments_2all.docx	FEAMSummaryDPR_ProposedAmendmentsNovember-2012.pdf
229 (2% L, 5% R)	243 (2%) L; 240 (5%) R	Parl only amendments_2all.docx	First%20Data.docx
170 (1% L, 3% R)	177 (1%) L; 177 (3%) R	Parl only amendments_2all.docx	Future%20of%20Privacy%20Forum%20White%20Paper%20on%20Consent.pdf
54 (0% L, 2% R)	55 (0%) L; 55 (2%) R	Parl only amendments_2all.docx	Future%20of%20Privacy%20Forum%20White%20Paper%20on%20De-Id.pdf
106 (1% L, 2% R)	113 (1%) L; 115 (2%) R	Parl only amendments_2all.docx	Future%20of%20Privacy%20Forum%20White%20Paper%20on%20Jurisdiction.pdf
28 (0% L, 4% R)	28 (0%) L; 28 (4%) R	Parl only amendments_2all.docx	Insurance-Europe-suggested-amendments-on-Data-Protection-draft-Regulation.docx
140 (1% L, 5% R)	144 (1%) L; 146 (5%) R	Parl only amendments_2all.docx	INTEL_Amendments_Data%20Protection_Tech%20neutrality%20and%20lawfulness%20of%20processing.pdf

35 (0% L, 3% R)	38 (0%) L; 38 (3%) R	Parl only amendments_2all.docx	ITRE-submission.pdf
89 (0% L, 4% R)	93 (0%) L; 95 (4%) R	Parl only amendments_2all.docx	Kirchen_Data%20Protection%20Suggestions.pdf
12 (0% L, 0% R)	12 (0%) L; 13 (0%) R	Parl only amendments_2all.docx	Kirchen_Stellungnahme EU%20Datenschutzgrundverordnung%2009%2011%202012endg.pdf
172 (1% L, 2% R)	180 (1%) L; 177 (2%) R	Parl only amendments_2all.docx	Microsoft.docx
254 (2% L, 2% R)	266 (2%) L; 260 (2%) R	Parl only amendments_2all.docx	Microsoft_final%20A%CC%88nderungsvorschla%CC%88ge%20EU-Datenschutzgrundverordnung.pdf
253 (2% L, 2% R)	265 (2%) L; 260 (2%) R	Parl only amendments_2all.docx	Microsoft_final%20DP%20amendments.pdf
12 (0% L, 1% R)	13 (0%) L; 12 (1%) R	Parl only amendments_2all.docx	Opower_position_EU-Data-Privacy-Reform_October_2012_final.pdf
381 (3% L, 6% R)	403 (3%) L; 404 (7%) R	Parl only amendments_2all.docx	Position-paper_eBay-Inc_ITRE-opinion-on-data-protection-regulation.pdf
485 (4% L, 6% R)	513 (4%) L; 508 (6%) R	Parl only amendments_2all.docx	Position-paper_eBay-Inc_JURI-opinion-on-data-protection-regulation.pdf

245 (2% L, 13% R)	255 (2%) L; 257 (13%) R	Parl only amendments_2all.docx	Proposals%20for%20amendments_Aggregate%20Data%20Reports.pdf
215 (2% L, 17% R)	224 (2%) L; 222 (17%) R	Parl only amendments_2all.docx	Proposals%20for%20amendments_Anonymous%20Data%20and%20Pseudonymous%20Data.pdf
425 (4% L, 5% R)	449 (4%) L; 441 (6%) R	Parl only amendments_2all.docx	Set-of-Amendments-implementing-the-Accountability-Principle-into-Law-Nov-2012-3pdf.pdf
498 (4% L, 4% R)	521 (4%) L; 523 (4%) R	Parl only amendments_2all.docx	Telefonica-Amendments-on-GDPR-Proposal.pdf
57 (0% L, 2% R)	59 (0%) L; 58 (2%) R	Parl only amendments_2all.docx	Yahoo%20on%20Pseudonymous%20Data.pdf