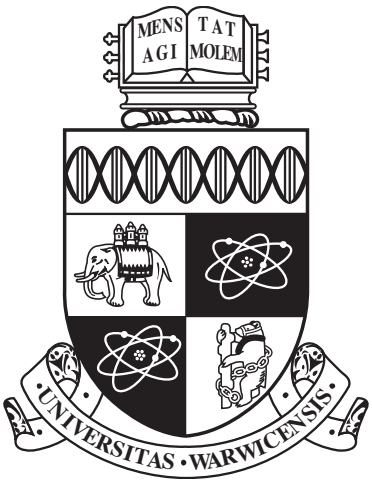

The Evolution of Privacy Regulation: Convergence and Divergence in the Transatlantic Space

by

Guillaume Beaumier

Thesis

Submitted to the University of Warwick and Université

Laval

for the degree of

Doctor of Philosophy

Politics and International Studies (Warwick) & Science politique (Laval)

December 2020

THE UNIVERSITY OF WARWICK

Abstract

This thesis explores the evolution of privacy regulations in the transatlantic space since the adoption of the European Data Directive in 1995 up until the adoption of the General Data Protection Regulation in 2016. In doing so, it more specifically investigates how the rules governing the use of personal data by private companies in the United States and the European Union were formed through the interactions between public and private actors in both jurisdictions. Looking at the process of rule formation, previous works have traditionally viewed national regulatory systems as discrete units of analysis that could affect one another and yet always remained fundamentally distinct. The starting point of this thesis is different. It considers that each jurisdiction's regulatory process is continuously shaped by decisions taken in the other and that through their interactions they actually form a complex governance system that evolves based on two joint processes: exploitation and exploration. The former emphasizes that privacy regulators will generally tend to exploit the data protection rules of those with whom they previously had direct interactions. Meanwhile, the latter highlights that when preexisting rules prove to be insufficient, privacy regulators will explore new ones based on the very same interactions and relation to the broader system. The formation of data protection rules is thus always understood in relational or systemic terms, rather than an individual process. Based on a mix of content and network analysis, I further demonstrate that by exploiting preexisting rules private actors offered a new institutional avenue for public rules to cross national frontiers and promote greater regulatory convergence. At the same time, the multiplication of privacy regulations and data protection rules adopted by private actors created second-order information asymmetries, which in turn limited their interest in exploring new ideas and experimenting with new data protection rules. In addition to contributing to the literature on privacy and introducing a novel database on data protection rules adopted over the last 20 years in the transatlantic area, this thesis highlights how growing economic interdependence upends national regulatory processes and brings into question many of the assumed boundaries in the study of international political economy.

Contents

List of Tables **vi**

List of Figures **viii**

Abbreviations **x**

Acknowledgments **xii**

Declarations **xv**

Introduction **1**

1.1 Why it Matters 4

1.2 Existing Accounts of Transatlantic Privacy Regulation 8

1.3 The Argument 12

1.4 Empirical and Theoretical Contributions 17

1.5 Case, Data and Methodology 19

1.6 Roadmap of the Thesis 23

Chapter 2 Regulating in a Complex World **25**

2.1 Global Rules for a Global Economy 27

2.2 The Market Power Explanation 30

2.3 From Public to Hybrid Rule-Making 33
2.4 Policy Diffusion: A Limited Approach to Study Interdependence 37
2.5 Taking Interdependence Seriously: A Complex System Approach 41
2.6 Conclusion 47

Chapter 3 The Transatlantic Privacy System: A Tale of Two Opposites? 50

3.1 Privacy as a Concept: From a Negative to a Positive Right 53
3.2 The American and European Privacy Divide 57
3.3 The United States and the Marketplace for Privacy since 1995 60
3.4 The European Union and Privacy Rights since 1995 65
3.5 Transatlantic Privacy Regulation: Between Public and Private Rule-Making 69
3.6 Conclusion 76

Chapter 4 The Evolution of Transatlantic Data Protection Rules 80

4.1 Transatlantic Privacy Regulation as a Complex Governance System 83
4.2 A Database on Transatlantic Data Protection Principles and Rules 88
4.3 European and American Early Models of Data Protection Rules 96
4.4 The Convergence of Data Protection Rules in the Transatlantic Space . . 102
4.5 From Convergence to Divergence: Innovations in the Transatlantic Regulation of Privacy 107
4.6 Conclusion 114

Chapter 5 Transnational Regulatory Networks and Rule Convergence 117

5.1 Public Authority and Private Networks 120
5.2 Limited Convergence After the Data Directive 129
5.3 American and European Interactions after the Adoption of the Safe Harbor Agreement 136

5.4 Transnational Trustmarks and Private Networks in the Early 2000s 144

5.5 Self-Regulatory Principles for Digital Advertising and Private Networks in the Late 2000s 154

5.6 Conclusion 161

Chapter 6 Industry Self-Regulations: Innovation, Implementation or Regulatory Capture? 164

6.1 Complexity, Regulatory Innovations and Private Rule-Making 168

6.2 Regulatory Innovations in Transatlantic Privacy Regulations 172

6.3 Private Regulators: Innovative Rulemakers? 181

6.4 Fragmentation and Regulatory Capture 187

6.5 Harnessing Private Regulation in the Shadow(s) of Hierarchy 193

6.6 Conclusion 201

Conclusion 204

7.1 Original Contributions 206

7.2 Complexity and International Political Economy 210

7.3 Practical Implications 212

7.4 Prospects for Future Research 214

Bibliography 216

Appendix A List of interviewees 249

Appendix B List of database documents 251

Appendix C Codebook 256

List of Tables

2.1 Transnational Business Governance's Regulatory tasks (Adapted from Eberlein et al. 2014: 7) 34

2.2 Different pathways for rule diffusion (inspired by Drezner 2007 & Lavenex 2014) 38

3.1 Main privacy laws adopted in the United States since 1995 62

3.2 Main industry self-regulations dealing with privacy adopted in the United States since 1995 63

3.3 Main privacy laws adopted in the European Union since 1995 67

3.4 Main indsutry self-regulations dealing with privacy adopted at the European level since 1995 75

4.1 Comparison of Early Data Protection Rules across the Atlantic 98

5.1 Comparison of Number of Shared Rules Between Early Industry Self-Regulation and American and European Rule Models* 130

5.2 Inclusion of 'European' Data Protection Rules found in the Safe Harbor Agreement by Safe Harbor Providers 139

5.3 Inclusion of 'European' Data Protection Rules found in the Safe Harbor Agreement by non-Safe Harbor Providers 140

5.4 Inclusion of 'European' Data Protection Rules outside of the Safe Harbor Agreement by Safe Harbor Providers 141

5.5 Inclusion of 'European' Data Protection Rules found in the Safe Harbor Agreement by the ICC and GBDe 147

5.6 Inclusion of 'American' Data Protection Rules by European private associations part of the e-Confidence Forum 149

5.7 Inclusion of 'American' Data Protection Rules by European private associations not part of the e-Confidence Forum 150

5.8 Inclusion of 'European' Data Protection Rules by TrustArc and the World Trustmark Alliance 153

6.1 Six regulatory innovations since 1995 173

6.2 European Support of Industry Self-Regulations since 1995 195

List of Figures

4.1 Sum of active industry self-regulations including data protection rules in the transatlantic space (1997-2017) 86

4.2 Average level of similarity between newly adopted regulations in a given year (1997-2017) 105

4.3 Sum of data protection rules promoted by public and private actors in the transatlantic space (1994 - 2017) 109

4.4 Sum of regulatory innovations in public and private regulations 110

4.5 Innovation cycle 112

5.1 Kelsen's pyramid of norms 121

5.2 The evolution of network of interactions between industry associations (1997 - 2017) 123

5.3 Transatlantic private network in 1999 135

5.4 Transatlantic private network in 2001 145

5.5 Transatlantic private network in 2008 152

5.6 Total number of active industry self-regulations including a rule requiring to maintain personal data for no longer than needed 157

5.7 Transatlantic private network in 2012 158

5.8 Total number of active industry self-regulations requiring companies to educate individuals about their data practices 159

5.9 Total number of active industry self-regulations requiring to gain the affirmative or express consent before collecting and processing sensitive data 160

6.1 Sum of data protection rules first enunciated by public and private actors after 1995 182

6.2 Sum of new data protection rules by type of actors and years 186

6.3 Sum of new data protection rules created by private actors in the EU and the U.S. since 1995 198

Abbreviations

APEC	Asia-Pacific Economic Cooperation
AICPA	American Institute of Certified Public Accountants
BBB	Better Business Bureau
BEUC	European Consumer Organisation
CCPA	California Consumer Privacy Act
CLOUD Act	Clarifying Lawful Overseas Use of Data Act
COPPA	Children's Online Privacy Protection Act
DMA	Direct Marketing Association
ECJ	European Court of Justice
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
ESOMAR	European Society for Opinion and Marketing Research
FEDMA	Federation of European Direct Marketing Associations
FIPPs	Fair Information Practices Principles
FTC	Federal Trade Commission

GBDe	Global Business Dialogue on E-Commerce
GDP	Gross Domestic Product
NGOs	Nongovernmental organizations
OECD	Organisation for Economic Co-operation and Development
GDPR	General Data Protection Regulation of 2016
IA	Internet Alliance
ICDPPC	International Conference of Data Protection and Privacy Commissioners
IMRG	Interactive Media in Retail Group
IAPP	International Association of Privacy Professionals
ICC	International Chamber of Commerce
IRSG	Individual Reference Services Group
OPA	Online Privacy Alliance
UNCTAD	United Nations Conference on Trade and Development
UNICE	Union of Industrial and Employers' Confederations of Europe (now BusinessEurope)

Acknowledgments

In this thesis, I argue that change and continuity in the regulation of privacy should be understood as systemic processes. If it is individual actors that create or adapt regulations, they never do so in isolation. They are always influenced and shaped by their previous interactions. This systemic thinking importantly also applies to this very work. While being the result of my sometimes long hours spent alone, it would have never been possible without the help and support of a number of people to whom I am truly grateful.

My first thanks must go to both my supervisors, Jean-Frédéric Morin and Matthew Watson, who followed me at every step of this journey. Since I mistakenly took his introduction to international relations' class, Jean-Frédéric has been a mentor and constant source of inspiration to me. If it was not for him, I would simply have never done a PhD. While I did question why I ever thought it was a good idea to do so over the course of my program, I am truly thankful to him for having helped me push myself and giving me such a model of excellence. I must also add that if at times I found it hard to follow his impressive path, he was always there to offer me his help. More than his academic knowledge, the greatest quality of Jean-Frédéric will always be for me his generosity. In contrast to Jean-Frédéric, I did not know Matthew before the start of my PhD program. I however quickly found out that I had not one, but two remarkable supervisors. I remember reading at the beginning of my program an article written by Mark Blyth in which he stated that Matthew had "made [him] think twice about almost everything". I can now safely say that it is also my case. I have been constantly amazed at how well Matthew was able to grasp the little details that I was not able to fully express in my written work. More than simply nourishing my academic thinking, though, Matthew was a model of kindness that I hope I will be able to replicate if I ever supervise students.

Throughout the four years of my PhD, I also met many people that helped me in a number of ways. At Warwick, I am especially thankful to Jack, Lorenzo, Javier, Te-Anne, and Aya for including me in their office as well as Johannes, Laura, Ruben, Julian, and Bo with whom I started my PhD program. In addition to be an excellent

reviewer, Andreas was a great squash and chess partner. At Laval, I was happy to share most of my journey with the members of the Canada Research Chair in International Political Economy. Mathilde, Laurie, Noémie, Krystel, Véronique and most recently Laure were amazing colleagues, but most importantly friends. More than anyone else, though, Marielle and Kevin are those that heard too many times about my doubts and fears. They helped me trust myself and go through all the different steps of my PhD. Outside both of my host universities, I moreover shared many good times with all members of the GEM-STONES' community. I am particularly grateful to Ulla and Frederik for all their organization and help throughout my PhD. During my 6-months stay in Brussels, I was finally fortunate to share a flat with Oscar, Charlène, Tiphaine, Mathieu, and Laura. I miss playing games, 'hearing' movies, going out or simply chatting with all of you. I look forward to my next trip to Brussels to see you all again.

Before the start of my PhD, I benefited from a great group of friends that supported me over the years. To all my fellow Jésuites, I just want to say that you have been like a second family for me for more than 10 years now. While we are now more spread out than ever, you remain an important part of my life. I want to express my special thanks to Ben whose many questions regularly forced me to think how I could best summarize my ideas. Since the beginning of my university studies, I also had many debates with Thomas, Luc-Antoine, Max and Rémi that have formed my thinking and I hope we will keep having them for many years more. Alex, Rachel, and Magalie you were finally those that probably most often saw me outside of my family in the last four years. You had to live with my ups and downs, but you still continuously made it fun to be with you. I am now happy to report that I can officially be the 'Ross' of the group.

I would obviously not be where I am today without my family. Since I can remember, both my parents, Jean-Paul and Christiane, offered me the best environment to thrive in. In addition to their unconditional love, they continuously provided me with the tools to succeed. My father was my first and still is today one of my favorite reviewers. He forces me to constantly respect what I have now heard him say way too often: "Ce que l'on conçoit bien s'énonce clairement, Et les mots pour le dire arrivent aisément". Meanwhile, my mother is not the one who talks the loudest, but I always gained from listening to the first postgraduate student of the family. I often found it interesting to discover the similarities in my research and her psychological approach. My sister, Marie-Laurence, was similarly a constant model of academic brilliance to me. The standard that she set for herself continuously pushed me to work harder and do better. I finally want to thank my uncle Alain that we, unfortunately, lost way too early for raising my interest in the international world since I was a kid.

Last but most certainly not least, I want to thank my wife Véronique who had the most difficult task of all: dealing with my constant self-criticism and crazy quest for perfection. More than simply bearing with it, though, she gave me strength when I had none and made me laugh when I was ready to give it all up. In all honesty, I do not believe that I would have been able to complete this PhD without her support and I

share this success with her entirely. I love you and I look forward to our next adventure with Sheldon.

Declarations

This thesis is submitted to the University of Warwick and the Université Laval in support of my application for the degree of Doctor of Philosophy and in respect of my Double Doctoral Degree Agreement. It is entirely the product of my own work and neither the thesis itself, nor any part thereof, has been submitted for examination at any other university. A preliminary version of parts of chapter 5 were published as a book chapter prepared for Christou, G., and Hasselbalch, J. (eds.) 'Global Networks and European Actors: Navigating and Managing Complexity'. London: Routledge, forthcoming.

Introduction

> *The amount of data that can be pulled in is really infinite at this point. With mobile devices - latitude, longitude, altitude; if someone's in an elevator, [we can change] an ad based on the floor that they're on in the elevator.*
>
> Frank O'Brin, CEO of Five Tier, 2019

In March 2018, investigative reporters from The Guardian and The New York Times broke the news with revelations that two of the most significant political developments in the United States and the European Union, the election of Donald Trump and the vote for Brexit, were tied with what was then the largest known data leak in Facebook history. Based on leaked documents and information obtained from an ex-employee turned whistleblower, they exposed that both the Trump and Leave campaign had contracted with the same little-known consulting firm, Cambridge Analytica, to send political advertising based on personal data harvested from between 50 to 87 million active Facebook users largely unaware of it. Using a feature at the time allowing app developers on Facebook to collect personal data from all personal connections of an individual using their applications, data scientists had more precisely built and then sold to Cambridge Analytica a database of psychological profiles that was used to send "microtargeted" political messages. The latter were expected to trigger emotional reactions (or "inner demons" in the words of the whistleblower behind the scandal) in voters that would steer them to vote in their desired direction. While it is still far from clear what the real impact of these political advertising methods had on the results of both elections,

these revelations laid bare for everyone to see how valuable the use of personal data was now considered to be by many companies and governments. Each political campaign in effect paid Cambridge Analytica millions of US dollars and British pounds as part of their bet to use personal data to steer election results in their favour.

Two months later, in what certainly appeared in hindsight increasingly needed, the new European General Data Protection Regulation (GDPR) entered into force and promised to reshape the regulation of privacy in Europe as well as globally. Following years of protracted battles among industry and civil society groups, it replaced the more than two decades old European Data Directive and introduced a revised and updated 'rulebook' for companies dealing with personal data from Europeans. Almost simultaneously, the legislature of California adopted the first comprehensive privacy law in the United States covering both the public and private sectors. Despite no similar step being taken at the federal level, it showed how far the United States had already come with regards to privacy regulation for its largest state and host to some of the world-leading digital companies to move in that direction. Other American states are now following suit, adopting their own privacy law and progressively displaying what a comprehensive privacy system could look like in the United States.

Both in the European Union and the United States, the regulatory framework governing the use of personal data is in effect significantly different than a few years ago. Just as new technologies dramatically transformed how personal data is being collected and used, as the citation in the epigraph highlights, new laws changed what types of data practices were considered acceptable in each jurisdiction and progressively contributed to shaping private companies' data uses. Legal changes are yet only one part of this evolution. Next to new laws, various private companies have developed their own set of rules listed in *terms of use* or *privacy policies*' statements. While often quickly glanced at, the importance of these private rules should not be understated. They determine how an individual's privacy will actually be protected on the ground and for many companies they are presented on an equal footing with public laws. Two years before the Cambridge Analytica scandal broke out, Facebook (2016) was in fact pleading that its community rules were equivalent to public laws and that new legislative actions from the Commission were not needed in a host of issue-areas, including data protection. As these rules evolved, they equally shape how our personal data is being protected.

How have data protection rules evolved in the United States and the European Union since 1995? What led to the specific set of rules now being promoted in the

European Union and the United States by public and private actors? To what extent did they influence each other? These are the main research questions that I aim to answer in the present work. The regulation of privacy has become an increasingly hot topic in a global economy where data flows are quickly outgrowing any other types of international exchanges. The European Union and the United States are moreover seen as the two global leaders on the topic, with each promoting a different approach and seemingly competing on the international stage to make its own adopted. In recent years, many were prone to maintain that the European Union was winning in the "marketplace of ideas" (Schwartz 2019). The adoption by the state of California of a comprehensive privacy law as just stated was given as a prime example of this European success. In addition to other countries, like Brazil and India, that had already followed suit and adopted a comprehensive law, this first adoption of the so-called EU model by an American public authority was viewed as a key sign of a shift of approach in the United States. If not for governments, others saw in the implementation of European rules by American companies throughout the United States an indication that the European Union had already won this regulatory competition (Bradford 2020).

Several blind spots however remain in these broad expressions of European success. The evolution of the European regulatory framework remains significantly unexplained. Touted as a new gold standard, the origins of the new rules set forth in the GDPR are simply not investigated in these explanations. They seemed to be seen as the result of purely European politics that concluded well before the United States and the European Union had any interactions with each other. Similarly, the American privacy model generally appears to be at a standstill up until being forced to change under European pressure. The different legal changes that occurred inside the United States are quickly disregarded as well as their very impact on the European Union. Various examples of the United States influencing the content of data protection rules in Europe yet exist. Rules on data breaches that are now part of the GDPR and the 'European model' supposedly exported all around the world are well-known to have been first enunciated in American law. Such examples of partial integration and hybridization of both models over time tend to be overlooked. Following a traditional 'two-step' logic of liberal theories (Legro 1997; Moravcsik 1997), the national (or regional) and international are neatly divided. Rules are first devised by domestic authorities and then clash on the international stage where the European Union is currently succeeding in promoting its rules due to its leadership, regulatory capacity, market size, or a combination of all of the above. Even though private actors can sometimes be seen as creating additional

bridges between the two jurisdictions, the process of rule formation remains primarily looked at through a domestic lens. To put it differently, international and transnational interactions are not themselves seen as a driving force of regulatory change.

Hereafter, I contest this idea and argue that the growing number of interactions between public and private actors in the European Union and the United States has actually created a complex governance system that transformed the process of rule formation in each jurisdiction (Kahler 2016; Oatley 2019; Orsini et al. 2019). Rather than having two political systems developing their regulatory models separately, I maintain that they evolved jointly based on their interactions over the last twenty years or so. This process was moreover often more incremental than explosive as opposed to what the recent literature on the global influence of the European model tends to indicate. In effect, one model's influence was never constant over time and regulatory changes were never limited to a specific time period. Both were continuously adapted based on decisions taken in the other. This view highlights that the growing interdependence of national economies does not merely create new issues to regulate or negotiate internationally, but also blurs the line between domestic and world politics (Farrell and Newman 2014, 2016, 2019*a*). As regulators operating in multiple jurisdictions increasingly interact with each other, what would traditionally be seen as domestic regulatory processes is shaped by dynamics that transcend domestic boundaries. Two processes, exploitation and exploration, are in the remainder of this work investigated to better understand how the regulation of privacy has evolved in the transatlantic area.

1.1 Why it Matters

Back in 1995, Irving Goldstein, then-director general of Intelsat[1], almost prophetically held that data "will be for the twenty-first century what oil and gas were for the beginning of the twentieth century. It will fuel economic and political power" (cited in Powers and Jablonski 2015: 75). A little bit more than twenty years later, the well-known journal *The Economist* seemed to give him reason with one article emphatically claiming that the "world's most valuable resource is no longer oil, but data" (Parkins 2017). As some rightly pointed out (Stucke and Grunes 2016: 49), comparing data to oil has many defects. For one, data is not a finite resource like oil (Powers and Jablonski 2015: 76). As the quote

[1]Intelsat was at the time an international organization in charge of satellite communications. It has since then been privatized.

in the epigraph notably highlights, the number of personal data collected has grown exponentially in recent years and now even almost appear potentially "infinite". From the turn of the millennium where only a quarter of all information was stored digitally (Mayer-Schönberger and Cukier 2013: 8-9), we now live in a world where a lot of what we do on a daily basis is digitally recorded and stored by various companies. The situation is such that even the definition of personal data increasingly comes to encapsulate a lot of different types of information.

Broadly construed, personal data are any information that would allow identifying someone or that could be related to an identifiable person. This traditionally includes information such as someone's social security number, health details, credit history, home address, phone number, and e-mail address. With new digital technologies that allow private companies to track our activities to an extent never seen before, this list has grown to include information such as our browsing history, location data, and even our biometrical information. Even supposedly anonymized data can often be tied to someone by combining it with other sources of information. Old pictures uploaded on social media by a distant friend can for example be tied back to us using our biometrical information for facial recognition purposes. Information on what we did or where we were years ago can increasingly be found without us being always aware that such information is available.

Apart from being potentially creepy and creating a sense of constant surveillance, the use of personal data has real economic and political value. According to estimates made by the McKinsey Global Institute (Manyika et al. 2011, 2016), the potential economic value of data analytics for many industries range in the hundred billions of American dollars. By gaining an in-depth view of our daily lives and previous histories, most private companies hope to successfully predict and influence our behaviour. In the case of the Cambridge Analytica scandal, data harvested from Facebook profiles was again used to build psychological profiles to identify swing voters and target them with tailored political advertising. Outside of political campaigning, various private companies now similarly use personal data in their commercial activities. Targeted advertising, price discrimination, customer segmentation, and eligibility determinations are all examples of recent commercial data uses (Spencer 2016).

This is not all new (Christl, Kopp and Riechert 2017: 5). Credit agencies have for long used personal information to make eligibility and price determinations. Different individuals are routinely offered different insurance policies and premiums depending

on their health condition, type of employment, and reclamation history. Advertising messages are also tailored to the medium being used and the specific audience that that they can reach. Even prices of goods and services are regularly adapted for different groups of customers. Discounts are sent to individuals living in specific neighbourhoods or offered to specific categories of individuals (e.g., students, seniors, etc.). Customer segmentation across countries is also known to be a common practice for transnational companies. Putting aside transportation costs and national taxes, companies often see an opportunity in adapting their prices to local markets to reap the highest benefits possible.

The difference with what is occurring these days is the reach of these practices. The exploitation of large databases with the help of new data analytic techniques increasingly allows private companies to target single individuals that do not realize that their personal data is being used or that they had even shared it in the first place. This in turn contributes to create a more than ever individualized world where two persons living in close proximity to each other might in practice experience two different realities. They might not have access to the same news as recent election cycles have highlighted in countries like the United States and the United Kingdom, but also Brazil to give just one additional example that attracted a lot of international attention (Martins dos Santos and Varon 2018). The same two individuals might neither be offered the same price for the same goods and services. While still difficult to spot as these are controversial and potentially anti-competitive practices that companies do not want to publicize, algorithms adapting prices based on individual characteristics or previously established profiles were already reported to be in use by both Amazon and Uber (Ezrachi and Stucke 2016; Khan 2017).

The end result is a highly unequal society in which disparities between the haves and the have nots tend to be exacerbated. If some had hoped or argued that wider dissemination of personal information would help fix market failures and help our economic systems to meet our actual needs (Posner 1978; Cate 2000), the truth is that it did not empower equivalently all economic actors. Individuals might sometimes benefit from accessing information online allowing them to more easily compare prices, evaluate production processes or judge the impact of public policies, but this is nowhere near to the pool of information that private companies and governments sometimes working with them now have access to or the means they have developed to act upon it. This should

not be that surprising and simply highlights that technological innovations are always political and not merely solutions to technical problems.

In this sense, though, privacy regulation is not only about protecting an abstract individual freedom but actually balancing power relations between individuals, companies, and governments. Recognizing this, both the United States and the European Union have acted to safeguard their citizens' privacy. The way they decided to do so however historically diverged with the United States continuously promoting a limited system where data protection rules apply to governmental entities while private companies are broadly encouraged to self-regulate themselves, and the European Union as a whole preferring to set out data protection rules for both public and private actors ever since the adoption of its Data Directive in 1995 (Newman 2008). This difference of regulatory approach is at the source of great tensions between the two transatlantic partners. As many businesses nowadays interact with individuals based in both jurisdictions and data flows are an integral part of their economic integration, the way each decides to regulate privacy has consequences for the other. It can in effect mean more restrictions for companies from one jurisdiction as well as potentially fewer guarantees for individuals in the other.

Over the years, two international agreements, the Safe Harbor (2000) and Privacy Shield (2016), were negotiated to provide what could be a common framework and appease these tensions between the two partners. Both agreements are now defunct following similar actions brought by civil activists before the European Court of Justice and were regularly criticized for implementation failures (see for example EDRi 2019). Any attempts at reaching a new agreement that could sustain future legal challenges look bleak without further regulatory convergence. Understanding what could be driving them closer as well as further apart is thus key to make sense of where the regulation of privacy is going. As an agreement on a set of rules between the United States and the European Union has moreover the potential to reshape privacy regulations in other countries around the world due to their joint economic size and normative influence, this makes it not only of interest in the transatlantic area but also globally.

Outside of privacy, this research contributes to growing debates in international political economy over the regulation of "non-traditional" issues. Not so long ago, the study of international political economy was largely geared towards "explaining the variations in the global rules governing merchandise trade, exchange rates, and foreign direct investment" (Drezner 2007: 8). As David Lake (2009: 221) rather puts it, it primarily

aimed at answering one of two sets of questions with regards to the regulation of international economic exchange: (1) why and how did countries open up to various international flows; and (2) how did this economic openness, in turn, affect national constituents and politics towards it. Nowadays, most researchers, however, go much further than that and recognize the international, or more aptly global, importance of a broader array of political economic issues, including but not limited to the environment, intellectual property, gender, race, labour, taxation, and privacy.

This partly answers early calls by Craig Murphy and Roger Tooze (1991: 24) to expand the "universe" of international political economy so as to move away from "the policy concerns of the government of the United States throughout the era of U.S. global supremacy and, especially, contemporary concerns about various challenges to that supremacy". At the same time, it reflects the broad recognition that economic interdependence has elevated many regulatory issues previously seen as being of national interest to the global stage. This is importantly made evident in the expansion of the number of chapters in preferential trade agreements that now present many of these regulatory debates as non-tariff barriers that need to be either removed or more closely overseen. This expansion of the universe of international political economy topics is thus very much a reflection of the similar expansion of the United States policy agenda. Putting aside the question of the geography of international political economy, though, the present study of the regulation of privacy in the transatlantic area provides insights on how to understand and analyze new regulatory debates of global interest.

1.2 Existing Accounts of Transatlantic Privacy Regulation

The regulation of privacy has long been a hot topic in transatlantic debates. Early on, it attracted a lot of attention in international circles where their disagreement was seen as raising the risk of disrupting increasingly important data flows between the two jurisdictions. The potential significance of policy decisions taken in each jurisdiction for the other was more broadly taken as a prime example of how globalization was putting new pressure on legal systems traditionally viewed as distinct and potentially reshaping national politics. In turn, various scholars attempted to explain the sources and consequences of their regulatory coordination or convergence over the years.

For some, cultural and historical factors primarily explain the origins of the transatlantic disagreement. Going back to their different experiences during the Second World War and with authoritarian governments, they argue that European governments have developed a sensibility to privacy issues that is absent in the United States (Singleton 2002). This would then explain why the first data protection law was adopted in the state of Hesse in Germany in 1970 (Long and Quek 2002: 330) and why the European Union elevated privacy to a human right in its Charter of fundamental rights adopted in 2000 while the United States continues to view the use of personal data by private companies primarily as a consumer issue. This difference of experience and the resulting views was, in turn, argued to have made the adoption of an international regime impossible as there was no point of agreement between them (Bessette and Haufler 2001; Haufler 2001; Dimitrov et al. 2007). Following the same line of thought, their diametrically opposed perspective is given as a prime reason why further harmonization of privacy regulation was not advanced in recent trade negotiations and why a 'digital divide' continues to exist between them (Aaronson 2015; Aaronson and Leblond 2018; Young 2015*a*). More specifically, the European human right lens makes privacy something that should not be seen as a trade issue and should not be negotiated as such.

According to Daniel Drezner (2007: 103-6), neither the United States nor the European Union moreover has the capacity to unilaterally impose its preference to the other. For him, they are the perfect example of two 'great powers' (i.e., political entities overseeing large internal markets) promoting a rival standard, which will always end up in a stalemate. In effect, none possess a sufficient bargaining advantage to push the other to adopt its standard and both have the means to sustain the potential costs of not agreeing on a common one. The best they can do is thus agree to disagree up until one internally changes its position for some external reasons. Somewhat differently, Henry Farrell (2003; 2006) maintains that they can and did actually work around this stalemate through the creation of what he calls a hybrid regime. While recognizing their mutual difference and inability to change the position of the other, he pointed out that they had actually worked around this stalemate by delegating regulatory tasks to private actors in the Safe Harbor and later on Privacy Shield Agreement. Rather than promoting a joint regulatory framework, what these agreements in effect did was to create a system allowing American private companies to self-certify that they would certain rules when using personal data coming from Europe. This then had the advantage to avoid any disruption of data flows without any of them having to change their national regulation. Drezner (2007: 106) was however dubious of the actual efficacy of these private mechanisms and the fact that

both international agreements promoting them are now defunct partly because of their problematic implementation certainly questions how durable hybrid solutions can be.

Meanwhile, Abraham Newman (2008) contests the idea that cultural differences are actually the source of this transatlantic dissension. He points out that this significantly fails to explain that not all European nations with a fascist legacy or authoritarian experience have been prone to adopt a data protection law. In fact, countries, like Belgium, Greece, Italy and Portugal, had not yet adopted one covering both the public and private sector when the European Data Directive was adopted in 1995 (Newman 2008: 84). His own argument is that the regulatory divergence observed between the United States and the European Union would better be understood as the result of different institutional trajectories. While the creation of data protection agencies in various European countries allowed the emergence of a transgovernmental network to lobby the European Commission in favour of the adoption of a comprehensive data protection law, the existence of multiple veto points in the United States (i.e., presidential veto, bicameralism, etc.) offered multiple opportunities for private businesses to block such an outcome.

Newman moreover argues that these different institutional trajectories have relevance for the regulation of privacy globally. By building up its regulatory capacity internally, the European Union in effect gave itself the tools to leverage its internal market and "set de facto international privacy standards" (Bach and Newman 2007: 836). It is because the Data Directive gave European regulators the statutory authority to block data flows from third countries lacking appropriate safeguards that it could force the United States to adopt the hybrid regime described by Farrell. If the United States was able to benefit from its own market size to escape further change or even entirely defend its model as Drezner would have it, it was not able to extend it as the European Union did by pushing 12 countries, including large industrial economies like Canada and Japan, to reform their data protection laws to be considered as 'adequate' and thus allowing data to flow freely between their jurisdictions and Europe. According to Newman, the lack of a similar institutional mechanism in the United States and the resulting gap in regulatory capacity explains why the European Union, not the United States, appears to be driving the global conversation on privacy (Newman and Posner 2015).

Building on Newman's argument, Anu Bradford (2012; 2020; see also Goldsmith and Wu 2006) maintains that in practice the United States have already adopted European data protection rules. She maintains that private companies operating in both jurisdictions indeed apply the same set of rules originally devised in the European Union.

According to her, the reason for this is basically that by having the most stringent rules and the regulatory capacity to enforce them, the European Union is able to force private companies all around the world to apply its standard even when dealing with the personal data of non-Europeans. This kind of 'trading up' phenomenon (Vogel 1995) or 'Brussels' effect' as she calls it is moreover made possible by two additional factors. First, the strict European data protection rules cannot be easily circumvented by moving European personal data to another jurisdiction. European authorities are indeed expecting European personal data to be treated as such wherever it is being processed. Second, it is either impossible or non-economically viable to maintain multiple privacy standards for the different sets of personal data owned by a company. As such, private companies are left with one option, which is to either keep out of the European market or use its rules throughout its business.

While agreeing that the case of privacy does fit most, if not all, the conditions highlighted by Bradford, legal experts Paul Schwartz (2019) and Karl-Nikolaus Peifer (Schwartz and Peifer 2017) believe that such expression of European unilateral power does not fully encapsulate the current trend of convergence in privacy standards around the world. Following the work of Anne-Marie Slaughter (2004), they emphasize that various "harmonization networks" are actually at play connecting regulators in Europe to those in various other jurisdictions, including the United States. The success that European data protection rules are currently experiencing is thus the result of a more co-optive form of influence (Lavenex 2014) where European partners progressively learn and become socialize to the European standard. The regulatory capacity developed over the years by the European Union here is viewed as contributing to the export of its rules based on its expertise or normative power, rather than unilateral imposition of coercion.

Focusing on the principles promoted to govern the use of personal data, Colin Bennett (1992; 2010) contrasts with most others while maintaining that regulatory convergence has actually been a reality for quite some time. If legal discrepancies do remain and policy instruments used in both jurisdictions differ, they have indeed been continuously moving towards the same set of basic principles. He believes such an outcome is primarily due to the "common set of attitudes that developed about the technology" (Bennett 1992: 51), which remain true today despite recent technological changes. More recently, Kenneth Bamberger and Deirdre Mulligan (2015) also contended that on the ground corporate practices of privacy management in the United States and Germany also shared many similarities. In their view, one reason for this was the existence of a

similar pressure coming from civil society organizations and other non-corporate actors that brought "the outside in" to use their words (Bamberger and Mulligan 2015: 220).

From all these explanations, we are left with a wide variety of variables and a relatively confusing picture of where the transatlantic regulation of privacy currently stands. To be fair, some of the distinctions discussed are due to the focus taken in each study. For one, Bennett sees a convergence because he focuses on broad data protection principles and Newman sees a divergence as he focuses on the regulatory approach taken in each jurisdiction. These are not necessarily contradictory, but the relations between these different elements and how they influence the evolution of privacy regulation could still be better explained.

One related blind spot to all these different analyses is their implicit choice to treat the United States and the European Union's regulatory framework as fundamentally distinct. They are indeed presented as two systems that evolve separately up until clashing with each other. This more broadly follows the widespread view of globalization as an external shock creating a pressure for adaptation on national economies and that fails to recognize that it is actually endogenously reshaping what used to be seen as national politics. In effect, the European or American privacy regulations do not evolve in isolation up until clashing with each other. They are indeed constantly informed by decisions taken in the other due to their growing interdependence and the various interactions that ensue from this. Recognizing this actually helps understanding how the different levels of analysis and variables just presented influence the evolution of the regulation of privacy as part of a coherent whole. Hereafter, I develop an argument highlighting how the close interactions between various public and private actors in each jurisdiction transformed their respective process of rule formation.

1.3 The Argument

The core claim that I make in this work is that the evolution of privacy regulation in the transatlantic area since the adoption of the European Data Directive in 1995 should not be viewed as the result of purely domestic forces nor very specific and circumscribed moments of international negotiations. Neither is it simply the result of a clash of systems where two privacy models fight for global dominance and one straightforwardly wins. It is rather the result of transnational interactions that shaped American and

European domestic institutions as well as their ability to affect global outcomes. Repeated interactions between public and private actors active in both jurisdictions more precisely generated multiple opportunities for influence and changed the content of the regulations adopted in each one. The outcome is thereby not regulations that should be viewed as being purely 'American' or 'European', but that are mixed in nature and include elements coming from both.

This does not entirely reject all the explanations just reviewed and actually builds on many of them. Indeed, it takes as a starting point the hybrid regime involving both public and private actors described by Farrell (2003; 2006). Yet, rather than looking at it as an institutional agreement solving the transatlantic relation, it approaches it as having supported the creation of an institutional environment in which public and private actors cooperated and interacted to shape data protection rules. By delegating regulatory tasks to private actors, both the United States and the European Union more precisely opened up new avenues for influence between them. In addition to direct interactions occurring between public representatives in various forums, industry associations also act as transnational links between the two legal systems. While both agreements that were negotiated to support this hybrid regime are now defunct, the organizations that were created still continue to exist and affect the content of rules promoted in each jurisdiction. The way they do so remains importantly dependent on the regulatory approach taken by public authorities where they are mainly active and the leeway that is accordingly given to them (Newman 2008). Together, these public and private channels moreover form the 'harmonization networks' viewed by Schwartz (2019). More than simply pushing towards regulatory harmonization, though, they are also informing the creation of new rules by providing additional opportunities to learn from what others did. In this sense, they are not a simple transmission belt for the European Union to unilaterally influence the American regulation of privacy as Bradford (2012; 2020) tends to portray it. They actually contribute to form a complex governance system that transforms the process of rule formation[2].

The adjective complex is here significantly not understood as meaning complicated. If the two terms are often conflated in popular and academic discourse, they actually describe two very different things in the present context (Morin 1990). 'Complicated' can be broadly defined as the quality of something that is hard to understand or

[2]This reflects the argument of Abraham Newman and Elliot Posner (2016*a*; 2016*b*) maintaining that transnational institutions can create 'second-order effects' by changing the political landscape in the jurisdictions that they connect to each other.

requires a specific type of knowledge to make sense of. Meanwhile, the term 'complex' is here taken to describe systems that "cannot be reduced or simplified without being strongly altered or "mutilated," and [which] behavior is not predictable from the study of their parts" (Orsini et al. 2019: 2). To put it differently, complex systems are characterized by emergent and non-linear properties that can only be explained by looking at them as a whole. They differ from complicated systems that can be made up of multiple components, but still can be understood by looking at them individually. Classic examples of complicated systems include clocks or planes whose inner workings are hard to understand for most of us but can still quite straightforwardly be disaggregated to mechanically explain how they work. The nuts and bolts that make these machines what they are continue to play the same role at any level of analysis or abstraction. Many social and governance systems however do not fit this description. The addition of components (i.e., actors, institutions, etc.) interacting with others in the system creates new dynamics that affect their evolution in sometimes surprising and unintended ways. In the present work, I specifically highlight two processes that shaped the regulation of privacy in the transatlantic space: exploitation and exploration (Duit and Galaz 2008; March 1991; Morin, Pauwelyn and Hollway 2017).

Exploitation refers to the tendency to make use of preexisting resources (March 1991: 71). In a regulatory context, this notably means using the rules that other actors have already spent time developing. The choice over which rules to exploit is however not random and is based on the actors with whom they had interactions in the past. If one can learn and be influenced by what others do very far from them without ever directly being in contact with them, this is generally less likely to occur than when two people directly exchange with each other. This is obviously the same for regulators. They indeed tend to use what they have been in direct contact with and this is reflected in the content of the regulations that they promote. This in turn allows them to save time, energy, and valuable resources, while also reducing the risks for potential errors or mistakes. Exploration meanwhile describes the broad process that leads to the creation of new resources (March 1991: 71). As the world changes, various actors regularly need to innovate and adapt themselves. For regulators, this means creating new rules to deal with new problems or new information that they are faced with. The way they do so is again importantly dependent on their previous interactions that shape their realm of possibilities. In effect, nothing is ever created out of thin air and what appears as being new is constantly the result of the combination of what already exists. Just as new technical devices are made of preexisting technical components, new rules are in

effect constructed from preexisting rules. In other words, the act of innovation is one of recombination.

Together, these two processes animate the evolution of complex governance systems in ways that cannot be comprehended by merely looking at their individual parts. In the present case, why the GDPR looks like what it is today cannot be understood without replacing it in the broader regulatory system that it is part of. As a whole, the current state of the regulation of privacy in the transatlantic space can also only be explained by looking at how the various interactions between the actors that promoted data protection rules shaped their regulations over time. This is notably because they are not moving towards one clear equilibrium or regulatory model, but instead following a changing regulatory framework. If exploitation can give the impression that in the short run different actors are moving towards one common set of rules and bringing order to the system, exploration introduces variations and constantly changes what the regulation of privacy will look like in the future. New rules explored at t=1 and exploited at t=2 become the source of new ones at t=3 and so on. Understanding who interacts with whom is thus essential to understand the direction that the transatlantic regulation of privacy and other complex governance systems are taking. This specifically embraces the concept of homeorhesis in biology, which describes systems that evolve following a trajectory as opposed to systems that continuously go back to the same single outcome or state of homeostasis (Haas 1982: 217).

From this broad theoretical argument, I draw two more specific conclusions in my empirical analysis. First, industry associations creating codes of conduct, and certification schemes supported a process of regulatory convergence by which the rules promoted in the United States and the European Union became increasingly similar over time (Drezner 2001; Knill 2005). Through their interactions, private associations active in both jurisdictions were more specifically encouraged to exploit rules coming from the other and in turn prompted businesses following their private forms of regulation to apply a similar set of rules. This did not occur suddenly but was part of an incremental process where rules from one jurisdiction made their way to the other as private associations that had incorporated the rules of their main jurisdiction of activity progressively created links between associations in the other.

This has meant that although the United States and the European Union still follow different approaches to the regulation of privacy, on the ground the rules being applied are closer than often assumed. By the time the state of California adopted the

first comprehensive privacy law in the United States, many companies were in effect already applying rules put forward by European authorities. Yet, this convergence was not only the result of a transfer or export of 'European' rules to the United States. Private associations in the European Union were also likely to exploit rules that were first devised in the United States following their interactions with their counterparts based there. Throughout this process, private actors importantly ended up extending the influence of American and European public authorities by providing them a "new institutional avenue to diffuse [their] rules" (Green and Auld 2017: 261). As the rules that they were sharing were partly those that they had first taken from their host jurisdiction, they sometimes became kind of private promoters of public rules. This was even reinforced when public actors, and in that regard especially the European Union, actively tried to shape their interactions.

Second, I highlight that private associations have more than only exploited data protection rules created by public authorities, they also explored and experimented with new ones. By combining rules that they had incorporated based on their previous interactions, they were indeed able to create rules that no other public or private actors had until then promoted. In doing so, they contributed to make the regulation of privacy more flexible as some scholars had previously argued (Abbott, Green and Keohane 2016; De Búrca, Keohane and Sabel 2014; Green and Auld 2017; Overdevest and Zeitlin 2014). At the same time, I find that this contribution of private associations was not as significant as it could have been expected. The exploration of rules was done by a relatively small number of private actors and in a very limited time span. Public involvement was moreover almost always needed to actually push these private associations to go "beyond compliance" (Bartley 2011, 2014; Prakash and Potoski 2012). It is really not as if private forms of regulation had proven to be so much more adaptive to a quickly evolving set of issues raised by the growing use of personal data.

By creating fragmentation, it stands out that the multiplication of industry associations reduced the signalling value that private companies could gain from exploring new rules and created "second-order information asymmetries" (Renckens 2020: 41). As the number of private regulations supposed to provide privacy guarantees rose, it became particularly hard for most users to distinguish them and know which ones were more or less stringent. Instead of resolving information asymmetries as private forms of regulation traditionally hope to achieve, they created more confusion by making it unclear what rules were applied. This acted as a disincentive for private associations to

add more requirements than they were legally required to. This is especially as these programs remain voluntary and need to prove their value to private companies using them and that often do not want to make their life more difficult than necessary. In this context, I show that codes of conduct or certifications even hindered the adoption of more substantive regulation by public authorities and appeared to act as a kind of regulatory decoys. While maintaining that they could supplement public rules, they actually sometimes helped private companies escape their obligations. This sub-optimal outcome, where private regulations attempt to capture the regulatory process, can importantly be overcome by greater public participation in their development.

1.4 Empirical and Theoretical Contributions

Throughout this work, I make both empirical and theoretical contributions to the literature on privacy, private authority, and global regulation. Empirically, I first provide the most comprehensive overview of how the regulation of privacy has evolved in the United States and the European Union since the adoption of the European Data Directive. I do so by notably building an original database (see section 4.2) that highlights when and how new data protection principles and rules have been integrated in both jurisdictions. This goes much further than the previous literature that focused on the different European and American regulatory approach to privacy (Newman 2008) and broad data protection principles (Bennett 1992). It also offers a more detailed picture than more recent work that only focused on a limited number of new public laws, like the GDPR and the California Consumer Privacy Act (Chander, Kaminski and McGeveran 2020; Schwartz and Peifer 2017). It finally allows me to delve deeper into the role that private actors have played in the regulation of privacy than the literature arguing for the existence of a 'Brussels' effect' (Bradford 2012, 2020). In addition to not taking for granted self-indication from American companies that they abide by the GDPR and actually looking at what rules are being promoted by private actors, I show when they also tended to go further than their legal obligations and when rules first devised in the United States had an influence in Europe.

My empirical work moreover brings light to the role of a specific type of private actors: industry associations and certification companies devising codes of conduct, guidelines, certification schemes, and other private forms of regulation that other companies are expected to abide by. Despite an early recognition that they could play a "public

role" in the regulation of privacy (Haufler 2001), they were up to now mostly analyzed for their role in the implementation of the Safe Harbor or Privacy Shield Agreements (Farrell 2003, 2006; Drezner 2007). In addition to excluding those active in Europe, this failed to account for cases where private actors contributed to privacy regulation without a clear delegation of authority from public actors. In the rest of this work, I highlight that they offered an additional avenue for the exploitation of data protection rules in both jurisdictions and actively contributed to the exploration of new rules.

Theoretically speaking, I answer recent calls to give more attention to the interactions between public and private forms of authority (Eberlein et al. 2014; Gulbrandsen 2014). Rather than looking at what these private associations and certification companies have been doing separately, I question how they are being layered on top of public rules and being actively shaped by public authorities. I notably end up showing that the different regulatory approaches taken in the United States and the European Union significantly changed how these private actors ended up contributing to the regulation of privacy. While in the United States they were more active in creating new data protection rules, those based in Europe were significantly less likely to do so. This reflects the view in Europe that they should not be left alone to regulate and where they were mostly expected to help in the process of harmonizing data protection rules in the European single market. In highlighting this difference, I go further than previous work on private authority focused on explaining its emergence (Cashore, Newsom and Auld 2004; Green 2013*b*; Mattli and Woods 2009) and question how public interventions in private forms of regulation can change their very content and future development. In doing so, I extend previous arguments that had linked different types of regulatory state to different forms of self-regulation by also highlighting how the different involvement of public authorities affect the process of exploring new data protection rules by private actors (Newman and Bach 2004).

The complex system approach that serves as the main theoretical foil for this work finally offers a renewed understanding of how cross-border rules emerge among interdependent economies. In recent years, complexity ideas have increasingly made their way in international relations and international political economy debates. The literature on regime complexes has for one been keen on highlighting how the proliferation of international institutions was creating new power dynamics and pathways for influence (Abbott 2012; Alter and Meunier 2009; Betts 2009; Davis 2009; Drezner 2009; Kellow 2012; Keohane and Victor 2011; Orsini, Morin and Young 2013; Raustiala and Victor

2004). Others have also shown how complex dynamics are also important among institutions forming what could be seen as single regimes or issue-areas (Kim 2013; Morin, Pauwelyn and Hollway 2017; Pauwelyn 2014). In this work, I introduce yet another form of complexity. Instead of focusing on the multiplication of formal international institutions, I highlight how economic interdependence between various jurisdictions opened up new channels of influence between private actors and in turn contributed to create a complex governance system where decisions taken in one jurisdiction can often affect the other without necessarily having to go through international negotiations.

Here, I partly build on the recent work by Henry Farrell and Abraham Newman developing a new interdependence approach and attempting to endogenize the effects of transnational interactions in domestic policy-making (2014; 2016; 2019*a*). Instead of focusing on how these interactions affect the strategies taken by public and private actors to advance or block institutional change, I, however, focus on their impact on the process of rule formation and more specifically how previous interactions between public and private actors affect the adoption and creation of data protection rules. This offers a picture where distinctions drawn between the 'international' and 'national' realms often become blurry. Rule-making is indeed not presented as being purely national. As such, I go much further than the traditional "second-image reversed" argument (Gourevitch 1978) according to which the international system also shapes domestic politics and present an analysis where the two are often merged together. The point here is not to say the United States and European Union have become a single coherent legal jurisdiction, which clearly is not the case. Yet, their regulatory processes are neither fully separate from each other.

1.5 Case, Data and Methodology

As already indicated multiple times now, the present work focuses on the regulation of privacy in the transatlantic area and more specifically between the United States and the European Union. The choice of limiting myself to this specific geographical area has many reasons. One is very simply their broad importance for the global economy. As Drezner (2007) rightly pointed out, they oversee the two largest internal markets and are in that sense two 'great powers', which decisions matter for the rest of the world. If they cannot unilaterally impose their regulatory preferences to the other, they can often do so for smaller third countries. This is notably the case with regards to the regulation

of privacy. On one side, the European Union has established an 'adequacy decision' mechanism to certify that third countries have an equivalent privacy system and allow data to flow freely between them. This has pushed many countries, including Canada and most recently Japan, to revise their own laws. On the other side, the United States has been active in promoting its regulatory model and set of data protection rules by negotiating the Asia-Pacific Economic Cooperation (APEC) Privacy Framework. If the two jurisdictions often appear as competing with each other, any agreement between the two would have the potential to reset the global regulation of privacy.

Two further reasons explain the choice of limiting this research to the transatlantic area. First, the present work follows the evolution of the regulation of privacy since 1995, a time where both jurisdictions were largely driving the global discussion on this question. As the goal of this research is to understand how we got to the set of data protection rules promoted today in the United States and the European Union, no other country or international organization appeared to have had a significant influence on their respective regulatory approach to data privacy. In recent years, China is often presented as a third "data realm" promoting its own model of privacy regulation and digital regulation. As the "world's largest digital market, with 731 million internet users, [and which] accounts for more than 40% of global e-commerce transactions" (Aaronson and Leblond 2018: 262), it could well have an important say in how privacy regulations evolve in the future. It was however not the case up until recently. If there were early indications that China was contributing to shape technical standards (Bach, Newman and Weber 2006), it only adopted its first significant law dealing with privacy issues in 2012 and did not actively contribute to global privacy debates until then (Geller 2020; UNCTAD 2020).

Second, the whole argument developed in this research, according to which the United States and European Union can be viewed as a complex governance system, is based on the fact that these two jurisdictions are in a close relation of interdependence and that as such their domestic decision-making process became intertwined (Lütz 2011). In effect, it considers that their "relationship is [...] a microcosm of globalization, with high levels of interaction and exchange between" the two (Farrell and Newman 2018). In the present case, this close interconnection is reinforced by the philosophical root shared by the concept of privacy in the United States and the European Union. While it is regulated differently, they indeed have a common history, as chapter 3 will highlight. It is notably because of this that the processes of exploitation and exploration could emerge between actors based in both geographical areas. There is clearly not the same level of

interactions nor shared understanding of the concept of privacy between China and both transatlantic partners. The same opportunities for influence thus did not emerge between them and it was excluded from this research. This is not to say that regulatory decisions taken in China never had any impact on the United States or the European Union, but if so it was significantly less than among these two jurisdictions. In that regard, the choice of excluding China as well as other countries aims to emphasize their close interconnection and thus serves both descriptive and analytical purposes (Cilliers 2001).

While focusing on the evolution of the transatlantic privacy system, I more specifically look at changes and interactions occurring at the American federal, European, or international level. This means that regulatory change in one American federal state, like California, or in one European member state, like France or Germany, as well as potential interactions between them, are not part of the main analysis. As two 'multilevel systems' (Lütz 2011), there are in effect many different actors active at many different levels in the United States and the European Union that can interact and shape the evolution of data protection rules. Including all of them would have however been too much and the analysis was thus limited to the interactions between actors at the highest level in both the United States and the European Union[3]. This reflects the fact that they are the ones that are most likely to have had repeated direct exchanges with each other. If sub-national (or national in Europe) can also have an important say in the set of final rules applied in many issue-areas, decisions taken by American federal or European authorities can often have a broader impact by forcing regulatory convergence inside their respective jurisdictions.

I use a mix of content and network analyses to understand how interactions between public and private actors active at these levels in the United States and the European Union shaped the evolution of their respective data protection rules. The manual coding of 126 regulations dealing with privacy issues more precisely serve to trace changes in the set of data protection rules promoted by different actors over time, which in this case represents the dependent variable. These 126 regulations include sectoral laws adopted by the federal government in the United States, European Directives and regulations, and private forms of regulations adopted by private associations or firms to

[3]As Farrell and Newman point out, there "is a controversy over whether the European Union should be considered a state" (2019*a*: footnote 21, ch. 1). In fact, viewing the European Union as a traditional foreign actor or a governance system can lead to different analyses and findings (Lavenex 2014). It is still considered that the importance of European politics for global regulatory debates combined with its relatively high level of independence from European national politics allows to view the European Union as a polity like other sovereign states.

regulate the behaviour of private companies. The full list of regulations was identified using previous research (Cavoukian and Crompton 2000; European Commission 2001*a*, 2012*b*; European Parliament 2012; Rodrigues and Papkonstantinou 2018; Trzaskowski 2006) and is listed in Appendix B. A network analysis and the broader structure of interactions between private associations then serve as the independent variables to explain how previous exchanges between them affected their exploitation and exploration over time. Data on their interactions were collected on the website of all private organizations. Two actors were considered to have interacted when one publicly reported having worked or be working with another.

I finally draw on 36 semistructured interviews to complete my analysis with representatives from American federal agencies (i.e., Federal Trade Commission & Departement of Commerce), European Commission directorate-generals (i.e., DG Justice & DG Connect), European institutions (i.e., European Data Protection Board, European Data Protection Supervisor), private associations (i.e., TrustArc, FEDMA, etc.) and civil society groups (i.e., BEUC). All interviewees were identified based on their work experience and affiliation. In fact, they worked at most of the public and private organizations looked at in this research. The full list of interviewees is reported in Appendix A. All interviews lasted more or less an hour and a third of them were conducted in person while doing a research stay in Brussels. The other two-thirds were done on the phone. Throughout this research, interview data is used in an "integrative" and "interactive" way with the other methods used (Bowen 2009; Seawright 2016). Rather than aiming to produce a different causal explanation, it serves to confirm the evidence coming from the content and network analyses. Interview quotes are inserted throughout the text to provide an additional layer of commentary. For confidentiality reasons, quotes are never associated with a specific interviewee. Interviews were moreover used to double-check the quality of the data collected from other sources. All interviewees were notably asked with which organizations apart from the one they worked at did they have contact over the years to verify the information collected online and used for the network analysis. They were also asked which other organizations did they consider to be the most important actors in the regulation of privacy to confirm that the population identified for this research was exhaustive. The content and network analyses were, in turn, used to generate interview questions and sometimes challenge interviewees on their answers when it did not necessarily fit the evidence that had come out from these two other methods.

1.6 Roadmap of the Thesis

The remainder of this work is divided into six chapters. Chapter 2 begins by building my theoretical framework and explaining how complexity theory can be used to comprehend the evolution of data protection rules in the transatlantic space. It details the epistemological and ontological shift that it suggests to study increasingly interdependent and interconnected economies. It does so by previously reviewing how the formation of rules was previously theorized in international political economy and notably in the literature specialized on private authority. It finally introduces the two main processes, exploitation and exploration, analyzed thereafter.

The theoretical framework in place, chapter 3 describes how the American and European privacy systems can be conceptualized as two closely interacting units instead of two competing legal systems as they traditionally are. In doing so, it traces the origins of the concept of privacy in both jurisdictions and how they compare to each other. It points out that while both start from a liberal root, the American approach has embraced a more 'market-based' approach and the European Union follows a more 'rights-based' approach. It then presents how these differences relate to their respective regulatory approaches. As opposed to most previous work on the topic, though, it ends up highlighting that from these broad differences they actually have a lot in common, and both in practice adopt a hybrid form of regulation rather than one of the ideal-type generally ascribed to them.

Chapter 4 builds on this finding to explain how the transatlantic privacy system actually forms a complex governance system and offers a broad overview of how it evolved since 1995. After detailing how the database used for this research was created, it showcases how the content of the rules promoted by American and European authorities differed early on. It subsequently indicates how this changed over time following the tendency of public and private actors to exploit and explore data protection rules based on their previous interactions. It finally points out that while the exploitation of rules has pushed them closer than ever to each other, the exploration of new ones has also spurred greater divergence and impeded them from ever becoming alike.

Chapter 5 gives a closer look at the process of exploitation and how private actors specifically supported a regulatory convergence between the United States and the European Union. It does so through a careful longitudinal analysis of the evolution of

interactions between public and private actors and the content of the rules that they included in their respective codes of conduct, certification schemes, and other forms of private regulation. The analysis follows a number of specific events that led to the development of new interactions and supported the exploitation of rules between American and European actors. It finally emphasizes how while doing so, they often ended up extending the influence of public authorities that had first devised these rules.

Chapter 6 turns its attention to the second main process, the exploration of new rules, animating the evolution of the transatlantic privacy system, and examines how private actors have contributed to it. While chapter 5 shows that private actors often ended up acting as a kind of transmission belt for public rules, this chapter questions to what extent do they also contribute to the creation of new rules. It first shows that they did create new rules by assembling previous ones that they came to include based on their previous interactions. Yet, it then highlights that it was never as significant as it was sometimes touted or expected. While providing an essential source of learning, the multiplication of sources of regulation indeed created fragmentation and limited the interest of many private actors to take risks and innovate. As such, they did not provide as much flexibility and even lead to a form of regulatory capture. It is finally emphasized that this sub-optimal outcome for states and consumers can be overcome by greater involvement of public actors in the process leading to the creation of industry self-regulations.

Chapter 7 concludes this research. In addition to summarizing its findings, it reiterates the value of adopting a complexity approach to study the evolution of global regulatory issues and what it can more broadly offer in the study of international relations and international political economy. It finally discusses some practical implications and avenues for future research.

Chapter 2

Regulating in a Complex World

If things were simple, word would have gotten around.

Jacques Derrida, 1977

There are few more central concepts in our modern societies than the one of rule. As we go about our daily lives, we are constantly faced with all sorts of rules. From very abstract constitutional ones that set the basic framework of our political systems to food standards that determine what we can eat, most of what we do is regulated in one form or another. Broadly defined, rules are "specific prescriptions or proscriptions for action" (Krasner 1982: 186) that in turn shape our realm of possibilities[1]. These obviously include legal rules that are enforced by public authorities, but these are just one part of it. As Peter Drahos and John Braithwaite aptly point out rules "do not have to be incorporated into state law or international law to have significance" (2000: 10). Many non-state actors regulate their own activities as well as those of others through

[1] As this definition should make clear, the concept of rule is closely associated with the one of institution and most definitions of an institution indeed refer to the concept of rule. Douglass North quite straightforwardly define institutions as the "*rules* of the game in a society" (North 1990: 3; emphasis added). While outlining the institutional standpoint in international relations, Keohane similarly talks of "students of institutions and rules" joining them as almost one and the same entity (Keohane 1984: 8). If one needed to make an absolute distinction between the two concepts, it would mainly be one of degree where institutions mostly represent a collection of rules and rules being the constitutive units of institutions. As this work is especially interested in what standards of behaviour are specifically promoted, the concept of rule was seen as more appropriate but the two could almost be used interchangeably.

the adoption of internal policies, codes of conduct, guidelines, and other forms of private regulation (Vogel 2008). The relatively recent rise of an entire certification industry aimed at promoting sustainable production processes in various global value-chains is one prominent example that attracted a lot of interest over the years (Auld 2014; Cashore, Newsom and Auld 2004; Grabs 2020; Renckens 2020). Not all cases of private rules are however as visible and many businesses make choices that set the boundaries for our future actions before we even become aware of it. Through technical design and various policy decisions, internet companies notably control what information we can access, with whom we can interact, how value can be exchanged online, and how personal data can be collected and used (Benkler 2011; DeNardis 2009; Tusikov 2016).

Despite years of neoliberal economic policies pushing for *deregulation*, we are thus still very far from living in an unregulated or even lightly regulated environment. Evidence indeed suggests that the widespread privatization of economic activities that occurred since the 1980s in many countries around the world was never associated with "an end to all regulation" (Majone 1994: 80; see also Levi-Faur and Jordana 2005*a*). The concept of deregulation is actually based on a wrongful dichotomy drawn between markets and rules. Following on the work of Hayek (1984), many economists and political scientists tended to see markets as a form of 'spontaneous order' that followed a different logic than the one promoted by regulations. The latter were then closely associated with an intervention of the state going against the supposedly natural ordering of markets and that should thus be kept to a minimum (Scott 2003: 148). In reality, though, rules are central to the good functioning and even constitution of markets (Levi-Faur 2017; Scott 2003; Shearing 1993). They set expectations and determine how actors are supposed to interact together. What changed in recent years, though, is who sets them. Rather than states being the sole or main source of rules, non-state actors nowadays also play an increasingly important role in the regulatory process and notably in the formation of new rules. As such, the whole deregulation discourse could really "better be described as "reregulation," but in a different form than before" (Renckens 2020: 15).

Non-state actors acting as regulators is not entirely new (Braithwaite and Drahos 2000; Cutler 2002). There is, however, a broad consensus that their importance has risen in recent years (Avant, Finnemore and Sell 2010; Cashore 2002; Cashore, Newsom and Auld 2004; Cutler, Haufler and Porter 1999; Haufler 2001; Green 2013*b*; Mattli and Woods 2009). What caused this is still debated (Büthe 2010). For some, it is "the scale and structure of contemporary global production [that] challenge the capacity of even

highly developed states to regulate activities that extend beyond their borders" (Abbott and Snidal 2009*a*: 44). Others argued that by challenging traditional geographical and jurisdictional boundaries new technologies are forcing a "retreat of the state" (Kobrin 1998, 2004; Spar 1999). While it is increasingly recognized that digital technologies did not really impede states from regulating the online world as some early technological enthusiasts perhaps hoped for, it is generally agreed that they did force states to collaborate more with new private intermediaries (Goldsmith and Wu 2006; DeNardis 2009). For yet others, this is all part of a broader transformation of capitalism and reconstitution of the public sphere on the global scene (Braithwaite 2008; Levi-Faur and Jordana 2005*a*; Levi-Faur 2017; Ruggie 2004). Despite obvious differences, all these explanations are united in their recognition that structural changes are reshaping the global economy and making it, for better or worse, more transnational than ever. What they all fail to grasp, though, is that more than simply allowing the emergence of new sources of authority and rules these structural changes have also altered the process of rule formation itself.

In the present work, I argue that the growing interaction between state and non-state actors developing rules in multiple jurisdictions can be viewed as a complex governance system that changes how global rules emerge (Kahler 2016; Farrell and Newman 2019*a*; Oatley 2019; Orsini et al. 2019). In the remainder of this chapter, I review some of the recent strands of literature that have addressed this question and introduce the theoretical framework that I will then use to analyze the formation of data protection rules in the transatlantic area since 1995. I start by highlighting the extent to which regulatory systems are now interdependent and what this means for regulatory debates. I then review how the 'market power explanation' has been used to explain the emergence global rules are formed and point out some of its limitations. I notably argue that it failed to pay sufficient attention to the role of private actors in the regulation of the global economy and I contrast it with the recent literature on private authority. Following on these points, I discuss how the literature on policy diffusion has made a first step at recognizing the interdependence of policy processes. I finally elaborate on the value and meaning of using a complex system approach to study global regulatory processes.

2.1 Global Rules for a Global Economy

In today's world, national markets are built on regulations developed in multiple jurisdictions and by multiple actors. As states open up their national economies, notably through

the negotiation of bilateral and multilateral trade agreements, rules that once had a limited geographical scope of application end up having effects outside of the jurisdiction where they were originally adopted (Bach and Newman 2007; Farrell and Newman 2010). Most companies nowadays have to consider how various jurisdictions regulate their activities before starting to produce their goods and services. Even when private companies do not realize it, they are more often than not influenced by rules adopted in multiple jurisdictions. If they are importing raw materials or part of their production processes is taking place in another country, their end products will most certainly have been shaped by rules not set by their national governments. This is assuming that it is easy to identify their nationality. Following the liberalization of financial flows in the last few decades, private companies are now regularly tied to multiple jurisdictions. While their head-office may be in one country, they will often have made or received foreign investments, which can force them to consider the financial rules of foreign countries.

The increasing use of extraterritoriality is yet another situation where private companies might be compelled to deal with rules from another jurisdiction even when they are not directly active there (Putnam 2009; Raustiala 2009). Based on this legal concept originally developed in the United States, many states now consider that they have legal authority over activities happening outside their jurisdiction if they have an 'effect' on their territory or citizens. With the advent of the Internet and the collapse of spatial distances (Der Derian 2003; Rosenau 2003; Ruggie 1975), the number of acts taken in one jurisdiction that can have an effect in another jurisdiction has risen considerably and increasingly lead public regulators to use extraterritorial measures. The General Data Protection Regulation (GDPR) in that regards continues the practice set out in the European Data Directive in specifying that it applies to the processing of personal data of Europeans wherever it occurs in the world (Art. 3). A non-European firm that could have never intended to be physically active in Europe will thus have to respect European data protection rules when dealing with the personal information of individuals from there.

The globalization of the economy has in short not only allowed the exchange of goods and services but also made national legal systems interact with each other. As opposed to "the ruleless space of anarchy" often assumed in international politics, market actors are faced with a world of overlapping rules and institutions (Farrell and Newman 2019*a*: 27). This is not without costs. Having to deal with multiple rules can be a daunting task for private companies, and especially smaller ones that do not

have the means to pay a legal team dedicated to ensuring that they respect all their legal requirements. In some cases, it might even be that complying with the rules of one jurisdiction will mean violating rules in others (Farrell and Newman 2019*a*: 27). A request from enforcement authorities in one jurisdiction to provide personal data for a criminal investigation could notably end up violating data privacy laws where the personal data is currently located or originally coming from. This was precisely the topic of a hotly debated case in the United States as Microsoft was requested to produce emails saved on servers located in Ireland by the Federal Bureau of Investigation. In the view of Microsoft and the European Parliament, which filed an *amicus curiae* in this case, fulfilling this request was however in violation of European privacy law. The case was since then vacated by the adoption of the Clarifying Lawful Overseas Use of Data Act (CLOUD Act) in 2018 specifying that law enforcement could require to have access to data located outside the United States. Far from solving the broader legal conundrum, the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS), the two main European privacy watchdogs, indicated that this new law could be in conflict with the application of GDPR. Other cases where private companies will have to deal with conflicting legal requirements are thus to be expected.

In addition to potential economic costs, the growing interdependence of national economies often raises normative issues. As products and services cross national frontiers, legal systems and rules also clash because of the different values that underpin them. For example, conflicts over food standards are not merely about economic gains but also cultural preferences over how what we eat should be produced. If the European Union has been constantly more wary of supposed proofs of the safety of genetically modified organisms, it is in part because it does not view it as being a purely scientific issue (Young 2003: 464-5). It is also a social issue that questions what individuals are ready to consume. Such normative clashes are present in a wide variety of other issue-areas, including privacy. While the latter is officially enshrined as a fundamental right in Europe, it is often seen as a consumer issue in the United States. How companies manage personal data in the transatlantic area thus necessarily tend to encroach on normative preferences (Schwartz and Peifer 2017). In the most extreme scenario, this divergence could lead to a simple end to personal data flows as feared by some businesses in what would not be too different from the current outcome in the case of genetically modified organisms.

In this context, both public and private actors thus have an interest in promoting global rules to ease these various tensions and ensure the proper functioning of a global economy. In the specific case of privacy, ever since the adoption of the Data Directive in 1995 the European Commission has in effect continuously attempted to ensure European rights were guaranteed wherever their data is processed and to simultaneously ensure a fair level playing field for its companies. The American government has similarly been prone to engage with its European, but also Asian, counterparts to ensure that data flows would not be disrupted. In both jurisdictions, private actors were also interested and sometimes even encouraged to adopt regulatory documents detailing how they would protect personal data. How global rules emerge in this complex environment is a key question for students of global economic governance.

2.2 The Market Power Explanation

Following on the work of Daniel Drezner, a leading answer has been that 'great powers' – here understood as "governments that oversee large internal market" – are the ones setting the rules of the game (2007: 5). More precisely, when the United States and the European Union have similar regulatory preferences, coordination will be successful. In the absence of "great power concert", any "coordination will [however] be incomplete, and nonstate attempts will prove to be a poor substitute" (2007: 5). The concept of 'coordination' is significantly used by Drezner to highlight that it is an agent-driven process and that the dependent variable does not necessarily have to take the form of regulatory convergence. Coordination could indeed result in an agreement "on the acceptable bounds of regulatory policies" and still not promote "identical rules or regulations" (Drezner 2001: 57).

While compelling, this 'market power' explanation leaves many questions unanswered. For one, it does not explain why the European Union, not the United States is broadly viewed as the new regulatory power (Lavenex and Schimmelfennig 2009; Newman and Posner 2015; Vogel 2012; Young 2015*b*). Even outside of academia, widely-read American newspapers have for quite some time now pointed out that Brussels has replaced Washington as the most important city for American lobbyists (Lipton and Hapkim 2013; Mitchener 2002). One answer to this is that the market explanation is a necessary, but not sufficient condition to explain a jurisdiction's global influence. According to Bach and Newman, the missing link is what they label as 'regulatory capacity' (2007). In short, a jurisdiction not only needs a large market, but also the capacity "to

formulate, monitor, and enforce a set of market rules" (Bach and Newman 2007: 831; see also Damro 2015) if it wishes to have any say on which rules are applied globally. The case of privacy is a particularly good example to see how.

Despite having limited results in unifying privacy regulations in Europe (Bamberger and Mulligan 2015: 9), the European Data Protection Directive of 1995 at the very least unified market access decisions to the European 'data economy' (Bach and Newman 2007). Following the adoption of the Directive, European regulators were in charge of allowing foreign companies to use personal data of European citizens, mainly through adequacy decisions[2] or binding corporate rules[3]. These powers were moreover consolidated with the creation of transgovernmenal institution, the Article 29 Working Party[4], which was tasked to advise the European Commission on the application of the Data Directive. Meanwhile, the American legal privacy system remains to this day fragmented and no single agency has the sole authority over privacy issues (Bach and Newman 2007: 836).

This important regulatory capacity combined with the importance of the European single market are essential elements to understand why the European Union has such an influence over the global regulation of privacy and why multiple countries, like Canada, Japan, India, Brazil, and most recently Nigeria, adopted laws seen as inspired by the European privacy rulebook (Chander, Kaminski and McGeveran 2020; Gordon and Ram 2018; Satariano 2018). It would also explain why the European Union was able to bring the United States to negotiate the Safe Harbor (2000) and then the Privacy Shield (2016) agreements setting out *sui generis* frameworks to govern the use of European personal data by American companies. These two agreements in effect aimed to replace an adequacy decision, which the United States could not get in the absence of a comprehensive privacy law at the federal level, by relying on 'enforced self-regulation'. In short, private companies were expected to self-certify their compliance with privacy principles listed in these two international agreements, which the Federal Trade Commission could enforce if violations were found. Again, for Drezner (see p. 9 above), this outcome was not considered to be a real example of coordination due to the multiple

[2]Adequacy decisions is a mechanism by which the European Union indicates that another country's privacy regulations are equivalent to its own and its companies may deal with the personal data of Europeans just like if they were in Europe.

[3]Binding corporate rules are rules that a company builds to allow for personal data of Europeans to be transferred to a country with no adequacy decisions. These rules need to be approved by national data protection authorities under an EU cooperation agreement.

[4]The Article 29 Working Party has now been replaced by the European Data Protection Board in the GDPR.

compliance failures that were notably at the heart of the demise of both agreements. At the same time, the United States did have to change its position to fit European preferences (Farrell 2003). While not being a complete reversal, it did show some form of coordination that seems hard to imagine if the European Union had not unified its market access and built up its regulatory capacity. It can moreover help explain why the United States was able to push back European privacy demands in the very specific cases of the use of personal data for law enforcement purposes (e.g., access to airline passenger data or financial transactions data), a policy area where the United States itself holds an important regulatory capacity (Bach and Newman 2007; de Goede 2012).

Still, this 'regulatory capacity' or somewhat updated version of the market power explanation has its own shortcomings. To go back to Drezner's point, it is striking that the European influence appears to have had a relatively limited direct impact in the United States. In addition to not bringing any regulatory change, there were not even that many private companies that self-certified to the EU-US Safe Harbor or Privacy Shield Agreements. According to the Department of Commerce's own report, there was just a little bit over 5000 by its demise in 2016[5]. Approximately, the same number of companies had also self-certified under the Privacy Shield[6]. If this could be taken to mean that the United States was actually successful in blocking any real change, it certainly does not explain why on the ground researcher find that American and European private companies follow similar practices when dealing with personal data (Bamberger and Mulligan 2015: 12). It also does not explain why rules that were first devised in the United States, including for the protection of children's data, the passive collection of personal data, or data breaches, are now part of the GDPR and the 'European' rulebook. This goes against the seemingly unilateral way that regulatory coordination is supposed to function according to the market power explanation.

Another important lacuna of this specific explanation is that it takes any regulatory outcome, like the Data Directive or more recently the GDPR, as a stable equilibrium. Following the adoption of the Data Directive, it is almost as if the European and American regulatory system did not change up until the adoption of the GDPR in 2016. As it will be discussed in chapter 3, both the European Union and the United States' privacy frameworks have however been continuously evolving in the last twenty years. In addition to legal changes, private companies even had the opportunity to build on the regulations adopted in both jurisdictions. According to interviews done by Kenneth Bamberger and

[5]The full list of companies is available online at: https://www.export.gov/safeharbor_eu.
[6]The full list of companies is available online at: https://www.privacyshield.gov/list.

Deirdre Mulligan with data supervisors in American companies (2015: 61-66), legal compliance with American or European rules was only a small part of their privacy practices, which are increasingly codified in codes of conduct or other soft law documents. This again points to the importance of giving more attention to the role of private actors to understand how the regulation of privacy has evolved in the last twenty years. Just as in so many other issue-areas, they are not merely implementing rules devised by governments or international organizations, but active regulators in themselves.

2.3 From Public to Hybrid Rule-Making

Despite early calls to look at the role of transnational actors in world politics (Nye and Keohane 1971; Strange 1994), the state-centric paradigm has dominated academic debates in international political economy since the early 1970s. In effect, the first outgrowth of the work on transnationalism of Robert Keohane and Joseph Nye (1971; 1977) has not been a greater recognition of non-state actors as a key unit of analysis, but a new focus on how states could achieve cooperation in face of the growing issues of living in an interdependent world. Over the years, regime theory and, more broadly, the study of international institutions (Haas 1980; Haggard and Simmons 1987; Keohane 1984; Krasner 1982; Young 1980) that resulted from this new research interest quickly became as state-centric as previous theories of international politics. The rise of transnationalism and interdependence thus became seen as an exogenous shock on international politics, rather than an independent or dependent variable.

Since the mid-'90s, there is however a revival of interest in the role of non-state actors (Risse-Kappen 1995). While early concepts like 'epistemic communities' (Haas 1992), 'transnational coalitions' (Risse-Kappen 1995) and 'transnational advocacy networks' (Keck and Sikkink 1999) emphasized the impact of non-state actors on domestic or international policy-making, many scholars were quick to point out that non-state actors, and chiefly private companies, could also act as regulators in their own right (Braithwaite and Drahos 2000; Cutler, Haufler and Porter 1999; Cutler 2002). For some, this was taken to be an indication that states had lost their lost their "monopoly position in the production of public goods" (Grande and Pauly 2005: 288). In reality, it can be questioned if states ever had such a monopoly position. Since medieval times, merchants have been key players of global governance and have regularly developed their own legal practices or *lex mercatoria* (See Braithwaite and Drahos 2000: 54 or Cutler, Haufler and

Porter 1999: 4). Having said that, private authority is now the source of a thriving scholarship and it is widely recognized that private actors can also act as rule-makers (See inter alia Avant, Finnemore and Sell 2010; Bartley 2018; Graz and Nölke 2008; Green 2010, 2013*b*; Mattli and Büthe 2003, 2005; Mattli and Woods 2009; Spruyt 2001; Vogel 2005).

In a relatively recent contribution, Burkard Eberlein and his colleagues (2014) built an analytical framework highlighting the different governance tasks where transnational businesses regularly interact with public actors. These are summarized in table 2.1 below. While each governance tasks has its own relevance, rule formation is the focus of this research and is defined as *the interactive process through which rules are devised and institutionalized in formal documents at the national, transnational, and international level*. In line with Eberlein et al. (2014), this process is taken to involve both governments and businesses. Other actors, like formal intergovernmental organizations and non-governmental organizations (NGOs), are also significant and should not be discarded easily (Abbott and Snidal 2009*b*, 2010; Raymond and DeNardis 2015). Yet, it appears that governments and businesses have had the last word in making the rules for the regulation of data protection and privacy.

Table 2.1: Transnational Business Governance's Regulatory tasks (Adapted from Eberlein et al. 2014: 7)

Regulatory tasks	Definition
Goal/agenda setting	Define the regulatory objectives to achieve
Rule formation	Set up the rules to be applied
Implementation	Apply the rules to a specific issue-area
Monitoring and information gathering	Oversee the application and gather information on it
Compliance promotion and enforcement	Encourage the respect of the rules and apply sanctions
Evaluation and review	Provide feedback on regulatory implementation

In the case of international organizations, the Organisation for Economic Cooperation and Development (OECD), Asia-Pacific Economic Cooperation (APEC), and Council of Europe have all been important forums where privacy rules have been formulated. As a matter of fact, the OECD privacy framework of 1980 and its revision of 2013 are still the closest thing we have to a global standard for privacy regulation. Meanwhile, the APEC privacy framework of 2005 and the Convention 108 of the Council of Europe are two additional forums where the United States and the European Union have

respectively pushed their regulatory agenda on the global stage. All three international organizations were thus significant, but not so much as agents of change themselves, but rather as forums where rules were formulated by governments and businesses. In all three cases, the rules formulated were the result of the work of a group of experts (OECD) or an international negotiation (APEC and Council of Europe) where the primary input came from government officials and non-state representatives. While it is not assumed that it could not be different in other issue-areas, international organizations are thus seen as the locus of rule-making, but not rule-makers themselves for the rest of this research.

As for NGOs, they also played a crucial role in the evolution of privacy rules in the last twenty years and it would be foolish to dismiss them too quickly. This is especially the case in Europe where the GDPR has been one of the most lobbied European regulation (Atikcan and Chalmers 2019). Private businesses or their associations were obviously behind a large chunk of this activity as it was well documented[7]. Yet, important civil society groups like The European Consumer Organisation (BEUC) and European Digital Rights (EDRi) were also quite active and were able to advance their propositions at multiple points in time. As opposed to private businesses, civil society advocates however largely did not themselves create rules. In effect, they mostly stuck with their advocacy role, rather than taking the one of rule-maker[8]. Many reasons, including financial ones, explain this, but it is noteworthy that civil society representatives do not seem to believe that it is their role to be rule-makers. According to one representative of a civil society organization interviewed for this research: "We don't pay much attention [to the development of private rules] because we focus on the actual law and implementation of it. [...] It is mostly a tool for companies, not for [us]." (Interview E13, done on February 14th, 2019). In an informal discussion, another similarly held that it was not their role to set the rules for private companies. In this context, this research will consider civil society groups as actors influencing the process of rule formation but who are not rule-makers themselves.

It must finally be emphasized that governments and businesses are not seen as equal actors in the process of rule formation. If both can be considered as rule-makers, their different source of authority has implications for their capacity to act as such. Studying the emergence of private authority, Jessica Green (2013*b*) differentiates be-

[7]For a good analysis of the influence of lobby demands on the regulation, see the following website: https://lobbyplag.eu/lp.

[8]One notable exception was the development of a trustmark by a network of consumer organization led by the British one named Which?.

tween a delegated and entrepreneurial form. While the former represents a "traditional principal-agent relationship, where the agent's authority stems from explicit transfer of authority from state [actors]", the latter describes a situation where "authority accrues through a process that culminates in the governed deferring to the governors" (Green 2013*b*: 33-34). This opposes a form of *de jure* to *de facto* authority and is at the heart of the difference between public and private regulators. Even though national governments cannot make any claims of legitimacy to devise global rules, they still are a source of legal authority. When they agree with each other, they can force private actors to respect the rules they want. At the domestic level, they also remain sovereign and can force private actors to adopt a specific behaviour in respect of their international obligations.

Meanwhile, without any delegation, private businesses only have authority insofar as the governed (themselves, but also governments) accept it. This importantly means that they cannot go against the will of public authorities. This would be counterproductive as they would only risk losing their authority. To put it differently, private rules are of use if they can "lower transaction costs, increase reliability, and generally achieve efficiency gains" (Büthe 2010: 10; see also Green 2013*b*: 41), which simply cannot be achieved by promoting rules going against the ones put forward by public authorities. What private businesses can however do is support additional rules. These can either be by specifying or adding new requirements, but they cannot really limit or undermine preexisting ones established by public authorities. What will thus often occur is not that public and private rules will challenge each other, but that they will be layered one on other (Bartley 2011; Green 2013*a*).

Even in cases of 'entrepreneurial private authority', private regulators will often try to link themselves to public rules to increase their legitimacy. In many ways, public rules can actually play a "coral reef function, attracting private rule makers" and catalyzing their rule-making activities (Green 2013*a*: 2). This specific nature of public regulators and their regulations will be key to understand the evolution of private rules. At the same time, both delegated and entrepreneurial forms of private authority can also influence public regulators. They can notably promote new rules, reformulate the problems at hand, diffuse public rules across jurisdictions, and help rule harmonization (Green and Auld 2017: 261). The distinction drawn between the 'delegated' and 'entrepreneurial' form of private authority can even collapse as public actors get involved in the regulatory processes of private actors (Renckens 2020: 6). Public actors can in effect attempt to support or limit the development of rules by private actors to which it did not

beforehand delegate any regulatory task (Cashore, Newsom and Auld 2004; Gulbrandsen 2014). Rule formation should thus be seen as an interactive process between both public and private regulators as highlighted in the aforementioned definition.

This interactive process of rule formation importantly also runs across national boundaries. As previously mentioned, the globalization of the economy has also meant that firms and governments increasingly have to consider rules adopted in other jurisdictions. This is moreover true both in terms of compliance and rule formation. In effect, the process of formulating rules and institutionalizing them is not happening in a vacuum. One of the main factors behind the adoption of a specific rule is what will already be out there. Just as international "negotiations do not start on a blank slate" (Meunier and Morin 2015: 146; see also Pauwelyn 2014), rule formation at both the national and transnational level always occurs in the backdrop of existing rules and institutions developed in multiple jurisdictions at the same time. How these actually affect the process of rule formation is the key argument of this research and will be further developed in the following sections.

2.4 Policy Diffusion: A Limited Approach to Study Interdependence

The literature on policy diffusion has probably been the first to explicitly recognize the interdependent nature of policy processes in international studies (Dobbin, Simmons and Garrett 2007; Elkins and Simmons 2005; Elkins, Guzman and Simmons 2006; Lazer 2005; Levi-Faur and Jordana 2005*b*; Meseguer 2005; Meseguer and Gilardi 2009; Meseguer 2009). As Gilardi (2012) recalls, this is however something that had long been recognized in other social sciences. Since the formulation of the "Galton Problem", named after the British statistician who originally enunciated it, it had been widely recognized that rules, customs or other practices in specific geographical areas can often come "from a common source, so that they are duplicate copies of the same original" (Gilardi 2012: 457). Building on this, the policy diffusion literature has over time identified four mechanisms through which it can occur: coercion, competition, learning, and emulation (Dobbin, Simmons and Garrett 2007). As summarized in figure 2.2, they all function according to different resources and forms of interactions.

Table 2.2: Different pathways for rule diffusion (inspired by Drezner 2007 & Lavenex 2014)

	Direct Political Influence	Indirect Socio-economic Influence
Material resources dominate	Coercion	Competition
Ideational resources dominate	Learning	Emulation

Coercion refers to a situation where an actor can use its material resources to directly force another to adopt its policy. The use of conditionality by the European Union is one common example (Lavenex 2014: 889). As other countries want to join its single market, they are required to adopt European rules. The promise by the United States to lower tariffs in exchange for policy reforms is a quite similar form of coercion (Dobbin, Simmons and Garrett 2007: 454). The use of structural adjustment programs by the International Monetary Fund is another case where specific states are hard-pressed to apply specific policies. Faced with the need to get financial help, many developing countries have in effect been forced to implement economic reforms following a neoliberal agenda elaborated in Washington (Gilardi 2012: 466).

While also based on the use of material resources, competition works indirectly. It occurs when policies in one jurisdiction risk to create externalities in another and force it to change its policy accordingly. For example, Beth Simmons and Zachary Elkins (2004) maintains that the adoption of financial liberalization policies in one developing countries can lead its neighbours to adopt a similar policy for fear of losing out international investments[9]. A similar, but perhaps more positive, logic is at play with the now famous "trading-up" phenomenon described by David Vogel (1995). According to it, private firms often end up applying regulations of big markets as they prefer to follow one set of rules. Originally developed to discuss the impact of California laws on other American states, it is now often used to qualify the normative power of the European Union and dubbed the 'Brussels' effect' (Bradford 2012, 2020; Damro 2015). It is here worthwhile to note that competition has also been seen as pushing towards greater divergence rather than convergence in the organizational literature. Michael Hannan and John Freeman (1977; 1989) most famously pointed out that organizations often aimed to 'survive' by finding 'niches' and differentiating themselves from others.

[9]As discussed extensively by Lauge Poulsen (2016), this is a particularly good example of bounded rationality as policy officials in many countries were blind to the high risks that these liberalization policies entailed.

As opposed to both coercion and competition, learning is an ideational process by which someone directly learns new evidence and change his belief accordingly (Dobbin, Simmons and Garrett 2007: 460). It can both take the form of a rational bayesian or socialization process. According to the first one, an actor will update his knowledge based on someone else's actions (also called vicarious learning). States can, for example, evaluate the results from the adoption of a specific policy in another jurisdiction. As Frank Dobbin and his colleagues (2007) point out, Tatcherism can be seen as a natural experiment on the impact of privatization of public institutions. Meanwhile, socialization "is less choice-driven" than what is portrayed in a Bayesian model of learning (Lavenex 2014: 890). Following the 'logic of appropriateness' (see Checkel 2005), it is considered that as actors get more information about a specific policy, they learn more about its normative value and decide to implement it for this reason. Nongovernmental channels, like advocacy networks and epistemic communities, are often recognized as important actors in such a process.

Finally, emulation is both an ideational and indirect process. Here, I slightly diverge in my definition of this mechanism than other prominent scholars that define it in very similar terms to the process of socialization just mentioned. Sandra Lavenex for example distinguishes emulation from socialization by the actors involved. Socialization occurs when states representatives are directly involved, while emulation is an indirect process that occurs when non-governmental actors are involved (2014: 891-2). For his part, Fabrizio Gilardi (2012) defines emulation exactly as Lavenex defines socialization and dissociates the latter from a learning process. Meanwhile, Frank Dobbin and his colleagues (2007: 450) largely subsume socialization and emulation together as being part of a constructivist approach to diffusion. These discrepancies importantly illustrate that both socialization and emulation are driven by ideational factors and not material ones. The difference that I draw between the two is however around the absence of direct or "point-to-point" interactions between the actors that are behind the diffusion (Meyer and Strang 1993; Meyer 2000). While socialization implies a direct relation, emulation describes a situation where an actor simply decides to adopt the policies promoted in another jurisdiction because of cultural linkages, close normative proximity, or similar economic circumstances. The institutionalization of similar theories or analytical categories can similarly support the emulation or "isomorphism" of the policies adopted (DiMaggio and Powell 1983). By its very nature, this mechanism is hard to verify empirically as it is supposed to occur without having any apparent or visible link. It has thus been often used to explain diffusion when other mechanisms do not seem to hold. David

Strang and John Meyer precisely justify this approach by arguing that the diffusion of many important policies (e.g., Keynesian economic planning or privatization) need to be understood in light of "levels of international interaction and interdependence [that] are not self-evidently high, relative to national or local settings" (1993: 490).

Altogether, the diffusion literature has been particularly good at identifying mechanisms playing a role in the diffusion of policies across borders. Here presented separately, it should be noted that they often coexist and this has often meant that each mechanism has been quite difficult to disentangle from the others, with some negatively concluding that different scholars often ended "attributing identical phenomena to different mechanisms" (Dobbin, Simmons and Garrett 2007: 462) or stating that "empirical evidence usually is ambiguous and unable to discriminate convincingly among these different explanations" (Gilardi 2010: 650). Rather than viewing them as competing hypotheses, they can however also be seen as mechanisms that reinforce each other, both simultaneously and over time. Paul Dimaggio and Walter Powell (1983) for example talk of "coercive isomorphism" to highlight that similar ideas institutionalized at the state or dominant organizations-level can then be directly imposed on others. Putting aside the difficult question of integration and development of cumulative knowledge, the diffusion literature was an important step in the study of policy interdependence. It notably goes further than the market power explanation by highlighting the existence of multiple pathways of influence working both through public and private actors. Most concepts associated with the four mechanisms just reviewed will actually be used throughout this research. At the same time, it did not succeed in fully integrating what interdependence has meant for the process of rule formation in different jurisdictions.

There was first a tendency to focus on the diffusion of large policies (Lütz 2011). Many diffusion studies looked at how regulatory capitalism, privatization policies, or models of bilateral investment agreements were spreading across the world (Elkins, Guzman and Simmons 2006; Jordana and Levi-Faur 2005; Simmons and Elkins 2004). This tends to obfuscate the fact that interactions now occur at many regulatory levels and that diffusion does not have to be limited to such broad policies. Similar rules can actually be adopted by regulators following different regulatory approaches. This is notably what will be seen in chapter 5 while discussing at greater length the case of privacy regulation. The time factor is also quickly brushed aside in many diffusion studies. The main argument concerning time is that diffusion will often take an S-shaped form with few adopters in the early days of an innovation followed by a significant rise in their numbers

and a few late adopters (Gray 1973). In most diffusion studies, the specific period of time where policies are quickly spreading is the dependent variable. How the patterns of influence and interactions themselves evolve throughout time are often not considered.

Concomitantly, the relation between specific agents and the structure of interactions is taken to be fixed. You either have one actor influencing another through a given structure of interaction or the broader structure influencing one given actor at a specific point in time. How they each influence their evolution is disregarded. This is linked with the most important blind spot of this literature, which is that it tends to present a unidirectional picture. Feedback situations where one actor would be influenced and later on be the 'influencer' are rarely if ever discussed. Similarly, how the diffusion of certain policies would affect the development of future policies is also outside their analytical framework. Only quite recently, research in this field has started to question how institutional or organizational novelty emerge (Padgett and Powell 2012). All of this reflects the conscious effort to simplify the real world and build a simple account of how interdependence affects the adoption of policies worldwide. This is in line with the traditional 'Newtonian approach' of science, which has come to dominate both natural and social sciences. As I will now argue, adopting a complex system approach would allow us to overcome these limitations and offer a more complete understanding of how interdependence affects the process of rule formation.

2.5 Taking Interdependence Seriously: A Complex System Approach

Following in the footsteps of economists (Ma 2007; Varoufakis 1998), students of world politics and international political economy have for quite some time adopted a 'Newtonian' or classical mechanic model. According to the latter, the world is akin to a clocklike machine that can be torn apart for analytical purposes (Bousquet and Curtis 2011). The 'clock metaphor' is significant. A clock is not a simple object and many people would have a hard time building or repairing one. However, it can be relatively easily split up into individual parts and the effect of one part on the other is linear (i.e., proportionate and constant). A clock is also (in theory) a closed environment, which means that its inner working is not affected by the outside world. Following this view, the study of

political systems traditionally aims to explain deterministic or probabilistic laws, which can be uncovered by looking at the relation between discrete elements (or variables).

Among international scholars, Kenneth Waltz probably most forcefully made the case for such an approach. In his seminal work *Theory of International Politics* (1979), he argued that any rigorous and scientific theory should explain laws. Just as the natural world, he viewed the social world as operating according to permanent regularities. According to him, theories should thus have "predictive power" (Waltz 1979: 69) as they fundamentally describe relations that should continuously repeat themselves. With that in mind, Waltz interestingly recognized that his theory should not be expected to successfully explain why state X chooses foreign policy Y at a specific point in time. According to him, this would be akin to ask the theory of gravitation to explain the fall of a leaf, which simply do not operate at the same level of generality (Waltz 1979: 121). As abstract constructs, theories should be able to explain and predict broad trends but not necessarily specific cases. This is a fair point. At the same time, his metaphor of the falling leaf highlights yet another issue of expecting theories to have a predictive capacity: the open nature of both natural and social systems. The falling leaf does not fall to the ground at the time predicted by the theory of gravitation found in a laboratory as other factors affect it (e.g., the wind). The same is true in social systems. Some could argue that this only means that more variables need to be accounted for, but this would actually mean mapping out how different variables interact together and form a system that shapes the outcome as this research precisely argues.

The market power explanation previously reviewed is a more recent example of the adoption of this 'Newtonian' or mechanic view. To understand how global rules are formed, it models a world where powerful actors – again, jurisdictions with large internal markets – can mechanically force others to adopt their policy preferences. The market size of country A thus has the same effect on country B or C. Moreover, the decision of country B to adopt the policy preference of country A is considered to have no impact on the choice of country C. The time at which country B or C decide to adopt their policy is similarly viewed as irrelevant. These reflect two important assumptions embedded in the use of a linear model in the market power explanation: unit homogeneity and independence (Hoffmann and Riley Jr. 2002: 307). The former means that the effect of a variable will be constant in different contexts and over time, and the latter that the dependent variables do not affect each other or the independent variable.

This does not reflect the fact that international governance systems are increasingly "complex governance systems" (Kahler 2016: 827). Amandine Orsini and her colleagues define complex systems as "open systems - that is, [they exchange] information with their environment - that include multiple elements (units) of various types intricately interconnected with one another and operating at various levels" (2019: 3). As opposed to the 'clockwork metaphor', this characterization emphasizes the dynamic and evolutive nature of global governance systems. Rather than being in a steady-state at any point in time, they are always changing according to the interactions between their constitutive elements and their environment. Without labeling it a complex system approach, James Rosenau (1990; 1995; 1997; 2005) was among the first to adopt it in international studies. In his work, he notably coined the term 'fragmegration' to indicate that global governance was in a constant process of becoming more fragmented and integrated all at the same time. He considered that the multiplication of actors, rules, institutions, and decision-making procedures were pushing for more fragmentation, but that their growing number of interactions also made the world more integrated than ever.

While most would probably agree that viewing global governance systems in this light is probably closer to reality than viewing them as mechanical machines, it is generally maintained that it is counterproductive to do so. As a leading proponent of this view, Richard Baldwin bluntly holds "that taking account of everything lets you understand nothing... [simplification] is all in the good cause of allowing a careful and complete examination of the main economic logic that links principal factors " (2016: 177). This is actually a reformulation of Bonini's paradox, sometimes also called the map paradox[10], which states that "as a model grows more realistic, it also becomes just as difficult to understand as the real-world processes it represents" (Dutton and Starbuck 1971: 4). Following this line of thought, many indeed argued that simple explanations should always be preferred to more complicated ones. In their seminal contribution, Gary King, Robert Keohane, and Sidney Verba maintain that "we should attempt to formulate theories that explain as much possible with as little as possible" (1994: 104). These ideas are notably at the core of many rational choice theories that can sometimes even end up promoting simplification over accuracy (Green and Shapiro 1996: 191).

[10]This second denomination is based on the Lewis Caroll's character Mein Herr in his novel *Sylvie and Bruno* who bragged about making a map of the size of the world and yet is forced to admit that it is never used as farmers complaint it would hide the sun. In the end, he says that they now use the world as the map itself and that it works just as well.

A complex system approach importantly does not entirely reject the need for simplification. Despite its name and obvious intent to capture a greater part of the world complexities, a complexity-based approach "simplifies too [and it] has to, because it is a product of the simplifying human mind" (Morçöl 2012: 7). Building a model that would include all aspects of world politics is in effect both impossible and useless. To be fair, it is partly why Rosenau's original work was not taken up by more researchers. His embrace of the complex nature of global governance was often so broad that his readers were often left with the idea that every society was interpenetrated by multiple channels of interactions, but it was not always clear how this, in turn, affected global politics. Here, an important distinction should be drawn between simple and parsimonious explanations. While parsimony is sometimes understood as synonymous to simplicity, it is actually better to see it as describing "explanatory models that are *no more* complicated than they need to be" (Elman and Elman 2003: 236; emphasis added). In that regard, complexity approaches are actually not antinomic to parsimony.

Scholars adopting a complex system approach to study the evolution of legal systems indeed do not attempt to integrate every factors that can be playing a role (Kim 2013; Morin, Pauwelyn and Hollway 2017; Pauwelyn 2014; Puig 2014; Ruhl, Katz and Bommarito 2017). The main insight that they share is that complex systems display properties that can only be understood when looked as a whole. The idea famously encapsulated in the dictum "the whole is different than the sum of its parts"[11] is that "patterns, processes, or properties arise from interactions among the elements of the system" (Orsini et al. 2019: 3). In other words, there are *emergent* properties that can only be understood by considering the interactions that tie a system together. The point is thus not to incorporate the full complexity of the world, but to recognize the dynamic and interactive nature of many social processes.

The new interdependence approach developed by Henry Farrell and Abraham Newman (2014; 2016; 2019*a*) is a prominent and recent example of how such complexity thinking can be applied in international political economy. As indicated by Thomas Oatley, their approach aims to endogenize "the evolution of global rules as a function of the interaction between globalization and domestic politics" (2019: 10). In their work, they more precisely distantiate themselves from the previous interdependence literature (Keohane and Nye 1974; Nye and Keohane 1971), which progressively came to see the

[11]The expression 'the whole is greater (or more) than the sum of its parts' has more often been used, but it actually came from an erroneous translation of the original German expression, which can wrongfully "call up images of metaphysical holism" (Jervis 1997: 12-13).

concept of interdependence as an external shock needing to be managed. Instead, they "begin from the assumption that increasing globalization [...] creates a condition of *rule overlap*" (Farrell and Newman 2019*a*: 27; emphasis in the original). From this specific condition of rule overlap *emerges* opportunity structures – that is, institutions allowing actors to collaborate and advance their interests – that allow both state and non-state actors to promote their preferred rules on the global stage. Based on the access that specific actors have to transnational forums and their preferences toward their domestic institutions, Farrell and Newman differentiate four strategies (Defend and extend; Cross-national layering; Insulate; and Challenge) that public and private actors can adopt.

The present research largely agrees with the new interdependence approach. Just like the latter, it sees globalization as creating a situation of rule overlap that acts as a structure conditioning the adoption of global rules. It also appreciates the focus on how this specific structure changes the strategies of state and non-state actors. The proximity of complexity-based approaches with ecological and organic metaphors can sometimes lead to losing sight of who are the agents and what do they want. In his presentation of a political economy of complex interdependence, Oatley (2019) rightfully mentions that the main scientific metaphor of complexity-based approaches is evolutionary biology. This however leads him to argue that the main unit of analysis is the system itself. Previous complexity scholars have however emphasized that complexity approaches actually want to "comprehend the relations between the whole and the parts" (Morin 2007: 10). It is neither the system nor the actors that are the main unit of analysis, but their interactions.

Having said that, the new interdependence approach does not achieve everything it aims to. First of all, it does not actually explain the *evolution* of global rules as Oatley holds (2019: 10). In reality, what it explains is how various actors choose different strategies to advance or block institutional change in an interdependent world. The explanation of how rules are created or adopted is outside the scope of their research. Moreover, and contrary to what Farrell and Newman originally claim, the context of rule overlap created by the globalization of the world economy is to a large extent taken as exogenous. In effect, the main independent variable is not the structure created by globalization, but an actor's access to transnational forums and institutional preferences. While they maintain that this structure is not fixed or in equilibrium, they do not explain how it evolves or how actors interact with it over time, and it quickly becomes a

contextual factor. Their research also ends up being relatively static[12] as they look at how opportunity structures at one specific point in time are mobilized by specific actors.

By looking specifically into the process of rule formation, this research intends to complement the new interdependence approach by providing a better understanding of how rules are created in the first place. The institutional overlap identified by Farrell and Newman is hereafter considered to be equivalent to a structure enabling and constraining public and private regulators creating and adopting rules. This structure is just as in Farrell and Newman's work not considered to be permanent. It is persistent, as it does not evolve rapidly (Oatley 2019: 3), but it is never in a static equilibrium. In addition, this research will particularly emphasize that while different, the structure and the agents are not distinct from each other (Cudworth and Hobden 2015). They co-constitute themselves. By creating new relations, public and private actors actively shape the structure of interactions that in turn influence their own regulatory decisions. To ensure that this research does not become indeterminate, though, their effect on each other will be analyzed separately and time will constantly be used as a kind of control variable. Hereafter, I follow John Padgett and Walter Powell's view that: "In the short run, actors create relations; in the long run, relations create actors." (2012: 2).

I more specifically argue that the relations or social interactions between public and private actors adopting privacy regulations create two joint processes that influence their regulatory decisions: "exploitation" and "exploration" (Duit and Galaz 2008; March 1991; Morin, Pauwelyn and Hollway 2017). These two processes first enunciated in organizational studies hold that organizations will tend to adapt to their environment by either exploiting "old certainties" or exploring "new possibilities" based on their previous interactions (March 1991: 71). These two concepts closely reflect those of selection and variation traditionally found in evolutionary studies according to which survival is determined by selecting existing practices or slight adaptation to new circumstances (Ashby 1960; Hannan and Freeman 1977, 1989). The terms exploitation and exploration are hereafter preferred as they tend to give a more active role to individual actors. While always influenced by their social interactions and the broader structure that they are part of, they are the ones that decide to 'exploit' preexisting resources or 'explore' new ones. The evolutionary terminology can otherwise introduce a "passive-voice functionalism" that can often come up in system and structural analyses (Kahler 2016: 828).

[12]To be fair, they do discuss how specific opportunity structures come to be, but it's largely a historical account that is external to their main argument.

In the context of this research, these two emergent processes more specifically mean that public and private actors adopting privacy regulations will decide to either use the same rules as the actors with which they have had previous interactions or to use these exchanges to develop new ones. The process of adopting or creating rules is always understood in relational terms. Importantly, this means that the dependent variable for this research is the content or the characteristics of the rules ending up being adopted. This contrasts with the diffusion literature for which the dependent variable was the *mechanism* through which rules were diffused, not their characteristics (Knill 2005). On this point, it is thus closer to the literature on policy convergence (Bennett 1992), which aimed to explain the growing similarity in policies adopted in various jurisdictions. Yet, instead of only focusing on the growing similarity between policies, it also looks at what creates more diversity by also looking at the process of exploration. Both the exploitation and exploration processes will be further developed in chapter 4 before being individually reviewed to explain the evolution of privacy regulation in the transatlantic space over the last 20 years in chapter 5 and 6.

2.6 Conclusion

In this chapter, I argued that the process of rule formation is not merely driven by public actors nor purely national. Up to now, these assumptions were however, to different degrees, at the heart of the dominant explanations looking at this question. This was most specifically seen when reviewing the 'market power explanation' (Drezner 2007), which basically maintains that countries with large internal markets will succeed in unilaterally exporting their regulatory standards when interacting with smaller states, but not when faced with other great economic power. This largely fails to explain why as this research will hereafter highlight data protection rules in the United States and the European Union grew increasingly similar over the years. It moreover does not consider how their respective regulatory frameworks evolved through their interactions. This reflects the theoretical choice behind the market power explanation of significantly minimizing the role of private actors in regulatory debates as well as disregarding the significantly transnational interactions that may connect two jurisdictions.

Discussing the literature on private authority and policy diffusion, I pointed out how previous contributions have already made important headways in taking better account of these variables. Looking first at the literature on private authority, I emphasized

that there is now a flurry of evidence in support of the argument that private actors contribute to the regulation of various issue-areas. In addition to help implement public rules, they often work to devise their own set of rules. Yet, it is not like states had disappeared or were even in retreat (Strange 1996). Even when private actors act in an 'entrepreneurial' fashion to use Jessica Green's (2013*b*) terminology, they will often, if not always, build on public rules and requirements. Such regulatory layering (Bartley 2011) and the interactions between public and private regulators that support it (Eberlein et al. 2014; Gulbrandsen 2014) are in turn key to understand the process of how rules are formed and evolve through time, which is what I will aim to explain in the remainder of this research.

I subsequently reviewed how the literature on policy diffusion had up to now tried to explain the impact of international interactions on national policies. After having discussed the different mechanisms that had been put forward in this literature, I maintained that it did not consider how their interactions were transforming national regulatory systems over time. Diffusion mechanisms were more specifically presented as creating an external pressure at a very specific point in time and in a linear fashion. They were yet not seen as creating a broader structure shaping the process of rule formation in an interactive fashion as it itself evolves. This generally led diffusion studies to focus on explosive moments where policies quickly spread rather than on the incremental changes pushing towards greater convergence. It also means that they did not consider how interactions between actors in different jurisdictions could also become a source of further regulatory change and novelty.

Taking stock of these discussions, I argued in favour of adopting a complex system approach to understand how rules are formed between interdependent jurisdictions. The latter starts from the assumption that interactions between the different parts of a system create patterns that can only be understood when looking at them as a whole. In the context of the regulation of privacy in the United States and studied here, this means that the interactions between public and private actors in the two jurisdictions will influence their respective process of rule formation through two joint processes: 'exploitation' and 'exploration'. The former emphasizes that privacy regulators will generally tend to exploit the data protection rules of those with whom they previously had direct interactions. Meanwhile, the latter highlights that when preexisting rules prove to be insufficient, privacy regulators will explore new ones based on their very same interactions and relation to the broader system. This moves beyond the traditional 'clash

of systems' that is often at the heart of global regulatory debates and posits that the multiple ties and connections between different legal systems are a source of regulatory change, rather than a mere contest for influence.

In the next chapters, I will now use this theoretical framework to explain how data protection rules have evolved in the United States and the European Union since 1995. I start by sketching how these two joint processes have supported two seemingly contradicting trends. As public and private actors have tended to exploit the same data protection rules, I point out that it supported a process of regulatory convergence by which both jurisdictions grew more alike in terms of the rules that they each promote. At the same time, I show that the exploration of new data protection rules limited this very trend and actually contributed to create more divergence over the years. While partly offsetting each other, I importantly emphasize that these dual processes built on each other and were both essential to ensure that the regulation of privacy continued to evolve over time. I also highlight the significant influence that private actors have come to have through these two joint processes. But before going there, the next section will review the origins of the regulation of privacy in both jurisdictions and discuss how they relate to each other. This first essential step will then allow me to justify the use of my complex system approach by detailing how in practice both jurisdictions have been constantly interacting.

Chapter 3

The Transatlantic Privacy System: A Tale of Two Opposites?

Privacy is doomed... Get used to it!

The Economist, 1999

Debates over privacy have long roots in western societies. Despite regular comments to the effect that the United States still lacks a "comprehensive system" (Newman 2008: 32) or an "omnibus law" (Solove and Schwartz 2011: 1062) to regulate privacy like the European Union does, the American legal system has provided privacy protections to its citizens for years. As a matter of fact, the earliest enunciation of a right to privacy came not from Europe, but from the United States. Back in 1890, legal scholar Samuel Warren and later-Supreme Court Justice Louis Brandeis famously published an article arguing that all American citizens had a natural "right to be let alone".

Since this first formulation, the concept of privacy has dramatically evolved both in the United States and Europe. A key element to emphasize is that this evolution obviously did not happen in a vacuum and was "deeply intertwined with the history of technology" (Gasser 2016: 61). As new information technologies were developed, social perceptions of what the private sphere should look like have fluctuated. Calls to the effect that privacy will or should disappear as the one formulated by the well-known journal *The Economist* cited in epigraph to this chapter are not new. At the time of

writing their article in 1890, Warren and Brandeis were precisely aiming to safeguard "the sacred precincts of private and domestic life" which they saw as being endangered by "recent inventions and business methods" (Warren and Brandeis 1890: 195). The development of instantaneous photography and "yellow press"[1] were particularly seen as allowing the distribution of information like never before and thereby raising the risk to "make good the prediction that what is whispered in the closet shall be proclaimed from the house-tops" (Warren and Brandeis 1890: 195).

In recent decades, new information technologies have continuously challenged our conception of privacy. In the 60s, the rising use of computers by governments questioned the ability of individuals to control how their information was used and shared by public agencies (Solove 2004). In the 90s, the commercialization of the Internet then made clear that privacy discussions needed to look more at the role of private companies, which were at the time starting to collect "[p]ersonal information about on-line consumers, such as buying habits and web-surfing preferences" (Haufler 2001: 87). And now, the development of algorithms and new data analytics' methods is pushing this last trend even further. The capacity to recombine multiple types of information coming from multiple sources makes it more and more difficult to distinguish what is or not personal information. One data point that could in the past be considered non-personal or anonymized can in effect be used to "map so-called patterns of life" (Amoore 2014: 109). A recent New York Times investigation specifically showed how the daily collection of hundreds of supposedly anonymized location data points by applications on our cellphones allowed various companies to easily identify us and get an extremely accurate picture of our lives (Valentino-Devries et al. 2018).

As all these innovative technologies were appearing, privacy rules did not stand still. Regulators in both the European Union and the United States worked hard to ensure that their citizens keep a minimal level of protection against intrusions in their private life. Importantly, these regulations should not be viewed as merely responding to the periodic apparition of new 'technological threats'. In many ways, they determine the nature of future technological innovations and the potential problems they will raise by allowing or limiting different types of activity. As one interviewee for this research pointed out, the exponential growth of web-based data collection methods is a direct product of policy choices that were made in the early days of the Internet:

[1] A form of journalism criticized for aiming to be sensationalist rather than factual that came to prominence with the diminution of printing costs.

> They [web-based data collection methods] are based on a policy mistake made years ago. In the 1990s, there was a sense that things needed to be more interactive and with the creation of personal web browsers almost immediately came the concept of cookie. The idea was that the Internet would be free with advertising, but as soon as you advertise you need to know who you are advertising to and thus the need for the development of third-party cookies. (Interview E37, done on May 6th, 2019)

Since the mid-1990s, the way that both the United States and the European Union decided to regulate privacy has significantly diverged. As mentioned, the United States is often criticized for its continuous "lack of [a] comprehensive baseline privacy legislation" at the federal level (O'Connor, Lange and Lange 2015: 22). As of now, it still relies on a number of laws that offer privacy guarantees to specific economic sectors (e.g., finance and health) or vulnerable individuals (e.g., children). In contrast, since the adoption of the Data Directive in 1995, the European Union has had a clear set of rules protecting the privacy of its citizens with regards to data collection and processing by both public and private actors[2].

Because of this, the United States is generally seen as lagging behind Europe in terms of privacy regulation. It is assumed that the United States will one day have to adopt a European-like comprehensive legislation. Instead of focusing on the questions of which regulatory system is normatively superior to the other, this research again aims to understand how their interactions have affected the development of data protection rules in both jurisdictions. Adopting the view that the European Union and the United States represent two privacy systems fundamentally opposed to each other, previous contributions have tended to question the capacity of one to export its regulatory model to the other (Bessette and Haufler 2001; Long and Quek 2002; Drezner 2007; Newman and Posner 2015). While disagreeing on the success of this effort, their analytical choice to describe them as two ideal-types of privacy regulation made them largely fail to see how both jurisdictions have continuously influenced each other.

In this chapter, I start to depart from these 'clash of systems' arguments and highlight that both the European and American privacy models are based on a common liberal paradigm. While their conceptions of privacy do differ, they basically agree that what they aim to protect is an individual's capacity to control the use of his or her personal information. This importantly means that at their heart they are not "two fundamentally incompatible [privacy] frameworks" (Chander, Kaminski and McGeveran

[2]Before 1995, several European countries had already adopted this comprehensive approach as it is well described by Newman (2008).

2020: 24) and that they can exchange and influence each other as they notably share a common background and language to do so. This is an essential condition for the complex system approach that I introduced in chapter 2 and that will be further developed in chapter 4 onward. Indeed, if there was absolutely no point of agreement between them they would more closely approximate the two rivals as often depicted in the literature. In the next section, I begin by introducing the liberal paradigm and basic concept of privacy followed by regulators in the United States and the European Union. From there, I review how the American came to be seen as promoting a market-based approach and the European Union a rights-based approach. I then show how in practice neither reflect these ideal-types and actually have a lot in common. I conclude by highlighting how this offered important opportunities for interactions among the transatlantic partners.

3.1 Privacy as a Concept: From a Negative to a Positive Right

What information should be part of the public or private sphere is a question that has long been debated. Even before the publication of Warren and Brandeis' paper on a "right to be let alone", early liberal thinkers like John Stuart Mill reflected on the "public\private dichotomy to determine when society should regulate individual conduct" (Solove and Schwartz 2011: 41). The fact is that at its heart the concept of privacy intersects with our basic understanding of how individuals should live in society. Thinking about privacy forces us to reflect on the very value we attribute to individuality. Different societies unsurprisingly came up with markedly different answers to this question. In Asia, for one, the relation between the individual and the collective has often been understood differently than in the Western world (Ess 2005). As Yao-Huai points out, the concept of private information was long associated in China with a "shameful secret" (2005: 8). In Thailand, the concept of privacy was similarly often seen in a negative light and a form of "possessive individualism" (Privacy International 2012: 4; see also Kitiyadisai 2005).

Importantly, this does not mean that privacy is only a Western construct. A distinction between public and private sphere of activities generally appears to have been part of most societies (Moore 1984). In many Asian countries, the concept of "saving face" (i.e., respecting one's honor) is for example historically associated with a duty of not interfering with the private or familial affairs of others (Kitiyadisai 2005).

The main difference is actually where the line has tended to be drawn and, in that respect, the United States and the European Union share a strong philosophical root[3]. Although often presented as opposites, they both follow a liberal privacy paradigm, which reifies human individuality. In effect, both start from the assumption that society is composed of "relatively autonomous *individuals*", which are generally assumed to be able to determine their interests (Bennett and Raab 2006: 4). Society is seen as nothing more than the sum of the individuals it represents. Following this atomistic view of the world, a clear distinction is drawn "between the individual and other individuals, and between the individual and the state" (Bennett and Raab 2006: 4). The respect of the ensuing boundary is originally what privacy is about in both Europe and the United States.

Before going any further, an important clarification is needed. In privacy debates across the Atlantic, there is often confusion between what is privacy and data protection. To make things more blurry, it is common in the United States to talk of "information privacy law" for what in Europe is generally called "data protection law"[4] (Schwartz and Peifer 2017: 122). As a general legal concept, privacy refers to the basic human right internationally recognized in the Universal Declaration of Human Rights of 1948 and the International Covenant on Civil and Political Rights of 1966 (Bauman et al. 2014: 132). In Europe, the right to privacy is furthermore enshrined in the European Convention on Human Rights of 1950 and the Charter of Fundamental Rights of the European Union of 2000 (Bellanova and De Hert 2009). While the American constitution does not explicitly include the respect of privacy as a fundamental right, the Supreme Court of the United States has in the past argued that such a right was present in its "penumbras" or "zones of shades" (Solove and Schwartz 2011: 35). The Fourth Amendment was most notably recognized by the Supreme court as primarily aiming to protect the right to privacy of American citizens (Bellanova and De Hert 2009: 70).

Meanwhile, "information privacy" or "data protection" refers to the body of law that deals specifically with how personal information[5] should be used and shared to respect basic privacy principles. In judicial terms, it is the *lex specialis* that deals with the

[3]A full discussion of the meaning and impact of the cultural differences over privacy is outside the scope of this research, but it should be noted that privacy cultures are not static and that important changes have been ongoing in many countries around the world for a long time (Bygrave 2004; Ess 2005).

[4]Data protection is actually derived from the German expression Datenschutz (Bennett and Raab 2006: 8).

[5]This research considers the expressions "personal information" and "personal data" to be synonymous and will use them interchangeably.

information that our activities generate on a daily basis. How that specific body of rules has evolved through the interactions between the European and American jurisdictions is again the main question of this research. For now, though, my aim in this chapter is to examine to what extent the regulatory approaches adopted in the European Union and the United States actually differ from each other in light of their respective privacy conceptions.

According to their joint liberal viewpoint, privacy guarantees are supposed to ensure that free and rational individuals have sufficient personal space to realize themselves. It should moreover be a space in which other individuals or the state refrain from intruding. In John Stuart Mill's work, the dichotomy between the public and private sphere was specifically used to determine when an individual's activities should be subject to public regulation or not. The "right to be let alone" enunciated by Warren and Brandeis follows the same logic. In its essence, it is a negative obligation that requires individuals to abstain from interfering with the private space of other individuals. Governments are similarly expected not to take any actions that would violate this individual right to privacy. In the end, "the protection of society must come mainly through a recognition of the rights of the individual" (Warren and Brandeis 1890: 219-20).

Over the years, the right to privacy however became understood in more positive terms. As more and more information could be collected, analyzed, and shared, it became difficult to sustain the illusion that individuals could easily maintain a strict boundary between their public and private life. The rise of computers and the growth of personal record-keeping activities by governments in the 50s and 60s particularly challenged this early view. Relatively vague definitions of privacy emphasizing the obligation of *not* intruding in anyone's private life were quickly becoming pointless (Rule 2009: 23). Alan Westin is generally recognized for the modern redefinition of the concept of privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (1967: 7). From there, privacy has increasingly been seen not as the capacity to limit access to ourselves but to decide how personal information gathered from us is used. As Charles Fried wrote one year after Westin:

> At first approximation, privacy seems to be related to secrecy, to limiting the knowledge of others about oneself. This notion must be refined. It is not true, for instance, that the less that is know about us the more privacy we have. Privacy is not simply an absence of information about what is in the minds of others; rather it is the

> control we have over information about ourselves. (Cited in Solove and Schwartz 2011: 47)

This "privacy as control" approach importantly played a crucial role in the formulation of the first clear set of privacy rules in the 70s. Leading the way, the United States Department of Health, Education and Welfare adopted the first official report indicating that individuals should have the capacity to influence how information about them is used and disclosed. While not arguing that they should have complete control over their personal information, the report maintained that "a record containing information about an individual in identifiable form must [...] be governed by procedures that afford the individual a *right to participate* in deciding what the content of the record will be and what disclosure and use will be made of [it]" (U.S. Department of Health Education and Welfare 1973: 41; emphasis added). To operationalize this, the report went on articulating what would become known as the Fair Information Practices. The latter was a set of five basic principles that governments and private actors were expected to follow in order to guarantee the privacy of individuals:

> 1. There must be no personal data record-keeping systems whose very existence is secret.
> 2. There must be a way for a person to find out what information about the person is in a record and how it is used.
> 3. There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent.
> 4. There must be a way for a person to correct or amend a record of identifiable information about the person.
> 5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data. (U.S. Department of Health Education and Welfare 1973: 41)

Together, these five principles are still today at the heart of the regulatory approaches to privacy in both the United States and Europe. In 1974, the Privacy Act adopted in the United States largely drew on them to determine how public agencies should guarantee the privacy of American citizens in their dealings with them (Rule 2009: 24). The first wave of modern privacy laws adopted by European states, like Sweden, was also influenced by these very principles (Newman 2008: 25). These even ended up being the core component of the OECD Guidelines on the Protection of Privacy and

Transborder Flows of Personal Data adopted in 1980, which are still today the closest thing we have to a global agreement on the regulation of privacy (Solove and Schwartz 2011: 1062). This relative consensus however should not be overplayed. The OECD guidelines represent a lowest common denominator more than anything else. Since their adoption, "the scope of enforcement and implementation mechanisms has [moreover] varied across countries, especially with regard to the private sector" (Newman 2008: 26). As Europe took a more and more active role in the regulation of the use of personal information by private actors, the United States still maintains a relatively hands-off policy towards the private sector. Before looking into how the regulatory approaches in these two areas have evolved since 1995, the next section will discuss how their respective conceptions of privacy have moved apart while both following the same liberal paradigm.

3.2 The American and European Privacy Divide

Even though the United States and the European Union share a common liberal view of privacy, whereby claims to privacy are made by relatively autonomous individuals, they both significantly diverge in the degree to which they think governments should actively oversee the use of personal information in the marketplace. The difference is such that prominent privacy scholars stated "that we must acknowledge... that there are, on the two sides of the Atlantic, two different cultures of privacy" (Solove and Schwartz 2011: 1066). Others have talked of the existence of a literal chiasmus between Europe and the United States (Bellanova and De Hert 2009) and that both have merely been able to "agree to disagree" (Bessette and Haufler 2001: 88).

This 'cultural clash' over the protection of privacy rests primarily on their opposition over "an essentially utilitarian logic of *efficiency* and a Kantian logic of *rights*" (Rule 2009: 27; see also Kobrin 2004). According to the former, the use of personal information and more broadly surveillance by any entities should be evaluated against the benefits they provide. It is "the total utility or pleasure generated by [their] use" (Rule 2009: 11), which matters rather than the individual intrusion. The use of personal data by credit agencies, health providers or even marketers can in other words be justified if it provides individuals or our societies with sufficient benefits. Meanwhile, the rights logic embraces the Kantian concept of 'categorical imperatives' and the idea that each individual has fundamental rights that need to be respected in all circumstances. According to this approach, no personal or group gains could justify any form of invasion of privacy. At a

minimum, individuals have a fundamental right to decide how information about them can be used by others.

In the United States, the utilitarian logic has especially grown in importance since the 70s and the development of the influential law and economics movement. Emanating from the Chicago School, this legal scholarship promoted the use of free-market views to analyze and change various fields of law[6]. With regards to privacy, legal scholars adopting this specific economic analysis of law centrally argued that it is just one of two economic goods existing in the 'information market'. For them, the natural desire of individuals to conceal information about themselves only exists next to the equally natural interest of other individuals for "casual prying [...] motivated, to a greater extent than we may realize, by rational considerations of self-interest" (Posner 2009: 394).

This view fundamentally rests on the adoption of a pure rational choice model, which assumes that access to as complete information as possible is essential for any democracy and economy to prosper. Citing the former member of the Federal Reserve Board Governor, Edward Gramlich, Fred Cate maintains that the more information is available "the more accurately and efficiently will the economy meet [our] needs and preferences" (2000: 882). By contrast, the more information is hidden, the more risks there are of miscalculations or mistakes. Seen in this light, demands for privacy can obviously even be seen negatively as they might produce sub-optimal outcomes. This is nowhere near as evident as in Posner's equation of privacy to an individual's desire for manipulation and misrepresentation:

> It is no answer that such individuals have "the right to be let alone." Very few people want to be let alone. They want to manipulate the world around them by selective disclosure of facts about themselves. Why should others be asked to take their self-serving claims at face value and be prevented from obtaining the information necessary to verify or disprove these claims? (Posner 1978: 400)

For him and other proponents of this economic analysis of law, any regulations should "treat [privacy] preferences as a matter of individual taste, entitled to no more (and often much less) weight than preferences for black shoes over brown or red wine over white" (Cohen 2000: 1423). In line with their utilitarian logic, they do not consider

[6]Apart from privacy, antitrust is another field of law where the influence of the law and economics movement has been particularly significant. Following the publication of *The Antitrust Paradox* (1978) by Robert Borke, courts have progressively adopted a 'consumer welfare standard' to evaluate merger and acquisitions. Based on a neoliberal theory of price, this specific standard is now criticized for having allowed the rise of a new Gilded Age (Khan 2017; Wu 2018).

privacy to have any intrinsic value. One's preference for keeping information private should in practice always be evaluated against another for having access to it. Individual control over information and, by extension, privacy rights should in the end be allocated to the individual or company that values it the most (Solove 2004: 78). Following Ronald Coase's theory of transaction costs, the question of privacy thus becomes one of ownership allocation. Governments should merely set basic property rights and then let the 'information marketplace' *efficiently* ensure that the appropriate level is achieved by letting each individual freely decide which information they want to share based on their own cost-benefit analysis. Information readily shared by individuals should not be seen as private. Meanwhile, information collected by a company and seen as valuable when kept secret should stay private.

As opposed to this market-based approach to privacy that has come to define the American privacy regulatory framework, Europe has increasingly adopted a rights-based approach (Schwartz and Peifer 2017; Simitis 1995). While also rooted in a liberal paradigm, it starts from the very different assumption that privacy is not a matter of preference but "of fair and just treatment of individuals" (Cohen 2000: 1423). It is a fundamental right that has value for its own sake in a free and equal society. The respect for privacy is nothing less than a question of human dignity and democracy, not of managing an 'information market'. As such, the law should primarily aim to set basic conditions under which an individual's information may be used, rather than establish basic property rights.

Importantly, this does not mean that the concept of ownership is entirely alien to a right-based approach. To the discontent of many privacy advocates, property rhetoric often makes its way in public debates over privacy. The fact is that both the notions of private and control that are central to any privacy discussions adopting the liberal paradigm tend to create questions of data ownership. If any information is to be kept out of the public's eye and under the control of someone, it should be someone's private property the usual thinking goes. As Cohen interestingly points out, linguistically speaking the word private notably means not 'common' and in other words not owned by anyone else (Cohen 2000: 1379). The lack of non-ownership words to describe things over which anyone has private control is precisely why property talk regularly pervades rights-based discourse of privacy.

Talking of ownership according to a fundamental rights logic is however significantly different than according to an utilitarian one. First and foremost, it rejects the

commodification of personal information that is generally hidden behind ownership talks. Property is in effect not seen as being over a tradable asset, but a fundamental element of an individual's personhood (Radin 1982). As such, the aim of talking about property rights is not to solve market efficiency or to allow for personal information to be traded, but to ensure human dignity. The allocation of rights is accordingly not based on the instrumental value granted by an individual or a company to a specific piece of information. It is rather attributed following a natural rights logic that considers that all individuals have the right to own their personal information based on their fundamental humanity (Solove 2004: 77). With that in mind, concepts of ownership are rarely promoted by proponents of a rights-based approach to privacy. Doing so is generally seen as a slippery slope towards the very commodification that it notably aims to escape.

Having now defined and contrasted the utilitarian and Kantian logic respectively preferred in the United States and Europe, the next two sections will present in more detail how they are each reflected in the regulatory approaches followed by both jurisdictions since 1995. While doing so, it will retrace the main regulatory moments and actors that shaped their evolution. This will then be used to emphasize in the last section that in practice neither fully embrace the logic attributed to them. In effect, both recognize to some extent that "people have some special rights over disposition of 'their' information" (Rule 2009: 11). They also both give an important role to private actors and expect the marketplace to contribute to the regulation of privacy.

3.3 The United States and the Marketplace for Privacy since 1995

Contrary to what is sometimes portrayed in public debates, the American legal system does offer privacy protections to its citizens. While they might be considered insufficient (O'Connor, Lange and Lange 2015; Reidenberg 1992; Schwartz and Peifer 2017; Zuboff 2019), any analysis of the American regulatory approach towards privacy needs to start by recognizing their existence. As pointed out above, the American Constitution has on multiple occasions been considered to guard American citizens against various intrusions in their private life by state agencies. Although no part of the Constitution specifically mentions privacy[7], various amendments that form the Bill of Rights have in effect been

[7]Some federal states, like Alaska and Florida, do specifically provide a right to privacy.

understood by the US Supreme Court as providing Americans with a right to privacy. In *Katz v. United States* (1967), the US Supreme Court for example established that all Americans had a right to a reasonable expectation of privacy based on the Fourth Amendment that prohibits unreasonable seizures and searches by public authorities. In *Roe v. Wade* (1973), the Supreme Court also famously concluded that a woman had a right to *privately* decide to terminate or not her pregnancy with her doctors based on the Fourteenth Amendment guaranteeing due process. Other Amendments that have over time been construed to give privacy guarantees to American citizens include the First that protects the right of association and the Fifth that protects against self-incrimination (Solove 2004: 62-3).

Next to these constitutional rights, the United States federal government also adopted a number of statutory laws to govern the use of personal data. The Privacy Act of 1974 chiefly ensures that all federal agencies apply the previously discussed Fair Information Practices when dealing with the personal information of American citizens. Accordingly, individuals can access their personal information held by the federal government and request changes to it if necessary. This however does not cover the collection and use of personal data by private entities. The latter indeed falls outside the purview of this Act that only applies to federal agencies and leave private businesses to decide for themselves what rules they should follow when dealing with personal information. Various laws were passed since then to regulate their activities, but these significantly remained limited to specific economic sectors or groups of individuals. Following the disclosure by journalists of the list of movies rented by the Supreme Court Justice nominee Robert Borke, Congress for example adopted the Video Privacy Protection Act in 1988 to prohibit video renting companies to share information about what movies consumers rent or buy (Solove 2004: 69).

Since 1995, sectoral laws were more specifically enacted to further limit the activities of private companies dealing with various types of personal data, including health data, children data, financial data, marketing information, and credit scores. All these laws and their respective years of adoption are summarized in table 3.1 below. Laws, like the PATRIOT Act of 2001 and the CLOUD Act of 2018, that gave more surveillance power to police forces were knowingly excluded as they were considered to primarily create security exceptions rather than creating general privacy rules[8]. As can be seen, no

[8]The links between privacy and surveillance should not be understated. As security exceptions are created, they can undermine privacy protections that citizens would have normally been entitled to. The evolution of surveillance in both the United States and the European Union has, in turn, had significant

laws were adopted after 2003. Amendments did periodically modify part of the preexisting rules, but no new major legislative acts were passed. As such, the use of personal data in many economic sectors remains nowadays lightly regulated by public authorities and industry self-regulation is expected to fill in the gaps.

Table 3.1 Main privacy laws adopted in the United States since 1995

1996	Health Insurance Portability and Accountability Act (HIPAA)
1998	Children's Online Privacy Protection Act (COPPA)
1999	The Gramm-Leach-Bliley Act (GLBA)
2003	Controlling the Assault of Non-Solicited Pornography And Marketing Act (CAN-SPAM)
2003	Fair and Accurate Credit Transactions Act (FACTA)

This combination of laws providing relatively strong privacy protections for the public sector, while "granting private-sector actors wide latitude in their use of personal information" forms the heart of the American limited privacy regime (Newman 2008: 30). Rather than having one comprehensive regulation that covers both the public and private sectors, the United States in effect relies on a patchwork of laws and private rules to govern the use of personal data. This has importantly not meant that American citizens have enjoyed no privacy protections or only those in the few sectoral laws just mentioned. Starting in the mid-1990s, various types of industry self-regulations have been adopted and extended the use of the Fair Information Practices to various economic sectors.

Table 3.2 adds to the previous list of privacy laws all industry self-regulations dealing with privacy adopted in the United States since 1995. These were importantly identified based on an extensive review of preexisting research (Cavoukian and Crompton 2000; European Commission 2001*a*, 2012*b*; European Parliament 2012; Rodrigues and Papkonstantinou 2018; Trzaskowski 2006) and only include documents that set out how private companies should collect and use personal data. These do not include policy documents setting out technical standards, like the Payment Card Industry Data Security Standard, Mozilla's 'Do Not Track' open standard or Internet protocols (cf. DeNardis 2009, 2014; Harcourt, Christou and Simpson 2020). Self-regulations adopted by transna-

consequences for their privacy regimes (see e.g., Chapter 2 in Farrell & Newman, 2019*a*). This is however outside the scope of this research, which aims to understand how privacy rules have evolved in both the United States and Europe, and not how their application has been affected by surveillance imperatives. To put it somewhat differently, surveillance laws are not taken to be constitutive elements of the privacy regulatory framework although they might affect it.

tional private actors, like the International Chamber of Commerce or the Global Business Dialogue on Electronic Commerce, were moreover excluded to focus on the regulations that primarily aimed to oversee the American market[9].

Table 3.2 Main industry self-regulations dealing with privacy adopted in the United States since 1995

1997	Individual Reference Services Group's Principles
1997	American Institute of Certified Public Accountants' Webstrust Program
1997	Better Business Bureau's BBBOnline Privacy Program
1997	Direct Marketing Association's Ethical Business Practice
1997	Internet Alliance's Code of Conduct
1997	TrustArc (then-named TRUSTe)
1999	Online Privacy Alliance's Guidelines
2000	Electronic Commerce and Consumer Protection Group's Guidelines
2000	Entertainment Software Rating Board's Privacy Online Principles
2000	Network Advertising's Code of Conduct
2000	PricewaterhouseCoopers' BetterWeb Standards
2001	SquareTrade's Seal Program
2004	Entertainment Retailer Association's Code of Conduct
2009	Digital Advertising Alliance's Behavioral Advertising Principles
2011	Interactive Advertising Bureau's Code of Conduct
2014	Verasafe's Privacy Program

As it can easily be seen, the number of privacy regulations significantly increase as soon as we consider the ones adopted by private actors. A couple of patterns can moreover be observed by looking at table 3.2. First, industry self-regulations never stopped to be created. While their rate of adoption clearly slowed over time, new codes of conduct or certification programs were continuously adopted. These are in addition to the revisions made to early ones and are not listed in table 3.2. Just like national laws, industry self-regulations will in effect be amended or adapted over the course of their life. As such, the American regulatory approach towards privacy appears more dynamic when considering industry self-regulation rather than only statutory laws. Second, most of these private regulations were however created at the turn of the millennium just like almost all statutory laws (see table 3.1 above). This reflects the heightened interest that privacy came to take with the commercialization of the Internet (Rothchild 2016) and the

[9]Over the years some privacy programs, like TrustArc and Verasafe, have developed services for other markets. They were however kept in the table as their most important source of activity remains in the United States.

first clash over this issue between the European Union and the United States following the adoption of the European Directive (Farrell 2003; Kobrin 2004). This shows that as public scrutiny was lower in the mid-2000s, the incentive for private actors to create new regulations was also lower. Here, it must be noted that the demand for industry self-regulation is not infinite and it is quite normal that as time passes fewer are being created. Even more so as industry self-regulations adopted in the early 2000s were also revised and updated as just indicated. Having said that, it is still noteworthy that new regulations only appear as the public oversight by the FTC began to become stronger after 2008 and when online advertising was again on the rise (Gellman and Dixon 2016).

One recurring argument for embracing the use of industry self-regulations is significantly their supposed dynamism. For them, the complex and quickly evolving nature of new data technologies can simply best be managed by letting private businesses regulate themselves.v Similar thoughts were held by interviewees for this research who were supportive of self-regulation:

> [T]he problem with legislation is that it takes a long time. It is not enough in a world of fast-paced technological change. [...] In a fast innovative area, legislation cannot keep up with the speed of technological development. [...] If it's doing the job you should let it go and not regulate it. (Interview E25, done on March 15th, 2019)

> Traditionally speaking, states cannot easily manage cross-border regulatory issues such as data which is fundamentally borderless. (Interview E27, done on April 4th, 2019)

> Given the complexity of the digital economy and the ubiquitousness of data, [data protection authorities] simply do not have the means to do this alone. (Interview E39, done on May 6th, 2019)

Such arguments should however be carefully considered and certainly not taken at face value. While the regulation of new technologies can indeed present a challenge to public regulators (Tene and Hughes 2014: 442), it is well exaggerated to maintain that they are helpless in front of them. It is actually worth remembering that many so-called disruptive innovations like computers or the Internet have been developed by the public sector or in partnership with it (Mazzucato 2011; Spar 1999; Weiss 2014). Far from being disconnected, public officials thus often have a good understanding of the technological changes taking place at various points in time. Moreover, the adaptation capacity and flexibility of private forms of regulations as compared to public ones is often assumed more than empirically verified. As indicated above, the adoption of new

regulations was rarely dissociated of the level of public scrutiny and, in 2010, the Federal Trade Commission (FTC) even remarked that "industry efforts to address privacy through self-regulation have been *too slow*, and up to now *have failed* to provide adequate and meaningful protection" (2010: iii; emphasis added). As it will be discussed at greater length in chapter 6, the exploration of new rules by the private sector has indeed not been as significant as it might have been hoped for.

More than anything else, the adoption of industry self-regulation reflects the utilitarian logic and more broadly (neo)liberal agenda that came to prominence in the United States and questioned the utility and even capacity of states to govern various issue-areas, including privacy. In its analysis of the evolution of the European and American privacy regimes, Newman argued that representatives of the private sector were able to use institutional features, and more precisely the number of veto points, existing in the American political system to block the adoption of comprehensive privacy rules for the private sector and support the use of industry self-regulation (Newman 2008: 57-60). At the same time, he highlights that this went against the previously well-established practice of creating "independent agencies to overcome the problems posed by the growing complexity of governing a modern society" and reflected the growing unwillingness of American public authorities to delegate tasks (Newman 2008: 72-3). More accurately, though, it did not end delegation practices but merely replace the entity to which tasks were delegated. Private actors instead of public ones were given the role to police the marketplace. This significant change should be understood in light of the broader dismissal of the role of public regulators happening in the 70s and that specifically flourished with the rise of the law and economics movement previously discussed. Since then, the delegation of regulatory tasks to the private sector has been a constant feature of the American regulatory approach to privacy. The next section will now present in greater detail the European approach.

3.4 The European Union and Privacy Rights since 1995

In stark contrast to the United States, privacy is clearly recognized as a fundamental human right in Europe since the adoption of the *European Convention of Human Rights* in 1950 (Bellanova and De Hert 2009: 65). Without having to make an extensive reading of any articles or looking at the "penumbras" or "zones of shades", its article 8 conspicuously states that "[e]veryone has the right to respect for his private and family life,

his home and his correspondence". Following on this broad recognition, the *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data* (Convention 108) adopted by the Council of Europe was the first internationally binding instrument to propose clear privacy rules for both the public and private sectors. As opposed to the regulatory approach being simultaneously developed in the United States, the goal of this early European regulatory framework was to "approach all privacy issues in a centralized and enforceable manner" (Bessette and Haufler 2001: 78).

In practice, though, the regulation of privacy remained highly decentralized and not all European countries adopted rules for the use of personal data by the private sector. While France and Germany adopted privacy laws covering the private sector back in the 70s, countries like Belgium, Greece, Italy, and Portugal had not ratified the 1981 convention and had no national privacy regulations up until the mid-1990s. Spain that had ratified the convention back in 1983 also did not even adopt a privacy law covering the use of personal data by the private sector before 1999 (Newman 2008: 84). Thus, many European countries did not have an approach so different from the United States just a few years ago.

This all changed in 1995 with the passage of the *Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data.* Following years of negotiation, the adoption of this European Directive promoted the adoption of a comprehensive privacy regime in Europe for the first time. In effect, all Member states of the European Union had to adopt one set of "rules for the public and private sectors, enforced by independent regulatory agencies" (Newman 2008: 43). As a directive[10], each Member states had some leeway in how they wanted to set up their own regulatory framework, but they all had to achieve this broad objective by 1998. While not all respected this deadline, all came to adopt a comprehensive law in the early 2000s at the latest and created data protection authorities to oversee them.

Since then, the European Union has continuously adopted new directives or regulations to complement and strengthen its privacy regime as shown in table 3.3. In 2001, it first adopted a regulation covering the use of personal data by European Institutions (i.e., European Commission, European Parliament, etc.) and, in 2002, it added the E-Privacy Directive that provided rules for the use of personal data in electronic communications.

[10]As opposed to regulations, directives are not directly enforceable. Member states must adopt an implementing legislation to give it legal effect. While they are required to do so, they enjoy some flexibility in this process as indicated in article 288 of the *Treaty on the Functioning of the European Union.*

Table 3.3 Main privacy laws adopted in the European Union since 1995

1995	Data Protection Directive
2001	Data Protection Regulation for EU Institutions (45/2001)
2002	E-Privacy Directive
2006	Data Retention Directive
2009	Amended E-Privacy Directive
2016	General Data Protection Regulation (GDPR)
2018	Revised Data Protection Regulation for EU Institutions (2018/1725)

The latter was also amended twice with the adoption of the Data Retention Directive in 2006 and the revised E-Privacy Directive in 2009. Both in turn helped ensure that the rules for the use of personal data were keeping up with the development of new electronic services.

While important, these amendments and revised laws however did not fundamentally change the European privacy regime as the General Data Protection Regulation (GDPR) did when adopted in 2016. In addition to extensively update the European rulebook, the move from a directive to a regulation broadly means that data protection rules negotiated at the European level are now directly enforceable in all Member States of the European Union. This specifically ensures that the same set of rules should now be applied throughout Europe. Although the Directive succeeded in promoting a comprehensive approach towards privacy, it had in effect failed to fully harmonize data protection rules. Significant discrepancies remained between the laws adopted in each European country and limited the development of the European digital single market.

The GDPR has moreover raised the bar in terms of sanctions that can be applied for non-compliance. In the future, private companies violating its rules may receive administrative fines of up to 20 million euros or 4% of their annual worldwide turnover, whichever is greater (Art. 83). This drastically contrasts with the Data Directive, which did not even provide specific rules for the size of the administrative fines that data protection authorities could hand out and that often ended up to be quite small. In 2018, Facebook was for example fined 500,000 pounds by the Information Commissioner of the United Kingdom for the Cambridge Analytica scandal, which was the maximum it could levy based on the British law implementing the Data Directive. If the GDPR had been in force[11] at the time, Facebook could have instead faced a fine of up to 1,27 billion

[11]The GDPR came into force on May 25th, 2018.

pounds or 4% of its 2017 worldwide turnover (Waterson 2018). Since the entry into force of the GDPR, various data protection authorities in Europe have in effect used their new powers and handed out larger fines to private companies. In 2019, the French data protection authority gave a fine of 50 million euros to Google for not having properly informed its users about its data practices (Satariano 2019). While still being far from the maximum fine it could have handed out, this was the largest ever applied for privacy violations in Europe.

This reliance on comprehensive rules and independent regulatory agencies to regulate the use of personal data since 1995 is in line with the rights-based approach preferred in Europe. As a fundamental right, privacy is not seen as something that should be mainly regulated by the private sector. Limits should be set and enforced by public authorities to ensure that business interests do not take precedence at any point in time. Nor should individuals have to accept fewer privacy protections for better services. The same rules should be applied to all and no one should be left to decide how much value they want to attribute to their own information. This link between this privacy conception and European regulatory approach was explicitly recognized in the 1994 report on *Europe and the global information society* drafted under the direction of then-Commissioner for the internal market Martin Bangemann. While generally supportive of the use of market mechanisms by the European Union to regulate the digital economy to remain competitive with the United States (Franda 2001: 84), it emphasized the leadership role of Europe "in the protection the fundamental rights of the individual with regard to personal data processing" (European Commission 1994: 22) and urged Member states to quickly adopt the comprehensive approach promoted by the Data Directive. Interviewees for this research similarly pointed out the link between the nature of privacy as a fundamental right and today's European regulatory approach towards it:

> [Private codes] can be used to demonstrate compliance, but they cannot replace the law. [...] There needs to be legal rules backing private codes. [...] Privacy is a fundamental right. (Interview E18, done on February 27th, 2019)

> Self-regulation alone doesn't do the trick. [...] The protection of fundamental rights, cannot be left to private operators. (Interview E20, done on March 3rd 2019)

This understanding of privacy as a fundamental right is at the very heart of the opposition between the European and American privacy regimes. Although rules promoted in both jurisdictions might not always be that different as chapter 5 will show,

their different conceptions of privacy makes them disagree on the role that public and private actors should play in its regulation. While the United States federal government champions the role of private actors, the European Commission supports the adoption of comprehensive public rules. Such disagreement is evidently hard to bridge and clearly limit possibilities to develop a harmonized approach. At the same time, it is wrong to present both regulatory frameworks as having no points in common and existing independently from the other. As the next and final section will highlight, they are in practice both closer to hybrid forms of regulation than the two ideal-types just described and have had opportunities to influence each other over the years.

3.5 Transatlantic Privacy Regulation: Between Public and Private Rule-Making

Despite their broad differences, it should be reemphasized that both the European and American privacy regimes start from the same liberal root that draws a clear distinction between the individual and the collective. Based on their belief that society is made up of relatively autonomous and rational individuals, they both agree on the basic idea that all individuals need to have some form of control over their personal information to actively participate in society. Being able to withhold details about oneself is simply put viewed as a condition for the development of one's own opinion and personality, which forms the heart of what being a distinct person means from a broad liberal standpoint.

This joint adoption of a liberal privacy paradigm is important because it allowed both jurisdictions to have similar concepts to talk about privacy. Concepts like consent, transparency, accessibility, security, and limitations have formed the heart of the American and European privacy regimes since the first adoption of the Fair Information Practices in the United States in the 70s. While disagreeing on their exact meaning and who should primarily be in charge to oversee their application, these shared concepts provide a common platform to discuss privacy regulations. This does not ensure a common understanding as the use of a similar language combined with different basic privacy conceptions creates high risks of confusion. This can regularly be observed as officials from both jurisdictions often seem to talk past each other (Tene and Hughes 2014: 442). Each side tending to oversimplify the legal framework proposed by the other to promote

its own. Nevertheless, these shared concepts serve as a basis from which they can and have exchanged over the years.

Interactions between the two jurisdictions' regulatory frameworks were also eased by the fact that none of them is a pure reflection of the ideal-types described in the last two sections. State intervention is neither fully rejected in the United States nor the only option considered in Europe. Moving away from their broad characterization as "limited" or "comprehensive" systems (Newman 2008: 26-30), each regulatory frameworks in practice rely on a mix of rules established and enforced by public and private actors to deal with the use of personal information by private businesses. As such, they follow more hybrid or co-regulation approaches (Hirsch 2011) that have importantly been moving closer to each other through their joint influence.

In the United States, industry self-regulation rarely occurs without any public intervention. Generally speaking, private companies and associations are relatively free to determine what rules they want to create for themselves or their members. The American federal government has a more limited influence at the drafting stage of industry self-regulations. It is nonetheless really active in enforcing them once created. As indicated above, one characteristic of the American limited system is that no independent regulatory agency was created to deal specifically with the use of personal data. However, the FTC progressively came to play that role through the application of its prohibition of unfair or deceptive practices, which allowed it to prosecute various private companies for cases of non-compliance with the privacy rules that they had maintained to be following. Discussing the American regulatory approach to privacy, one interviewee highlighted this particular nature of its self-regulation system:

> There is still a misunderstanding in Europe about how the US privacy system works. I would say that it is enforceable self-certification, rather than self-regulation. [...] At the same time, you need that back stop enforcement that the FTC provides. There must be penalties so that folks stay in line. (Interview E28, done on April 19th, 2019)

This enforcement role is far from minor. As another interviewee noted, the FTC "often gives much bigger fines than those the EU gave under the 95 Directive and even what is discussed under the GDPR" (Interview E15, done on February 19th, 2019). In fact, following the Cambridge Analytica scandal, the FTC imposed a $5 billion fine on Facebook (Federal Trade Commission 2019), which is 7750 times larger than the fine that Facebook received for the same scandal in the United Kingdom. To be fair, the fine that

it received was again based on the Data Directive, not the GDPR. Yet, the highest fine it could have levied against Facebook on the GDPR was still almost 5 times smaller as previously noted (i.e., £1,27 billion).

In addition to this enforcement role, the American federal government also contributes to the development of industry self-regulation in various ways. Despite institutional constraints making this role more marginal (Newman and Bach 2004: 394), it cannot be entirely discarded. Back in 1998, the FTC importantly published guidelines based on the Fair Information Practices indicating what self-regulatory programs developed by the industry should minimally include (Federal Trade Commission 1998: 15-6). These became an unofficial benchmark for industry self-regulation and contributed to establishing the role of the FTC as the main governmental agency dealing with privacy in the United States. As of now, it is still often sought for its views on privacy regulations by many industry associations. Its enforcement role obviously creates a particularly strong incentive for the industry to get its input. One interviewee for this research actually maintained that receiving the FTC's advice was integral to the process of developing a self-regulation in the United States:

> It's a two-way street relationship. We meet with the FTC multiple times every year. [...] If we have a new code, we always share it with the FTC to get their feedback on it. It is a very important part of that process. (Interview E32, done on April 25th, 2019)

All in all, few interviewees went as far as that. The role of the FTC remains primarily related to enforcement, not rule-making. The general view was that the FTC could indeed play a guiding role, but it was often indirect. In addition to publishing additional guidelines and case-studies, the FTC has for example organized workshops allowing the industry to exchange ideas. They would, however, "not provide a lot of remarks on these [self-regulatory] programs" (Interview E38, done on May 16th, 2019). One notable exception is the Safe Harbor program established under the 1998 Children's online privacy law (COPPA), which provides an official role for the FTC in the drafting of industry self-regulation. In American law, "safe-harbors" are legal provisions that limit the liability of private operators by specifying what conduct would not be deemed in violation of a specific rule. Copyrights, tax, and environmental law are just a few legal fields that make regular use of such types of provisions. In COPPA, it is foreseen that private companies that abide by self-regulatory programs approved by the FTC will be deemed to be compliant with its rules. As part of this process, the FTC provides detailed

feedback and invites public comments on industry self-regulatory initiatives that want to be approved to become official "safe-harbor certifiers" under COPPA.

In addition to the FTC, the Department of Commerce has also played an active role in influencing the development of industry self-regulation by negotiating various international instruments. Of particular importance, the EU - U.S. Safe Harbor framework, the Privacy Shield, and the APEC Cross-Border Privacy Rules (CBPR) system have all served to set basic rules for private companies dealing with personal information coming from Europe or Asia that went further than the requirements in the original guidance put forward by the FTC. In the case of the Safe Harbor and Privacy Shield, the Department of Commerce was able to sell to its European counterparts the just presented concept of a Safe Harbor and agree on seven principles that if complied with would limit the liability of American companies dealing with the personal data of Europeans. In a similar fashion, the CBPR system developed a set of principles based on which private companies operating in Asia could get a voluntary certification from a private accountability agent to demonstrate their respect for privacy. In both cases, the possibility of legal enforcement by the FTC is supposed to ensure that these self-regulatory programs have real teeth.

Just as in the United States, co-regulation has been a defining feature of the European regulatory approach towards privacy. While starting from the position that basic rules should be set by public authorities, the European Union has constantly given a role to industry self-regulation. Far from only relying on public rules and enforcement by independent public agencies, the 1995 Data Directive specifically carved out a role for the private sector. In its article 27, it indicated that Member States and the European Commission should promote the creation and adoption of "codes of conduct" by various economic sectors. It also provided that these codes can be officially approved by the European Commission through the Article 29 Working Party, the advisory body created to oversee the application of the Data Directive and primarily composed of representatives from data protection authorities in each Member States. As expressed by multiple interviewees, the European Commission has on multiple occasions helped industry came together and exchange with other stakeholders to develop self-regulatory programs:

> The Commission plays a role of coordinator and facilitator. It helps industry to come together and organize various workshops. (Interview E12, done on February 12th, 2019)

> The Commission acted as a facilitator. It hosted [industry's] work and helped them invite various stakeholders. (Interview E24, done on March 15th, 2019)

> It is self-regulation, but the European Commission is so involved that it might be more accurate to name it co-regulation. [...] Industry still has to do the work, but it is under the stewardship of the EU. (Interview E26, done on March 22nd, 2019)

In some cases, it even went as far as being the initiator and specifically asked industry representatives to develop codes for specific sectors:

> The trigger in both cases was public policy. [...] The European Commission wanted to see more activities in both sectors. Studies had shown that the EU was lacking behind the US and Asian countries in adoption of these services and it wanted the private sector to raise trust in the marketplace. (Interview E26, done on March 22nd, 2019)

As opposed to the American approach that principally plays a role in enforcing the rules devised by the industry, the European approach to self-regulation has thus been a "coordinated" (Newman and Bach 2004) or "regulated" one (Shulz and Held 2004). In practice, the European Commission aims to be involved early on in the process and actively influence the content of industry self-regulations. Rather than creating new rules *per se*, it is moreover hoped that they can help by specifying how public rules can be applied in different sectors and relatively uniformly all across Europe. In the words of the European Commission, the use of co-regulatory tools can help it have "greater flexibility in the way that [its] rules are implemented on the ground" and support their "[m]ore effective enforcement" (European Commission 2001*b*). At the same time, this co-regulatory approach helps it limit the lack of legitimacy and the democratic deficit of pure forms of private self-regulation (Christou and Simpson 2007: 22, see also Börzel and Risse 2010).

While giving less freedom to private actors, this European approach did lead to the creation of various industry self-regulations (Rodrigues and Papkonstantinou 2018). Table 3.4 lists all those adopted at the European level since 1995. It includes both codes primarily aimed at privacy as well as those dealing with it among other things. Just like in table 3.2, these were identified based on preexisting research (Cavoukian

and Crompton 2000; European Commission 2001*a*, 2012*b*; European Parliament 2012; Rodrigues and Papkonstantinou 2018; Trzaskowski 2006) and excludes self-regulatory programs that have been active in both jurisdictions at the same time, like the one of the International Chamber of Commerce and the Global Business Dialogue on e-commerce. It also excludes regulatory documents that would mainly set out technical standards. It finally does not include all the codes developed and active in a single European Member State. Only self-regulations that were devised for the entire European market or were minimally active in multiple European countries were kept. Including all codes and other self-regulatory tools adopted at the national level would give an even stronger feeling that self-regulation has truly been an important feature of the European approach towards privacy regulation, but it would simultaneously depict a more dynamic regulatory ecosystem than it actually is. The fact is that many codes adopted by national associations reflect the ones of an umbrella association representing them at the European level. Some national associations, like in Spain and the Netherlands, acted as pioneers and should should be recognized as such. This research nevertheless knowingly limits itself to the regulatory developments happening at the European level.

It is noteworthy that only one code developed by the Federation of European Direct Marketing Association (FEDMA) followed the process envisioned by the article 27 of the Data Directive and was officially approved by the Article 29 Working Party. Others either never tried to get the official approval or gave up because the process was considered to be too burdensome. In effect, it took FEDMA almost five years to have its code adopted. The European 'coordinated' or 'regulated' approach thus seems to have partly limited the development of self-regulations and many interviewees for this study were prone to maintain that there was in fact only one real code that had been adopted in Europe since 1995 (Interviews E5, E11, E16, E24, E26, E36). Regardless of this limited number of codes that were officially approved, the European Union interestingly did not put an end to industry self-regulation in the GDPR and even extended its role. Articles 40 to 43 of the GDPR now indicates that the European Commission and the European Member States should continue to promote the adoption of codes of conduct as well as certification schemes. Next to codes of conduct, which are expected to specify how privacy rules apply in specific economic sectors, certifications are seen as tools to be used to validate the compliance of private businesses with the rules of the GDPR. Moreover, both codes of conduct and certifications can now potentially serve as a sufficient legal

[12]This self-regulatory program drafted in partnership by the Union of Industrial and Employers' Confederations of Europe (UNICE; now called Business Europe) and the European Consumer Organisation (BEUC) ended up being never adopted.

Table 3.4 Main indsutry self-regulations dealing with privacy adopted at the European level since 1995

1997	Interactive Media in Retail Group's (IMRG) Code of Practice
1999	Which's Webtrader Code of Practice
2000	Eurocommerce's EuroLabel
2001	UNICE - BEUC e-Confidence Project[12]
2001	Clicksure Quality Standard
2001	Trusted Shops' Quality Criteria
2001	TUV SUD Safe Shopping Standard
2002	European eCommerce and Omni-Channel Trade Association's (EMOTA) Convention
2003	SafeBuy's Code of Practice
2003	Federation of European Direct Marketing Association's (FEDMA) Code of practice
2005	Electronc Retailing Association (ERA) Europe Marketing Guidelines for Electronic Retailers
2011	European Advertising Standards Alliance's (EASA) Recommendations on Online Behavioural Advertising
2011	Europrise's Privacy Seal
2011	Interactive Advertising Bureau (IAB) Europe's Online Behavioural Advertising Framework
2012	European Digital Advertising Alliance's (EDAA) Self-Certification Criteria for Online Behavioural Advertising
2015	E-Commerce Europe Code of Conduct
2017	E-Commerce Foundation SafeShop Trustmark

basis for the transfer of personal data outside Europe. This is significant because this gives an important role to private actors in the key question of how personal data should be protected when crossing national frontiers. The European Data Protection Board, the entity that replaced the Article 29 Working Party in the GDPR, actually expects that these private mechanisms will help the European Union "in the promotion and cultivation of the level of protection which the GDPR provides to the wider international community" (European Data Protection Board 2019: 10).

This continuous support for self-regulation in Europe seems related to the broader trend in favour of accountability mechanisms (Guagnin et al. 2012). Since the adoption of the Data Directive in 1995, it became increasingly clear that one of the key issues in the protection of privacy was the question of compliance. Having a comprehensive law is not in itself sufficient as you still need to ensure that it is applied and as one

interviewee straightforwardly said, "regulators will never have enough resources to do it [check compliance of all companies], so you have to figure out a way for companies to pay for certification services while also being answerable" (Interview E37, done on May 14th, 2019). This is precisely what the inclusion of certification schemes in the GDPR aims to achieve. This renewed interest for self-regulatory tools based on the concept of accountability is not disconnected from developments in the United States as the latter have promoted the adoption of certification programs since the creation of the APEC CBPR system. For them, the main rationale was that agreeing on certifications was the best way to allow for the transnational flow of data to continue without having to agree on a global set of privacy rules. This view now seems to be partly shared by the EU as it again included certifications as a potential tool for data transfers outside Europe and hopes that it will help it promote its rules globally.

3.6 Conclusion

As I tried to highlight in this chapter, the protection of privacy is not only a European story. The United States has been at the forefront of privacy debates for more than a century now. In addition to being American legal scholars who were at the origins of the modern concept of privacy, the Fair Information Practices developed by the United States Department of Health, Education and Welfare in 1973 still form today the heart of the privacy regimes in both the European Union and the United States. Since then, the regulation of privacy in the United States moreover never came to a standstill. At the federal level alone, new sectoral laws and industry self-regulations were continuously adopted and contributed to reshape how private companies could collect and use personal data in the United States. The federal government remained also active on the global stage by negotiating international instruments like the Safe Harbor and Privacy Shield with the European Union and the CBPR system with APEC countries. Far from being a laggard, the United States should thus be seen as having adopted a different regulatory approach than Europe.

With this in mind, I point out that this difference in regulatory approaches between the United States and the European Union does reflect a different conception of what privacy is. Despite starting from a similar liberal paradigm, both jurisdictions have indeed progressively diverged on what they believe is the exact nature of privacy. While the United States tends to see privacy as an economic good that can be traded

and should generally not be subject to extensive public regulations, the European Union views it as a fundamental right that is intrinsically linked with what it means to be an individual. This distinction is a clear source of misunderstanding and one important reason why a global privacy regime has never emerged and why different countries still maintain "conflicting regulatory regimes to deal with [the] issues" brought by new information technologies (Haufler 2001: 70; see also Dimitrov et al. 2007). Yet, I importantly caution against overemphasizing the importance of these differences and argue that, in practice, both the European Union and the United States are closer to each other than the two ideal-types generally ascribed to them.

Hybrid or co-regulation approaches are in effect used in both jurisdictions to ensure that the use of personal data by the private sector is respectful of the privacy of their citizens. In the United States, the FTC and the Department of Commerce have particularly contributed to the creation of industry self-regulations. Through its enforcement capacity, the FTC even actively promoted the adoption of specific obligations by the industry. In that regard, this form of 'enforced' self-regulation is not too dissimilar to the European 'coordinated' approach, which continuously tried to spur and organize the development of industry rules. The recognition of this hybrid or co-regulatory nature of both the European and American regulatory approaches to privacy is key for this research and it is where I start to depart from the previous 'clash of cultures' or 'clash of systems' arguments. By acknowledging the actual proximity that exists between them, I can more aptly show how they actually interacted and influenced each other's data protection rules over the years.

Back in early 1999, Clinton's head advisor for e-commerce, Ira Magaziner interestingly considered that "if the privacy protections (sic) by the private sector can be spread internationally, that will become the *de facto* way privacy is protected, and that will diffuse this disagreement [with the European Union]" (cited in Farrell 2003: 289). By promoting the use of self-regulatory tools globally, he hoped to limit the EU's influence in the United States as well as globally. To some extent, the adoption of the EU - U.S. Safe Harbor Agreement represented a success in that regard. By making the European Commission accept as sufficient the use of industry self-regulations, it did limit calls for the adoption of a comprehensive federal privacy law as well as the direct influence of the European Data Directive in the United States. The adoption of the CBPR system and the broader promotion of accountability mechanisms by American actors have also partly achieved Magaziner's hope by promoting self-regulatory tools as 'interoperability'

mechanisms between different privacy systems. As one interviewee who worked close to these negotiations indicated:

> We promoted the concept of interoperability because we believe that we cannot end up with the exact same vision of privacy. Privacy is a cultural thing, which means it will be implemented differently in different regions of the world. (Interview E27, done on April 4th, 2019)

This use of self-regulatory tools as an interoperability mechanism is now part of the European regulatory framework. As mentioned above, the GDPR specifically indicates that codes of conduct and certification mechanisms can be used to allow the transfer of European personal data to third countries. This contrasts with the adequacy decision procedure under which the European Union expects its partner to have a legal framework equivalent to its own before agreeing to allow personal data to flow freely between them. Although private tools like Binding Corporate Rules (BCRs) already allowed the transfer of personal data under the Data Directive, this heightened support for industry self-regulations does reflect a recognition by the European Commission that exporting its comprehensive privacy model throughout the world is far from an easy task. As specifically highlighted by one interviewee:

> [A]dequacy findings are challenging policy tools. [...] You look at the adequacy with Japan. It took close to 4 years to be negotiated and it will have to be reviewed every 4 years under the GDPR. This process is way too long and burdensome. Realistically, they probably do not have the means to go through this with all countries around the world. If it's a tool to export European rules, I would say it's an inefficient tool. [...] I think certification by private companies is more realistic. It is easier to have a conversation with companies than an international negotiation. (Interview E15, done on February 19th, 2019)

Significantly, industry self-regulations have not succeeded in entirely diffusing the disagreement as Magaziner might have hoped for at the end of the 1990s. With the recent adoption of the GDPR and the (re)negotiations of new adequacy decisions, the European Commission still keeps on promoting its comprehensive privacy system and to sometimes clash with the United States globally. Repeated legal challenges by privacy activists, like Max Schrems, to any agreements allowing data to flow between both jurisdictions moreover show on an almost daily basis that this transnational conflict is alive and well. Indeed, industry self-regulations did not become "the *de facto* way privacy is protected globally". Yet, they did become an important part of its regulation and have created new spaces of interactions between the two.

Rather than only being the American and European public authorities that co-operate on the regulation of privacy, there are now various industry groups and private companies that work together to define the data protection rules that govern the use of personal data. Through their work, they create new bridges and avenues for each regulatory systems to influence the other. As notably seen with the case of the original EU - U.S. Safe Harbor Agreement, they sometimes even work directly with public regulators in that process. Overall, this multiplication of public and private regulators and regulations creates a complex governance system that alters the process of rule formation in both jurisdictions through two joint processes: exploitation and exploration. Before reviewing each of them, the next chapter will explain at greater length how the transatlantic regulation of privacy can be conceptualized as a complex governance system and introduce the database of transatlantic data protection rules that I have built to analyze it.

Chapter 4

The Evolution of Transatlantic Data Protection Rules

They think GDPR is a revolution, but it's an evolution

Věra Jourová, European Union's Justice Commissioner, 2018

Far from simply being two rival models, the European and American approaches share a strong philosophical root. In effect, both start from a liberal paradigm to conceptualize privacy and broadly agree on the basic idea that individuals should have some form of control over their personal information to realize themselves. This contrasts with views according to which the broad public interest should prime over individual privacy interests. Over the years, exceptions made for security concerns, whether or not justified, have challenged this original standpoint (de Goede 2014). While having significant consequences for the regulation of privacy, they remain presented as exceptions or temporary (at least officially) deviations from this general principle. This basic agreement on the meaning of privacy is significant. While this can sometimes create misunderstandings as these broad principles are not always understood or applied the same way across the Atlantic, it still provides American and European regulators with a similar conceptual framework and language to discuss the regulation of privacy. As I will show in this chapter, this is made evident in their respective adoption of the same set of

basic data protection principles, including notably consent, access, quality, security, and transparency.

Moreover, their regulatory approaches have often been more hybrid, involving both public and private actions, rather than only relying on one or the other. Again, it should be clear that the point is not that categorizations opposing the American and European "limited and comprehensive systems" (Newman 2008), "sectoral to omnibus laws" (Solove and Schwartz 2011) or "market-based to rights-based approaches" (Schwartz and Peifer 2017) are wrong, far from it. They all reflect the real existence of a transatlantic divide over the question of privacy and have given us essential tools to reflect on it. As broad models that simplify our world, they however hide as much as they provide new light. In effect, just as they emphasize the differences between the two jurisdictions they minimize their similarities. In practice, even though the European Union has clearly been more forthright in its desire to regulate privacy issues, governmental agencies in the United States have also been active. In addition to play an important role in ensuring the enforcement of industry self-regulations, agencies like the FTC often coordinated their activities. Similarly, the European Union has not only relied on public rules but also supported the development of rules by the industry.

Recognizing this actual proximity between the regulation of privacy in the United States and the European Union both in terms of their conceptual background and regulatory approaches was a first key step to consider how they could be seen as forming a complex governance system. If either one of them were to reject the basic idea that privacy is about protecting individuals' control over their personal information, there would hardly be anything for their regulators to exchange on and it would be hard seeing them as together forming one regulatory system. Such fundamental disagreement can actually appear in debates over the increasing use of security exceptions, which precisely tends to reject individual interests for individual privacy for the supposedly collective interest. Although the European Commission has also shown an interest in deploying surveillance techniques of its own and sometimes readily worked with the American government (de Goede 2012), this is an area where interactions between their regulators are particularly difficult. The existence of a close cooperation between police and surveillance services in the United Kingdom and the United States is now a key reason why the former European Member State might not receive an adequacy decision and will have a hard time to cooperate with its European counterparts on privacy issues in the future,

even though it has in place an almost if not identical regulatory framework as it already implemented the GDPR (Espinoza and Khan 2019).

Putting aside these nonetheless important security questions, the early adoption of a similar set of basic privacy principles and hybrid forms of regulation have allowed the United States and European Union to influence each other in ways that have often gone unnoticed. This chapter is the first of three that attempts to specifically demonstrate how interactions between public and private regulators in both jurisdictions have shaped the formation of data protection rules since the adoption of the European Data Directive over a little bit more than twenty years ago. These three chapters will importantly emphasize that it is not merely a story of a shift in leadership (Vogel 2003) nor of competition (Drezner 2007) as previous scholars have argued. These are certainly part of the explanation and will be mentioned where relevant, but each significantly fails to see how their domestic regulatory processes have been and are still being shaped by the regulatory exchanges taking place between various public and private actors. Rather than simply being two national regulatory systems evolving in isolation from each other and then attempting to impose their regulatory preference to the other, their constant interactions have created a complex governance system (Kahler 2016; Oatley 2019; Orsini et al. 2019) that upended their respective process of rule formation from the very beginning. In other words, transnational interactions have been endogenous to the process of rule formation in both jurisdictions rather than exogenous forces occurring after each adopted their respective regulations.

In the rest of this chapter, I explain why the transatlantic regulation of privacy can be conceptualized as a complex governance system and what it means for its analysis. To do so, I start by extending the definition of complex systems that I introduced in chapter 2 and explains how it more precisely fits the present case. I take this opportunity to specifically emphasize the value-added of looking at regulations from a multilevel perspective where they are not only seen as single coherent policy documents but also as varying collections of principles and rules. I then detail how I built an entirely novel database of transatlantic data protection principles and rules that serves as the primary source of data for the remainder of this research. After having introduced the main elements of this complex governance system, I begin to trace its evolution by describing the early sets of data protection rules promoted in the United States and the European Union back in the mid-1990s. This will form the starting point to look at how they have evolved up to the adoption of the GDPR in 2016. In the last two sections, I finally define

and sketch the two joint processes, exploration and exploitation, that have driven the evolution of this complex governance system and that will be further analyzed in the following two chapters.

4.1 Transatlantic Privacy Regulation as a Complex Governance System

The formation of rules to govern the global economy does not happen in a vacuum. Whether it is governments adopting a new law or industry associations putting forward a new self-regulation, it is always influenced by what previous actors have done and this is no different in the case of data protection. Again, data protection or information privacy rules (in the United States), hereafter discussed, refer to the set of rules that define how personal data should be used to ensure respect for privacy. When devising such rules, governments and industry associations increasingly start from a dense institutional environment. Over the years, the absence of a global privacy regime (Dimitrov et al. 2007; Haufler 2001) as often led it to be seen as having a relatively low institutional density (Newman and Posner 2015). The lack of international rules codified in one multilateral international treaty or enforced by an international organization was seen as creating an environment where national regulators were left relatively unconstrained. The absence of such an interstate agreement or international organization, however, does not necessarily translate to a weakly institutionalized environment. It does mean that it is less centralized as there is no single actor setting or adjudicating the rules for all, like the World Trade Organization (WTO) is supposed to do for the trade regime, but it clearly does not mean that there are fewer institutions. If anything, the lack of a central authority has allowed a proliferation of competing actors and institutions aiming to set data protection rules, which form a complex governance system.

As mentioned in chapter 2, complex systems are "open systems [...] that include multiple elements (units) of various types intricately interconnected with one another and operating at various levels" (Orsini et al. 2019: 3; see also Bousquet and Curtis 2011, Kavalski 2007,Mitchell 2009, Morin, Pauwelyn and Hollway 2017). They moreover lack central coordination and order results from the continuous interactions between the elements of the systems rather than a single source of authority as in hierarchical systems (Orsini et al. 2019: 3). From this broad definition, I keep that complex systems share five

key characteristics: (1) no central coordination, (2) openness, (3) multiple heterogeneous elements, (4) interdependence, and (5) multilevel structure. The transatlantic regulation of privacy has all of them.

First, and as just mentioned, there is no single entity with the capacity to authoritatively define data protection rules in the transatlantic space. As the United States and the European Union never reached the adoption of a formal interstate agreement detailing what rules should private companies follow when using personal data, there are in effect no international organization or institution deciding what the content of these rules should be. The Organisation for Economic Co-operation and Development's (OECD) *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* of 1980 and its revised version of 2013 are probably the closest thing to it. Yet, their status of guidelines precisely means that they lack the authoritative status that WTO agreements for example have. Moreover, they represent more of a lowest common denominator than a complete set of rules. As it will be detailed below, the early European and American models of regulation were already quite different from the OECD guidelines in the mid-1990s. The Council of Europe's *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (Convention 108) of 1981 could be a new contender for the role as it is now open for non-European countries to join, but the United States is still not part of it and few countries outside of Europe are.

In the absence of such a supranational agreement, it could still be thought that the United States and the European Union are internally the central authority that can each define their preferred set of data protection rules. This is certainly in line with the traditional approach to view national systems as being hierarchical and perfectly orderly. In practice, though, the formation of rules does not have to only come from public authorities as the previous chapter pointed out. Both the United States and European Union rely on a hybrid form of regulation that explicitly recognizes the capacity of private actors to create rules, which can even become part of public regulation later on. While public authorities indeed have the power to enforce their laws and force private companies to abide by their rules, private actors can still create their own rules separately or on top of public ones. The process of rule formation is thus neither centrally managed in these two jurisdictions taken separately.

Second, the transatlantic regulation of privacy is open to external influences coming both from other geographical areas and policy fields. Although this research focuses

on the American and European interactions on privacy due to their historic and particularly close relationship, both have been interacting with actors in other regions of the world and notably Asia. While the United States negotiated a privacy framework with countries part of the Asia-Pacific Economic Cooperation (APEC), the European Union negotiated an adequacy decision with Japan and now works on one with its neighbour South Korea. Similarly, many private actors discussed below had interactions with some of their Asian counterparts. Other policy fields, like telecommunications and competition, have also sometimes informed its regulation and notably supported the creation of new rules as briefly discussed in chapter 6.

Third, there are multiple public and private regulations that have been adopted to define what should be good data practices for private companies. These include both hard and soft law-type of regulations (Abbott et al. 2000; Vogel 2008). Next to public laws, like the Data Directive in Europe or the Children's Online Privacy Protection Act (COPPA) in the United States, and soft laws, like the OECD privacy guidelines, industry associations were prone to create codes of conduct, certifications or other private forms of regulation to govern their own activities. Figure 4.1 actually shows the significant growth in the number of active industry self-regulations including data protection rules in the European Union and the United States from 1997 to 2017. Again, this only includes regulations created by industry associations at the European level or aimed to apply in more than one European country. Industry attempts at developing rules applicable on the world stage and potentially having an influence in both the European Union and the United States are included and shown separately.

The visible spike in the mid-1990s and the beginning of the 2000s is clearly associated with the adoption of the European Data directive in 1995 and the Safe Harbor in 2000 and highlights that the evolution of industry self-regulation is closely related to the level of scrutiny by public authorities as previously noted (see section 3.3 & 3.5). The relative stability in the number of industry self-regulations is however not only due to a slow-down in the adoption of new ones, but also the termination of some early ones. As time passed, industry associations that had adopted a self-regulation indeed ceased to exist or simply stopped being active in the privacy space. The relative stability that emerged in the number of industry self-regulations over time thus also results from the fact that the creation of new ones closely approximated the number of those disappearing. This kind of 'plateauing effect' is moreover reinforced by the fact that instead of having new actors coming in and creating new regulations, what we see occurring is in-

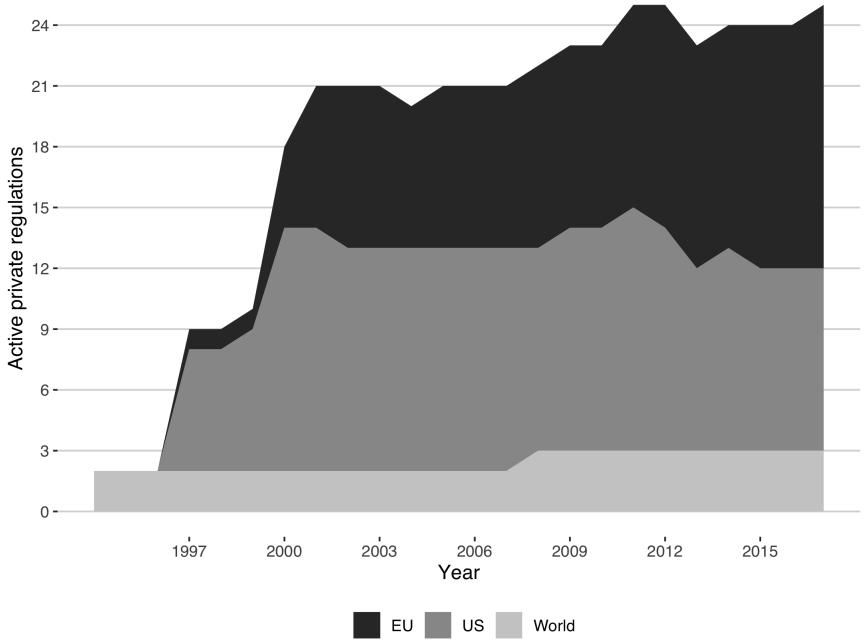

Figure 4.1: Sum of active industry self-regulations including data protection rules in the transatlantic space (1997-2017)

dustry associations that revise the one they already have in place. To observe change thus requires to look into the content of each regulation rather than only looking at their rate of adoption, which the multilevel approach explained below specifically allows.

Fourth, while different and being promoted by a diverse set of actors, all these regulations are tied together. At their heart, they are all based on the same liberal paradigm and, despite differences in how they apply it, they do agree on some core data protection principles (i.e., consent, access, quality, security, transparency, etc.). As explained in chapter 3 (see especially p. 54), both jurisdictions effectively start from the broad viewpoint that their societies are made of autonomous individuals that are able to determine their own interests and that need to be given the relevant space to do so. From this broad conception, they again part ways on how it should be protected. While the United States traditionally views it as a question of managing an information market, the European Union sees it as a human right that cannot be traded away. Yet, they do agree on the basic point that privacy rights aim to empower individuals. This in

turn offers them a common language to influence each other as previous work focusing on their different choice of regulatory approach again failed to see.

Moreover, private companies obviously have to respect the rules of the countries where they do business. As in other fields of law (Bartley 2011; Green 2013*a*), private forms of regulation will thus quite straightforwardly use these public laws as the basis to devise their own rules. This, in turn, tends to blur the distinction between 'delegated' and 'entrepreneurial' form of private authority as I previously hinted at in chapter 2 and will further discuss in chapter 6. In addition to these ties between the rules in their regulations, public and private actors often directly interact with one another. It is not unusual to find individuals that worked over the years for many organizations behind these regulations. Among the interviewees for this research, some notably worked for both public agencies and multiple private organizations that put out privacy-related regulations. Apart from these personal ties, links also exist between the organizations they represent. Official partnerships, joint projects, institutional support, and lobbying are all different forms of direct interactions that regularly take place between public and private actors in the regulation of privacy. Together, all these are the interactions that drive the evolution of the system and will be crucially investigated in the next two chapters.

Fifth, and finally, the transatlantic regulation of privacy operates at multiple levels that feed into each other. As a whole, it represents the entire American and European legal systems. These are more precisely made of regulators operating at the international, regional, national, and even sub-national levels. As widely recognized, decisions taken by one regulator at a higher level can trickle down and influence regulations at another as in a traditional hierarchical system, but the contrary is also possible. Regulations and rules developed by sub-national authorities (e.g., the government of California) can influence regulations adopted at a higher level. Regulations themselves can also be viewed as existing at multiple levels. As a whole, they are relatively coherent documents that aim to achieve a specific policy goal (i.e., guaranteeing an individual's privacy). Yet at another level, they can be viewed as collections of rules and show much more diversity than otherwise thought. Interestingly, trends and patterns of change appearing at one level might not be as significant or evident to spot at another (Modelski 1996). The adoption of a new rule could notably have significant legal consequences, while not fundamentally challenging the legal system in place. Similarly, the adoption of a new regulation that might appear as revolutionary by the people it targets might still show a lot of continuity

when looking at its individual components (i.e., rules) as a whole. This is certainly the case of the GDPR, which is often portrayed as representing a radical change due to its directly enforceable nature in all European member states and stronger enforcement mechanisms. Yet, as the European Union's Justice Commissioner cited in epigraph to this chapter rightfully pointed out, the GDPR represents more an evolution than revolution as it still largely follows the same principles and rules previously found in the Data Directive and other regulations adopted since then. At the level of its constitutive rules, the GDPR is in fact not as novel or disruptive as many think. It might also be that seemingly small changes at one level have disproportionate consequences at another. Changes in how consent is gained could for example upend some of the most basic principles of the regulation of privacy in one or both jurisdictions.

The recognition of the multilevel nature of regulations offers a new way to look at regulatory changes and is one of the key contributions of the present work. In contrast to previous studies focusing on the global influence of one paradigm or policy idea (Elkins, Guzman and Simmons 2006; Hall 1993; Meseguer 2009; Simmons and Elkins 2004) as well as recent work like the one of the United Nations Conference on Trade and Development (UNCTAD) Global Cyberlaw Tracker comparing the presence or absence of legislation, the current approach can go further and highlight how the adoption of seemingly similar adoption of privacy regulations can actually hide a lot of diversity. It also differs from many strands of work in political science that tends to see change in stark opposition to continuity, such as those emphasizing how critical junctures break from otherwise path-dependent tendencies (Bell 2011; Cappocia 2015; Kelemen and Cappocia 2007). In effect, the multilevel approach that I take here allows me to see that the same regulation can simultaneously support processes of convergence and divergence, which are both key in the evolution of a complex governance system as I noted in chapter 2. Before introducing how each process materializes itself, the next section will present the original database on data protection principles and rules in the transatlantic area that I built for this research.

4.2 A Database on Transatlantic Data Protection Principles and Rules

The primary source of data for this research is an original database that I created on data protection principles and rules found in 126 public and private regulations adopted in

the transatlantic area and in force after 1995. As no other contributions had previously attempted to do such a comprehensive analysis of the evolution of data protection rules promoted in the United States and the European Union, I did not have much to start from and largely had to build it from scratch. It includes the OECD privacy guidelines adopted in 1980 as they were still promoted up until their revision in 2013. The only other regulation created before 1995 and that I included in this database is the code on market and social research jointly adopted by the International Chamber of Commerce (ICC) and the European Society for Opinion and Marketing Research (ESOMAR) in 1994 and then only revised in 2001. The entire list of regulations included in the database is listed in appendix B and include all the regulations and their revisions identified in the previous chapter (see table 3.1, 3.2, 3.3 and 3.4).

Again, I identified all these regulations based on previous research (Cavoukian and Crompton 2000; European Commission 2001*a*, 2012*b*; European Parliament 2012; Rodrigues and Papkonstantinou 2018; Trzaskowski 2006). In building this specific corpus of regulations, I aimed to be as exhaustive as possible and to include all those created at the American federal level, European level, or international level by public or private actors. In line with the complexity approach taken in this research, it was indeed essential that this database includes all constitutive elements of this system to uncover how each interacted differently with the other and, in the end, affected its evolution. The network methodology that I use and discuss at greater length in chapter 5 moreover made techniques like random sampling difficult as they could have led me to miss out on essential elements of the system, changing its structure and potentially giving a wrong picture of who are the important actors and pathways of influence (Wasserman and Faust 1994: 31-34; see also Carrington, Scott and Wasserman 2005; Cunningham, Everton and Murray 2016). While more targeted forms of sampling can sometimes be used, they need to ensure to provide a similar network structure at a lower scale than the full network. As the number of privacy regulations was already limited, building such a sample was in this case almost impossible and only created risks of losing crucial information on the evolution of privacy regulations.

With that in mind, the creation of this original database still required to define what exactly formed the population of this transatlantic regulatory system and, concomitantly, what were its boundaries. As noted above, one characteristic of complex systems is that they are open to their external environment and that their external boundaries are not always as clear as closed systems for which we can normally identify without too

much doubt all of their constitutive elements. One common example of this is a plane, which can be viewed as a system of integrated components that can be relatively easily listed, if not by the present author, by one of its engineers. Doing so for a regulatory system is however a much harder task as there are different ways to define what constitutes them. Which elements should be included or not then becomes not only a matter of external and verifiable reality but of the analytical strategy being used by a researcher (Cilliers 2001: 114). In this case, one of these very choices that I made was to focus on the transatlantic area. Other studies could well have decided to look at the evolution of privacy regulation from a global, Asian, or another perspective. As previously noted, the focus on the transatlantic area reflects both their long-lasting and significant relationship, as well as their importance for global privacy debates. Their joint adoption of a liberal paradigm was moreover seen as creating a sufficient link between the two to view them as one regulatory system made of different regulators.

Two other important choices that I made in the definition of the population forming the present database relate to the levels of analysis included in the present research. First, only regulations adopted at the American federal, European, or international level were included. This means that laws adopted by federal states or European Member states are not part of the present database. This choice was not taken lightly as previous research has emphasized the significant catalyst role that some of these actors can play. In the United States, the state of California has long been recognized as having the capacity to act as a catalyst for the adoption of regulations (Vogel 1995; Chander, Kaminski and McGeveran 2020). Similarly, France and Germany are regularly pointed out as having a particular say in shaping the regulation of various issue-areas in Europe, and notably privacy (Green Cowles 2001; Recio 2017). As this research is fundamentally about the interactions between regulators on both sides of the Atlantic, it was however considered that these different entities did not engage with each other as repeatedly and significantly as American federal agencies and the European Commission. While including these additional actors could have provided more detailed information about internal dynamics in each jurisdiction, it also created additional risks of missing more interactions between these different regulators and ending up with an erroneous picture of the transatlantic system. In effect, it even risked creating more noise in the analysis as not all federal states or European member states are of equal importance nor have a global influence. Considering that the American federal government and the European Commission moreover have the legal authority to supersede these federal or national laws, their own interactions and how it affected the content of their regulations have

more influence over the content of the rules promoted in each jurisdiction. Having said that, mentions to relevant laws of federal states or European member states will be made when necessary. These are simply not presented as the core regulators that interacted with each other in the transatlantic area.

My decision to only include regulations at the American federal, European, or international level is also valid for private regulators. While in the United States there does not seem to have been a lot of industry self-regulations created for one specific state, this choice is quite significant in Europe where each member state often has its own set of industry associations developing codes of conduct, guidelines, or certification programmes. Early codes adopted by the ancestor of the industry association now named Adigital in Spain or ECP.NL in the Netherlands notably appeared in a preliminary research as having played an important role in the development of private forms of regulation in Europe and even globally in the mid-1990s. In the case of ECP.NL, their code notably ended up being referenced in a recommendation on the development of private codes of conduct for e-commerce adopted by the United Nations Centre for Trade Facilitation and Electronic Business in 2001. Just as federal states or European member states, most of these national actors were however less active in the transnational space and were members of larger European associations setting out their own regulations that they were supposed to follow. The Federation of European Direct Marketing Association (FEDMA) that had its code approved by the Article 29 working party created by the Data Directive is actually representing direct marketing associations in most European member states, which all are supposed to implement its code. This is not to say that the relation of influence never goes the other way around or that they did not play any role, but as a whole, they are not as significant and were thus discarded. National associations that actually became active in more than one European member state were the only ones kept in the database.

A second important choice that I made when defining the population of regulations included in my original database was to only include industry self-regulations setting up rules for multiple private companies. This means that I included codes of conduct devised by an industry group for all its members or certification programmes built by one company but used by many. Meanwhile, I excluded internal policies adopted by a single company for its own use. Although those of large and well-known companies may lead others to adopt the same practices, few have such a systemic impact. Moreover, most of these companies actually base their policies on the codes of conduct put forward by

industry associations they are part of or the requirements of a certification programme that they voluntarily follow. Microsoft and Apple for example had their privacy policies certified under TrustArc's certification programme, which is included in the database used for this research. Similarly, Google and Facebook are current members of the Direct Marketing Association (DMA) and thus have to abide by its code of conduct that is also part of the database. As these industry self-regulations also directly apply to many small firms, they give a more systemic view of which data protection rules are promoted by private actors and how do these evolve over time. It does not mean that it would not be relevant to look into the relations between private companies' internal policies and these different industry self-regulations. Doing so could show that some companies perhaps do not fully implement the industry self-regulations that they are supposed to follow. It could also highlight that industry self-regulations are not the ones devising new rules and are rather used by some companies to project their owns onto others. On that last point, it could however be the opposite and that some companies simultaneously active in multiple industry associations are the ones promoting the rules of an industry self-regulation in other fora. Despite potentially providing additional insights on who sets data protection rules and how, these dynamics will not be further investigated in this work as doing so would have made my current data collection too cumbersome and raised the risks of getting a wrongful representation of the system in place. Future research could however add to the present work by looking at this extra-layer of interactions as I will briefly discuss in the conclusion of this research.

Having specified these inclusion and exclusion rules[1], 126 regulations were manually collected from publicly available websites. As reiterated above, I identified these regulations based on previous research, including some specifically funded by public agencies aiming to get a better understanding of industry self-regulations in the e-commerce and privacy space (Cavoukian and Crompton 2000; European Commission 2001*a*, 2012*b*; European Parliament 2012; Rodrigues and Papkonstantinou 2018; Trzaskowski 2006). I also asked all my interviewees who were according to them the main public and private regulators that had adopted privacy regulations. Their answers were then compared with the information that I had found in these documents. In the end, there was only one private organization that I had missed and that I then duly added to my database.

Public regulations were retrieved from the different governments' or agencies' websites. Amendments adopted over time were included as separate regulations. In cases

[1]These rules are summarized in the introduction to Appendix C that explains at greater length how documents were collected and coded to ensure replicability.

where the amendment only modified one or few rules, a separate document including both the original law and the amendment was added to the database. This allowed seeing more clearly the evolution of a regulation through time. Compared to public regulations, accessing older industry self-regulations proved more tricky. Not all private associations kept a public record of the previous versions of their codes of conduct, guidelines, or certification programmes. Only the latest set of rules was most of the time readily accessible online. To access these older versions and gain an insight into how they changed over time over time, I used the Internet archive *Waybak Machine* tool allowing to access most webpages created since the mid-1990s. In a few cases, it was unfortunately impossible to go that far back and to find their rules before 2000. These only represent a small number of cases and appropriate caveats will be made when needed in the analysis. When the version or year of adoption of an industry self-regulation was not clearly specified, making unclear if changes had been made, the text of the regulation available online at the beginning of every year was compared using a free online tool allowing to find textual differences between them. As soon as there was a difference in its content (i.e., not the title or the address of the organization), I considered that a new version of the regulation had been adopted and included it as a separate document in my database with the date of the year it was put up online.

Following a content analysis of these different regulations and their revisions, I tracked "change and development" in the regulation of privacy (Bowen 2009: 30). From the 126 identified public and private regulations, 14 principles and 71 rules were found and manually coded. Principles are here taken as broad "beliefs fact, causation, and rectitude" and rules as "specific prescriptions or proscriptions for action" implementing these broader principles (Krasner 1982: 186) . To put it differently, "principles are open-ended as to the range of actions they prescribe, while rules prescribe specific actions" (Drahos 2017: 249). As opposed to technical standards defining, for example, production techniques and that can be very detailed, many rules can still be general in how what they prescribe must be applied. Yet, they always prescribe a relatively clear action rather than a broad objective. To give a practical example from the current research, the first principle listed in the database is transparency, which foresees that the collection and use of personal information should be done in a clear and open manner. This principle is then divided into 11 rules that explain how it is applied. It notably includes the obligation to have a privacy policy informing individuals of how their data is being used, informing them of the type of data that is being used and to whom it might be disclosed.

All principles and rules are listed in Appendix C that presents the codebook used for manually coding all 126 regulations.

In recent years, both legal scholars and political scientists have increasingly made use of automated tools to analyze legal or political texts (Grimmer and Stewart 2013; Allee, Elsig and Lugg 2017; Alschner, Pauwelyn and Puig 2017). These are powerful methods allowing to quickly evaluate the similarity of multiple laws or other legal documents. As the latter often adopt the same language, they can spot textual patterns and repetitions across multiple texts and thus potentially single out when and where similar rules exist. Automated methods are moreover more easily replicated and verifiable as opposed to manual coding. There are evident risks when coding texts manually to find false positives (i.e., coding something that should not be) or false negatives (i.e., not coding something that should be). This does not mean that automated methods should always be preferred, though.

As Wolfgang Alschner and his colleagues notably point out, most automated techniques "are language-specific" (2017: 230). This means that they will only work if all the documents are in the same language. Of more relevance for this research, basic automated coding techniques do poorly with documents of different formats and types. In the present case, the database includes American laws, European directives and regulations, transnational agreements, and industry self-regulations. Although they all deal with the same issue, quantitatively comparing the presence of strings of text in these different types of regulations written using different drafting techniques will not produce something as meaningful as recent studies that compared texts sharing the same basic structure like trade agreements (Allee, Elsig and Lugg 2017). More complex automated coding techniques that would have for example relied on parts of manual coding could have been used. These would have, however, required a similar amount of work than to manually code this database and, as such, were rejected. Automated coding is finally well suited to classify and scale documents (Grimmer and Stewart 2013: 268), but it can hardly identify and single out specific elements (e.g., the rules) in a document. As this research notably attempted to identify the content of the new rules and principles emerging in the regulation of privacy over the years, qualitative coding allowing for the use of a partly inductive approach was thus again seen as the best option.

To ensure the highest possible coding reliability, I developed a codebook that can be found in Appendix C listing clear inclusion and exclusion rules for all principles and rules. Each rule was given a different definition and code, which were then attributed

to a single specific principle. These codes were created both deductively and inductively (Campbell et al. 2013: 311-2). Again, as far as I am aware, there is no other work that had previously attempted to develop a similar database and to categorize all existing data protection rules, making an inductive approach partly inescapable. As just pointed out, the interest in identifying new elements in the regulation of privacy also made an inductive work essential. The first set of codes was nonetheless created based on two sources of information. First, an early research by the Ontario privacy commissioner of industry self-regulations in the privacy space was used to identify the initial set of data protection principles and rules (Cavoukian and Crompton 2000). Second, resources put out by law firms and data protection offices in Europe and the United States summarizing the content of the GDPR were used to distinguish more recent data protection principles and rules. White & Case (2019) is one recent example of a law firm that put out a *GDPR Handbook* and the Information Commissionner's Office of the United Kingdom (2019) is one of a data protection authority that published a guide on how to apply the GDPR.

I then applied the first set of codes to a randomly selected pool of 20 regulations from the database. Following this first wave of coding, new codes were added for rules that did not fit any predefined one. Refined codes were also created for broad principles and rules that could sometimes be split into two or more. At this stage, a difficult balance had to be found between creating an increasingly complicated coding scheme and ensuring its reliability. While potentially providing a more detailed picture of the content of each regulation, the more detailed a coding scheme becomes, the more it risks losing its *discriminant capability* (Campbell et al. 2013: 301). As more codes are added, it becomes more cognitively demanding to distinguish elements in a text and thus raises the likelihood for coding errors. This means that some subtle, but still significant divergence in rules found in various regulations were certainly lost in the coding process. One example of this is the distinction between opt-in and opt-out consent, which unfortunately could not be included as it was not always clear which one a specific regulation was advocating for. This is, however, a major distinction in how privacy is protected on the ground. While the first requires to obtain the formal consent of individuals before collecting and using their data, the latter basically assumes that individuals using the services of a company and do not otherwise indicate their disagreement have consented to have their data collected and used. Making the distinction between these two forms of consent in a truly replicable manner was even more difficult as there are now also rules allowing individuals to withdraw their consent or to opt-out of specific data processing at any time. While different, the similar language used in these provisions truly made

it impossible to have two different codes for these two types of consent. As always, this limitation is specifically acknowledged when needed and integrated into the analysis insofar as possible. I finally used the updated codebook to code the entire corpus of regulations. Once done, I revised the entire coding one last time for consistency.

My original database built throughout this process will hereafter be used to look into how interactions between public and private regulators created complex system dynamics that influenced the content of each of their respective regulations. The next section will start by presenting the early regulation of privacy by comparing the early models of data protection rules promoted in the United States and Europe. This will, in turn, provide the basis for investigating how data protection rules have evolved through the two processes, exploitation and exploration, that simultaneously pushed towards greater regulatory convergence and divergence.

4.3 European and American Early Models of Data Protection Rules

Before detailing the two processes that have been animating the regulation of privacy in the United States and Europe, it is essential to determine what rules were originally promoted by both of them. Again, studies on the regulation of privacy in Europe and the United States generally start by pointing their different regulatory approaches (Newman 2008). While Europe has had a comprehensive law since the adoption of the Data Directive in 1995, the United States is seen as still lacking one. Such line of argument yet does not give a good sense of what are the actual data protection rules that each have historically hoped to see implemented. It focuses more on the different implementation strategies than the content of the rules being applied. The multilevel approach and focus on the content of privacy regulations of the present research promotes a more fine-grained analysis and aims to distinguish the different rules included by each of them early on. This will provide the starting point for the remainder of the analysis.

In the case of the United States, it is obviously not as easy to identify one clear set of rules as in Europe. Their reliance on sectoral laws and codes developed by different agencies makes it hard to say what is the exact set of rules that the American government hoped to see applied. While some could be tempted to maintain that they do not have a preferred set of rules or that they even do not want to promote one, this does not

seem to fit their actions. Since the United States Department of Health, Education and Welfare adopted its Fair Information Practices' guidelines in 1973, many federal agencies put forward data protection rules. These were followed by the adoption of various sectoral laws adopted by the federal government that all incorporated a similar set of core data protection principles and rules. Perhaps more significantly, though, the United States did negotiate data protection rules on several occasions at the international level, including with Europe, and clearly developed a position on what type of rules future privacy regulations should include. To identify the position of the United States back in the mid-1990s, I use the official guidelines published by the FTC in 1998 listing what good industry self-regulations should include at the time. As opposed to a law, these were voluntary in nature. Yet, the central role of the FTC in enforcing industry self-regulations unsurprisingly pushed private actors to them take quite seriously, if not in practice see them as mandatory. Moreover, these guidelines mostly included rules found in federal sectoral laws and the OECD guidelines previously negotiated by the American government. It should finally be noted that the FTC closely worked with the Department of Commerce and actually helped the latter develop its position when negotiating the regulation of privacy on the international scene. With this in mind, these guidelines adopted by the FTC were considered to represent a *de facto* model of what the United States would have liked to see included in a privacy regulation.

Table 4.1 compares the OECD guidelines of 1980, the European Data Directive of 1995, and the FTC guidelines of 1998. The OECD guidelines were added as a reference point. As previously noted, they were negotiated by both the United States and the European Union and in many ways represented the smallest common denominator between their preferred set of rules. Comparing it with the Data Directive and FTC guidelines thereby allows getting a sense of the evolution that had already occurred since the early 80s. To ease the reading, only rules that were included in at least one of these regulations were listed. When looking at table 4.1, we can first observe that both European and American regulations moved significantly further than the original OECD consensus. In effect, both the FTC guidelines and the European Data Directive added new rules to those found in the OECD guidelines. At the same time, we can see that the European Union was already attempting to have a more 'comprehensive' set of rules as its Data Directive included more than twice as many new rules as the FTC guidelines. Of particular interest, each of their new rules also did not deal with the same issues.

Table 4.1: Comparison of Early Data Protection Rules across the Atlantic

Principles	Rules	OECD Privacy Guidelines (1980)	European Data Directive (1995)	FTC Fair Information Practice Principles (1998)
01. Transparency	01.01 Privacy statement	•	•	•
	01.02 Data controller's contact information	•	•	
	01.03 Data types and purposes	•	•	•
	01.04 Data source		•	
	01.06 Third-party transfer	•	•	
	01.09 Automated or passive data collection			•
	01.10 Consequences of withholding personal information	•	•	
02. Consent	02.01 Original consent	•	•	•
	02.06 Right to refuse automated decision-making		•	
	02.07 Right to object		•	
03. Collection limitations	03.01 Purpose limitations	•	•	
	03.02 Fair and lawful	•	•	
	03.03 Third-party source			•
04. Use limitations	04.01 Original purposes	•	•	
	04.02 Fair and lawful		•	
05. Disclosure	05.01.01 Consent		•	
	05.03.01 Use limitations		•	
	05.03.02 Adequacy of processor policies		•	
	05.03.03 Contract		•	
	05.04 Third-country transfer		•	
06. Data quality	06. Data quality	•	•	•
07. Individual participation	07.01 Access and review	•	•	•
	07.02 Correction	•	•	•
	07.03 Erasure	•	•	
	07.04 Notification of third parties		•	
	07.05 Access denial	•		
	07.06 Right to challenge	•		
	07.07 Right to be informed of automated practices		•	
08. Sensitive data	08.01 Consent		•	
	08.02 Third-party transfer		•	
	08.03 Special security measures		•	
09. Children data	09.01 Special notification			•
	09.02 Special collection limitations			•
	09.03 Parental control			•
	09.04 Parental consent			•
	09.05 Parental access			•
	09.08 Special security measures			•
10. Data security	10.01 Commitment to data security	•	•	•
	10.08 Data protection officer		•	
11. Data retention	11. Data retention		•	
13. Enforcement	13.01 Complaint mechanism			•
	13.02 Compliance mechanism			•
Total		13	30	20

In Europe, we can first view a broad tendency to expand the list of data protection principles found in the OECD guidelines. Additional rules were notably included to ensure that private companies were transparent (Principle 1), respectful of an individual's consent (Principle 2), and allowed them to have some form of control over their personal data (Principle 7). Without going over all of these additional rules, it is noteworthy that in addition to requiring that individuals should have access to their personal information and have the possibility to correct and delete it when found to be wrong, the Data Directive expressly asked that such changes be notified to all potential parties to whom the data might have been disclosed "unless this proves impossible or involves a disproportionate effort" (Art. 12(c)). Following the adoption of the GDPR in 2016, one of the most widely discussed provision was the so-called right to be forgotten that is supposed to allow Europeans to ask for the erasure of their personal data (art. 17). Importantly, this obligation was not entirely new and, in fact, mostly expanded another right that was already included in the OECD guidelines in 1980. Rather than primarily allowing to request the erasure of personal data when found to be incorrect or incomplete, the GDPR more precisely offers several new reasons allowing individuals to request the erasure of their personal information, including when the data is no longer needed. In 1995, the Data Directive was in fact already expanding the rights to correction and erasure by requiring private companies to inform third parties with whom they had shared personal data of its correction or erasure.

Besides the creation of additional rules elaborating on preexisting principles, the Data Directive also included rules for three new principles: disclosure (Principle 5), sensitive data (Principle 8), and data retention (Principle 11). Without again describing each rule, it can be noted that the focus on data sharing (i.e., disclosure) between private companies with partners inside and outside of Europe was an early concern for the European Union. As new technologies used to collect and process personal data was also making it easier to share it with third parties, the European Union appeared highly concerned that exchanges of data between private companies would not lead to an indirect violation of the privacy guarantees offered to individuals, especially when data would be sent to companies in non-European countries.

Meanwhile, we can see that the United States attempted to generally stay closer to the rules found in the OECD guidelines. Instead of expanding the broad principles previously negotiated there, they generally stuck to it and sometimes even dropped some rules found in the OECD guidelines. One noteworthy absent is the rule on the erasure of

personal data. As opposed to the Data Directive that expanded it, the FTC guidelines did not even mention it. This discrepancy highlights the general tendency to give more freedom to companies using personal data in the United States. Rather than including the possibility for individuals to request the removal of their personal data altogether, it seemed like the FTC found sufficient to promote their mere correction. At the same time, the FTC guidelines also added one new interesting requirement in terms of transparency. It specifically indicated that industry self-regulations should require private companies to clearly state how they collected personal information and, notably, if it was through passive means. The latter occurs when our personal data is collected without us doing anything specifically. Over the years, this was increasingly done by storing electronic information on our computers to identify us and collect information about our online activities. This practice is more popularly known as placing an electronic "cookie", for which we regularly receive notice when visiting a website. These were created in 1995 and thus were not a known phenomenon when the Data Directive was drafted. A specific requirement to be transparent about the use of this tool was added in the 2002 ePrivacy Directive complementing the Data Directive. By that time, the FTC guidelines had already included a reference to the importance of informing individuals about the use of such data collection practices.

Apart from this, the FTC guidelines also comprised rules on two new principles that were not in the OECD guidelines nor the Data directive. First, it contained multiple rules aimed at protecting the privacy of children online. These mostly copied what can be found in COPPA, the American law ensuring the protection of children online adopted the same year based on the advice of then-FTC's Chairman Robert Pitofsky (Hertzel 2000: 437). Second, the FTC guidelines also had clear guidance for the creation of mechanisms to enforce data protection rules (Principle 13). This is in part due to the role of the FTC, which is notably to ensure that self-regulations are followed. Yet, it also reflects the particular legal culture in the United States and early interest for accountability measures noted in chapter 3. One interviewee interestingly remarked that "Europe didn't have a concept of accountability in the Data Directive, which was shocking for an American lawyer like me" (Interview E27, done on April 7th, 2019).

Table 4.1 finally shows that despite sharing some core elements, the early models of data protection rules in the United States and the European Union were significantly different. It is here essential to reassert that coding choices might even make them appear closer than they really are. As previously mentioned, although both the United

States and the European Union recognized the principle that the use of personal data should generally be based on an individual's consent or choice, they have historically differed in the way it should be collected. In the United States, it has been common to accept the use of an opt-out form of consent where individuals will be considered to have provided their consent if they use a company's services and have not specifically voiced their objections (opt-out) to the use of their personal data. Meanwhile, in Europe, it was originally expected that individuals should give their consent before using a company's service (opt-in). Due to the sometimes loose language used in the regulations analyzed, it was again impossible to draw a clear line between these two forms of consent, and the two models are both shown as including rules on the need of original consent in table 4.1.

This caveat should importantly make clear that regulatory divergences between the early 'European' and 'American' models of data protection rules ran deeper than the analysis that I presented here can actually demonstrate. Just as both jurisdictions ended up following two different regulatory approaches following a similar liberal starting point, they also diverged in the content of the rules that they promoted. At the same time, it is noteworthy that they were still following the same broad principles that they notably had negotiated at the OECD and that partly originated from the early work of the United States Department of Health, Education and Welfare in 1973 (see p. 56). We can effectively see that while diverging on the specifics of how different guarantees should be implemented, they did fundamentally agree that data protection rules should aim to ensure that individuals can control how their information is shared and being used. Here again, the approach of seeing regulations at different levels of abstraction allows for a more fine-grained understanding of the extent to which both jurisdictions shared similarities than studies focusing on the convergence of data protection principles (Bennett 1992) or their divergence in regulatory approach (Newman 2008). It also helps to see how they could practically interact and influence each other. Even though they might not have been agreeing on a common set of data protection rules, they still shared a core understanding of privacy made evident by their acceptance of similar principles.

Since then, new regulations adopted by public and private regulators in both the United States and European Union evolved based on their joint interactions. Interestingly and perhaps paradoxically, these interactions tended to push them both closer and further away from each other. Through their interactions, public and private actors in effect progressively came to share more rules than ever before. At the same time, the

creation of new rules based on the very same exchanges also tended to push them further apart and impeded them to become copies of each other. These dual forces reflect the general tendency of complex systems to evolve in a dynamic state of equilibrium (Kim 2013; Morin, Pauwelyn and Hollway 2017; Pauwelyn 2014; Puig 2014; Ruhl, Katz and Bommarito 2017). Rather than moving from one clear model (or equilibrium) to another, which simple comparisons of two regulations might seem to indicate (Chander, Kaminski and McGeveran 2020; De Hert et al. 2018; Macenaite and Kosta 2017), the transatlantic regulation of privacy grows through a much more incremental process where stability and change constantly co-exists. The next and final two sections will introduce at greater length the two joint processes briefly discussed in chapter 2, exploitation and exploration (Duit and Galaz 2008; March 1991), behind these converging and diverging trends and that will be analyzed in more depth in chapter 5 and 6.

4.4 The Convergence of Data Protection Rules in the Transatlantic Space

The first important trend in the regulation of privacy in the transatlantic area over the last twenty years or so has been towards greater regulatory convergence. From the early models of data protection rules put forward and respectively supported by the American government and the European Commission, public and private regulators in both jurisdictions have started to include the same rules. As two interviewees for this research specifically held:

> Convergence is the current keyword. [...] We are all progressively going in the same direction. (Interview E18, done on February 27th, 2019)

> We have convergence. Times change and there is a realization that you need something. [...] The GDPR, being the last and most comprehensive regulation, is becoming an important source of inspiration globally. (Interview E20, done on March 1st, 2019)

Importantly, though, this trend has not only been towards European rules. While European regulators certainly had a significant impact on the set of rules now being promoted in the United States, and in many other jurisdictions around the world for that matter, other regulators did not sit idly by waiting to approximate European rules

as they emerged. Many were indeed active in devising rules and looking to make them adopted globally. As another interviewee maintained:

> It is a global conversation, much more than the EU let it appears. [...] The GDPR certainly raised the awareness of consumers to privacy issues. I think the Commission was really good in their marketing campaign, but the reality is that it is a global discussion. (Interview E15, done on February 19th, 2019)

As new data protection rules populated the transatlantic regulatory system, regulators have in effect tended to gravitate towards a similar model, and these were not a purely 'European' one. As previously noted, the American government was, for example, the first to create rules on the protection of children's privacy and specifically pushing for the development of private enforcement mechanisms, which have since then been taken up by European public and private regulators. This similarly occurred for data breach rules first enunciated by the government of California and various other ones by private regulators. This process of convergence can be observed by looking at the rising similarity between regulations adopted in both jurisdictions over time.

Various methods exist to calculate the similarity between two or more texts. Most commonly, a Jaccard similarity (see e.g., Alschner and Skougarevskiy 2016) index is used. The latter calculates the number of elements (i.e., a string of x words or manual codes) that two texts share divided by the remaining number of potential elements (i.e., a non-similar string of words or non-coded text). To put it simply, it calculates the number of co-occurrences in two texts against the potential number they could have had. One limitation of this method is that it is sensitive to the length of the texts compared. Comparing a significantly longer text or more manual codes with a significantly shorter one or fewer codes will generally indicate a low level of similarity even though the shorter text might be an almost replica of part of the longer one. To minimize this phenomenon, a thematic similarity calculates the average between the number of similar strings of text or coded texts compared to the total number possible in one text (Armborst 2017: 3). The following equation expresses this idea mathematically:

$$t = \frac{1}{2}(\frac{n_{12}}{n_1} + \frac{n_{12}}{n_2})$$

In the latter, t is the thematic similarity index. It is given by adding the proportion of shared elements (n_{12}) in the first text (n_1) to the proportion of shared elements

(n_{12}) in the second text (n_2). It is then divided by two to get the average. In this specific case, the shared elements are rules that have been manually coded in both regulations. Importantly, this similarity calculus does not give the textual similarity *per se*, but the level of similarity in the coded content of each regulation. In other words, the index should not be taken as meaning that two regulations with a similarity index of 0.5 are half-identical, but that the mean of their shared rules compared to their total number of shared rules is 0.5. This could result from a situation where both regulations have half of their rules similar to the other (R_1 and R_2 both share 5 rules out of 10), but it could also result from two regulations with different ratios of similar rules (R_1 shares 3 rules with R_2 out of 4 and R_2 also shares 3 rules with R_1 but out of 12). These two scenarios obviously do not mean the same thing even if they produce the same similarity index and will be discussed when needed. For now, using this thematic similarity index[2] shows that regulations adopted since 1997 have on average become increasingly similar to each other.

Figure 4.2 depicts this trend and notably shows that despite important yearly variation the average similarity index between new regulations has risen from a bit more than 0.4 to close to 0.6[3]. This is particularly significant as the inclusion of new rules in regulations adopted in the United States and the European Union could have also pushed towards a greater dissimilarity as discussed at greater length below. For the similarity index to rise, it means that the number of similar rules rose faster than the total number of rules included in new or revised versions of previous regulations. It is moreover striking that the four regulations adopted in 1997 that had on average a lower level of similarity (0.41)[4] were created by four American industry associations, while the four regulations created in 2017 that have on average the highest level of similarity (0.65) were created by two American and two European industry associations. More than simply having more similar regulations in each jurisdiction, there thus seems to have been a real convergence between those promoted in the European Union and the United States. This is due

[2]The Jaccard similarity index was also calculated for comparison purposes. As expected, the level of similarity between all texts was lower and reflects the tendency of this index to undervalue the similarity between texts of different lengths. The standard deviation between similarity results using one of these two indexes remained almost identical, indicating that the difference in similarity between two pairs of texts remained constant.

[3]Two years (1998 and 2010) were excluded as they had two or less new regulations adopted.

[4]The already high level of similarity in 1997 can be explained by the fact that all regulations deal with the same issue (data protection) and were shaped by previous interactions, including the negotiation of the OECD guidelines in 1980. As recognized by previous research (Bennett 1992), the trend pushing towards greater convergence analyzed here was thus already underway when the European Data Directive was adopted in 1995.

to the rise in interactions between actors in both jurisdictions after 1995 as chapter 5 will specifically highlight. Although actors in both jurisdictions had already been able to influence each other before 1995, these efforts became increasingly important and numerous afterward.

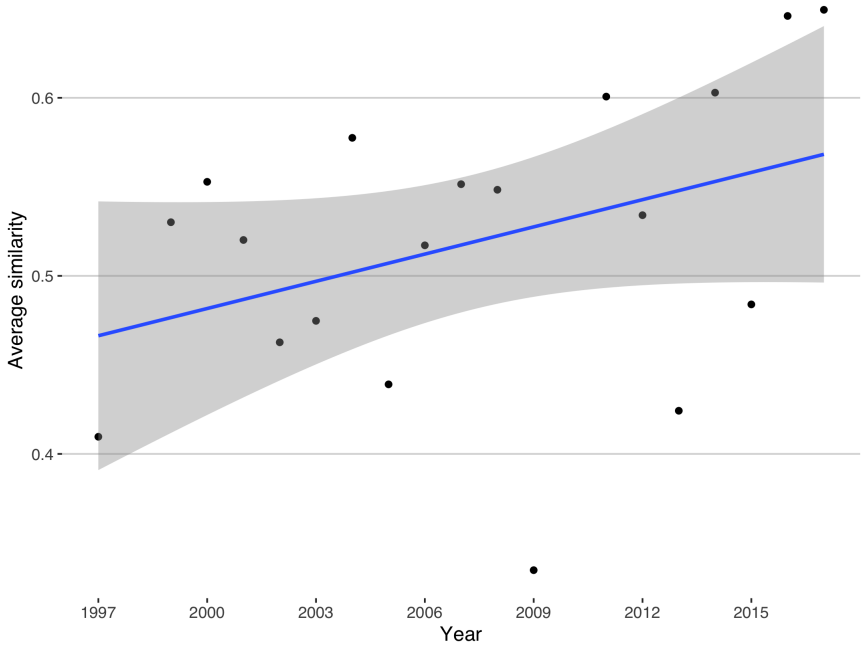

Figure 4.2: Average level of similarity between newly adopted regulations in a given year (1997-2017)

This specific trend towards greater regulatory convergence is in line with the first main process driving the evolution of complex governance systems: the 'exploitation' of preexisting resources (Duit and Galaz 2008; March 1991). As noted in chapter 2, the concept of exploitation describes a strategy of using "old certainties" to solve a given problem (March 1991: 71). Looking into the evolution of trade rules, Jean-Frédéric Morin and his colleagues more specifically define exploitation as the strategy of leveraging "existing capabilities through activities like reproduction, refinement, efficiency selection, and implementation" (2017: 372). When public or private actors start working on adopting a regulation on data protection or revising their previous ones, this means that they start by looking at what currently exists and attempt to use it. This has been repeatedly recognized in interviews done for this research:

> We were aware of other initiatives. We certainly look at best practices in the industry and we didn't want to reinvent the wheel. (Interview E7, done on February 4th, 2019)
>
> We did some pick and choose among what we thought were the best practices. (Interview E11, done on February 6th, 2019)
>
> It is always best if you do not have to reinvent the wheel. Otherwise, you risk to make a lot of mistakes. (Interview E26, done on March 22nd, 2019)
>
> As far as external sources, yes, we don't do this in a vacuum. [While talking about the influence of another organization on the work of his organization, he added:] Frankly, most often they are the ones that copy us. (Interview E32, done on April 25th, 2019)
>
> We believe that in every area there are already practices that we need to map and that will serve us to identify what we want to base ourselves against. We almost never start from nothing. (Interview E40, done on May 14th, 2019)

This tendency to exploit preexisting rules has many benefits. It is first less costly (Morin, Pauwelyn and Hollway 2017). Reinventing the wheel, to paraphrase some of the interviewees, is not an easy task and can be quite time-consuming. Everyone that had to come up with a new idea knows this. Writer's block is one illustration of this in the academic world. As scholars try to be creative, they can easily feel stuck in front of a blank page. It can moreover be risky to continuously try to create new rules that have never been implemented. As one interviewee cited above pointed out, mistakes can be made. New rules can be misunderstood and create unwanted behaviours. Failing to look at what already exists can similarly lead to omission and allow unwanted practices. Exploiting preexisting resources can finally help ensure some form of coherency, which is traditionally highly valued in regulatory systems. As Pauwelyn rightly points out, lawyers are often "critical of fragmentation and decentralization, and intuitively in search of order and central authority" (Pauwelyn 2014). They fear that fragmented systems of rules are prone to create conflicting behaviours and can quickly become chaotic. By making use of prior rules, public and private actors can help provide much-needed certainty and clarity with regards to the rules that need to be followed. As one interviewee pointed out, many private companies in effect find "it is easier to repeat what you do in one [regulatory] system to diminish the legal complexity. [...] It pays to have a unified approach" (Interview E21, done on March 8th, 2019). By supporting some form of order in complex systems of governance, exploitation strategies are, in other words, particularly valuable for private businesses.

Emphasizing the importance of exploitation strategies can easily lead to a sense that politics are not at play. In a way, it could be thought that this simply means that the content of new regulations is simply a function of the institutional environment in place at a specific point in time. This would be an erroneous conclusion. Not all preexisting rules will be equally exploited. The previously observed convergence in effect did not happen randomly and tended to be concentrated around the rules of actors holding specific positions in the system. Understanding around which rules regulators converge thus requires looking into the interactions between different public and private actors, which will be analyzed in chapter 5.

4.5 From Convergence to Divergence: Innovations in the Transatlantic Regulation of Privacy

Next to this tendency towards greater rule convergence, a second but equally important trend has been towards greater divergence. As seen in figure 4.2, new regulations adopted in a year never became perfect copies of each other. Indeed, their thematic similarity index never became equal to one, indicating that no regulations adopted in any given year included all the same rules. This is in part because the process of convergence is incremental and notably depends on the interactions that informed the exploitation strategy of an actor. Depending on with whom they previously worked, they do not have access to the same pool of rules to work from at a specific point in time. It should also be noted that the exploitation process does sometimes imply a selection between competing rules and that not all actors will necessarily make the same choices depending again on their previous interactions. Yet, these lasting discrepancies are also due to the creation of new data protection rules. Over time, regulators do not merely copy what others have done but also tend to innovate.

A 'regulatory innovation' is here understood as the creation of a rule that prescribes or proscribes a behaviour for the first time in the regulatory system. This can both be by further specifying a preexisting principle, like adding a requirement for the type of information that should be part of a private company's privacy policy statement, or creating a rule for an entirely new principle. It is moreover important to note that what is new in a given regulatory system might actually not be in another one. For example, it could be that a data protection rule appearing for the first time in the transatlantic

space already existed in Asia or elsewhere. A new data protection rule could also be used in another policy space (e.g., competition or financial law). Although it might not be the first-ever enunciation of a rule, the act of including it for the first time in a new regulatory system is still considered to be innovative as it generally requires to think of how it could be interpreted to fit in a new geographical space or for a new object of regulation. The choice of where the system boundaries are drawn yet becomes crucial to consider as it clearly affects what will be determined as new or not. In the present case, the exclusion of the European Member States and American federal states from the transatlantic privacy system will sometimes create situations where it could look like the European Commission or the American Federal government created a new rule while it is, in fact, German or Californian regulators that were behind it. As the goal of this research is not to pinpoint the definitive origin of a new rule but to understand broad processes animating the evolution of privacy regulation in the transatlantic space, this is not highly problematic and especially because these would still appear as 'European' or 'American' regulatory innovations. When possible, this additional level of detail will nonetheless be provided.

Figure 4.3 shows the rise of the total number of data protection rules identified in this research. It shows that in 1994, so one year before the adoption of the Data Directive in Europe, there were only 19 rules in existence and being applied by either public or private regulators. These largely represent the rules found in the OECD guidelines and negotiated by the United States and the European Union in 1980. As of 2017, this research identified a total of 71 data protection rules that a privacy regulation can potentially include. None obviously contains all of them. In fact, the GDPR adopted in 2016 has the second-highest number of rules with 48. The only regulation with more rules was created by the Europrise certification program primarily aiming to explain how private companies should implement the GDPR and includes 52 rules. Importantly, few tend to have as much. As the black line on figure 4.3 shows, active public and private regulations today include just over 20 rules on average. This number needs to be considered carefully. Regulations that are active today include some that were adopted in the mid-2000s and included significantly fewer rules than more recent ones that tend to be more comprehensive. In 2017, the four regulations adopted by industry associations, for example, included 38 rules on average.

Interestingly, it can also be observed that the growth of data protection rules appeared to reach a relative plateau in the mid-2000s, which could seem to echo the

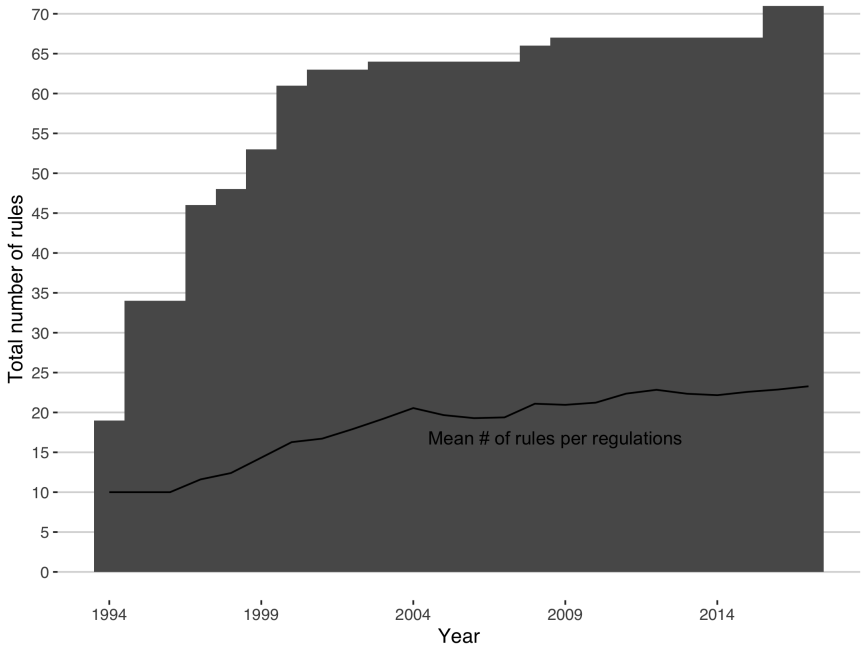

Figure 4.3: Sum of data protection rules promoted by public and private actors in the transatlantic space (1994 - 2017)

same phenomenon occurring in the number of active regulations over time as seen in figure 4.1. Here, it should first be recalled that the manual coding used most certainly does not allow to capture the full breadth of regulatory innovations in the transatlantic privacy system. Self-imposed restrictions in the complexity of the codebook necessarily led to the exclusion of rules that some actors might have created and yet did not stand out in a significant way. This is most likely the case for rules that were not shared by many actors or that worked by further specifying preexisting ones, which are two characteristics that more recent rules are likely to have. As they did not have the same time to be widely shared and will often specify preexisting ones, some were likely omitted. With this caveat in mind, it should not be thought that this slowdown in the creation of new rules is the mere result of the coding limitations of this research and rather reflects the non-linear nature of regulatory innovations. New rules are simply not evenly distributed over time and neither among regulations. Indeed, a few regulations tend to have a lot and many none at all as depicted in figure 4.4. As a single entity, the European Commission has been, and by far, the most innovative actor. The Data Directive and the GDPR together account for 38% of all new data protection rules adopted since 1995

in the transatlantic area. As mentioned above, some of these innovations and especially those in the Data Directive might partly come from regulations previously adopted by European member states. The rest is divided among a relatively small number of public and private regulators.

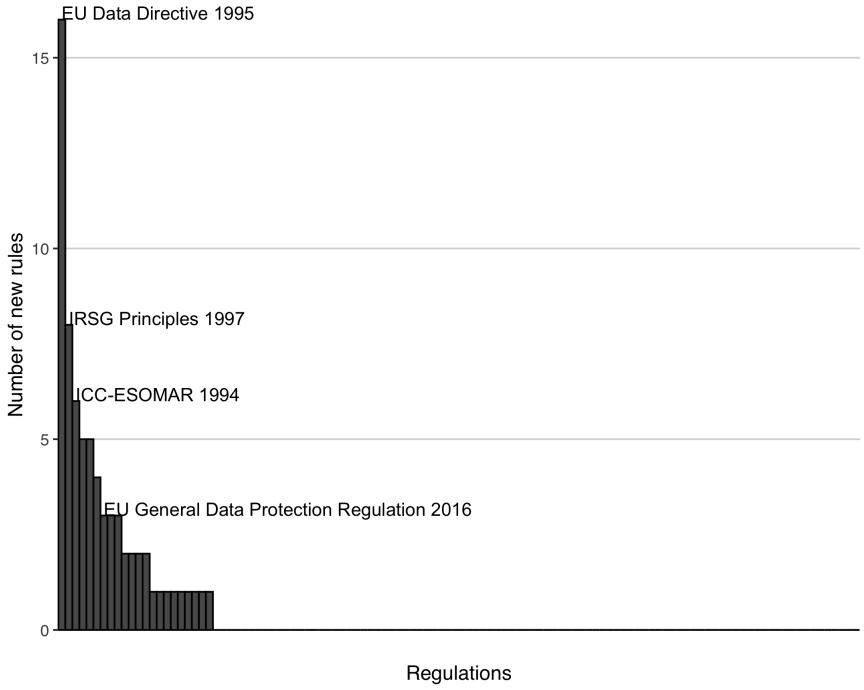

Figure 4.4: Sum of regulatory innovations in public and private regulations

These regulatory innovations importantly follow the second, but equally important process driving the evolution of complex governance systems: the 'exploration' of new strategies (Duit and Galaz 2008; March 1991). Again looking at the evolution of trade rules, Morin and his colleagues define exploration as "efforts to create future capabilities by means of 'search, variation, experimentation, and discovery', and implies venturing into the unknown, introducing chaos to a system" (2017: 372). Over the years, this specific process has often been linked to the work of highly skilled individuals (Morin, Pauwelyn and Hollway 2017: 375). This is particularly evident when looking at popular accounts behind the development of recent technologies in which people like Elon Musk and Steve Jobs are mythologized for their role in the creation of Tesla or the iPhone. The complex system approach that is taken here however pushes us to recast the process of exploration as a social process and system output.

From an observer's viewpoint, it is generally easy to attach the development of an object or idea to a well-known figure rather than trying to understand the complex process that led to its creation. For the innovators, it is also more rewarding to emphasize their own roles rather than detailing the contribution of everyone that might have had an input. Yet, when looking more closely at their breakthroughs or 'eureka' moments we can clearly see that they never happen in a vacuum. Any creators or innovators build on the preexisting work of others. Mariana Mazzucato (2011) forcefully made that point looking at the very case of the iPhone. She importantly highlighted that out of twelve key technical components (e.g.: GPS, Internet, touchscreen, Siri, microprocessors, etc.) making the iPhone what it is today, all had been created by previous research funded by the American government (see also Weiss (2014)). This is yet not specific to the technology sector as any type of novel idea needs to start from something. As Drahos and Braithwaite eloquently put discussing the adoption of public policies in various jurisdictions around the world:

> Creative geniuses tend to be plagiarists, clever at appearing not to be so and deluding themselves that they are not so. The ancients, who appear the most original of all scholars, may only appear so because the work of those they imitated has been destroyed. (2000: 584)

To be clear, the process behind the exploration of new ideas, or in this case new rules, should never be seen as simple plagiarism as that would be closer to the strategy of exploiting existing resources discussed in the previous section. It is, however, a much more *relational* process where innovations emerge from the recombination of preexisting ideas or technical elements. (Carstensen 2015; Pagliari and Wilf 2020). Recent studies on the adoption of patents in the United States precisely show that new ones will almost always make references to multiple preexisting ones (Youn et al. 2015). In other words, innovations, be they technological or regulatory, "are never created from nothing" (Arthur and Polak 2006: 23).

Far from undermining the role of innovators, this relational lens portrays them as working as part of an ecosystem that shapes the development of their new ideas. It requires recasting their work in the environment in which they operate and what information an actor has had access to and integrated into its work over time. When asked what led to the creation of new data protection principles, one interviewee replied: "They came from my head. [These] are based on my 20 years or so of experience in this field" (Interview E37, done on May 14th, 2019). This seemingly trivial sentence

is illuminating and aptly describes the crucial relationship between the innovator and its environment. The interviewee was indeed prone to attribute the innovative elements to his/her own work. As pointed out, it is more than normal for innovators to do so. Retracing the complex process that led them to their result is an uneasy task and it is more rewarding for them to emphasize that they were the central element in it. The second part of the interviewee's answer is, however, precisely hinting at the simple truth that it was also the result of a specific system of interactions and, more precisely, the one in which he/she had evolved for 20 years. Understanding the origins of the data protection rules thus requires recasting them in the context of the system of interactions they evolved in.

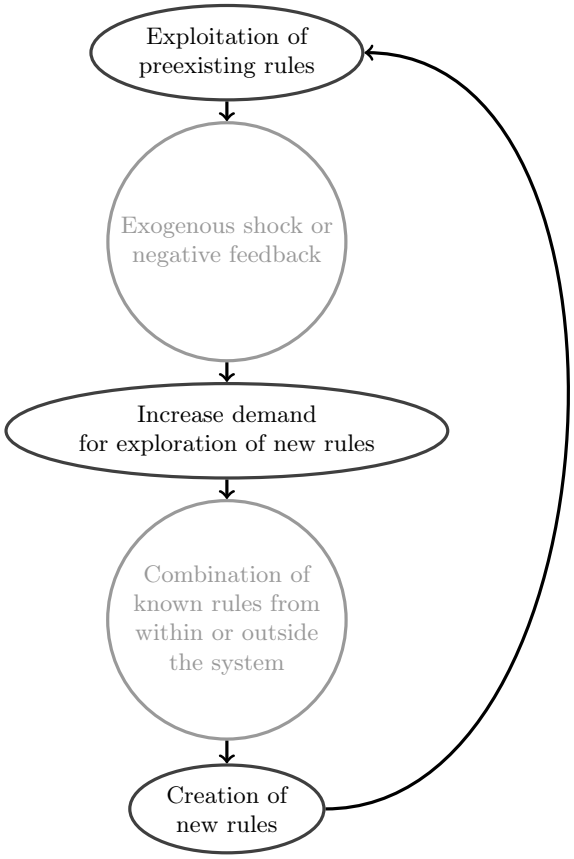

Figure 4.5: Innovation cycle

Figure 4.5 summarizes the relational process behind the exploration of new rules and highlights its circular nature. As discussed in the previous section, actors will most of the time prefer to exploit the rules of actors with which they have interacted when developing their regulations. As one interviewee explicitly recognized:

> [Industry groups and certification providers] could add new obligations, but in practice we don't see that very much. [...] It is just such a big job to decide how to interpret their existing obligations and they do not want to make their jobs harder than it already is. (Interview E26, done on March 22nd, 2019)

In effect, being innovative requires time and resources. It is also a risky endeavour as the actual effects of a new rule can never be entirely known. How it will be interpreted and applied in relation to other rules is never as clear as those that have been promoted by other actors for a relatively long time. Faced with these different costs and risks, many regulators thus often want to 'make their job easier' and exploit what already exists as discussed in the previous section. Exogenous shocks or negative feedback, however, create a demand for new rules from time to time. The former more precisely describes events occurring outside the regulatory system that create a pressure for change (e.g., Snowden's revelations) and the latter events occurring inside the regulatory system that highlight inadequacies in the current rules (e.g., data subject's complaints). Faced with either of these situations, actors will draw on the preexisting set of rules they are aware of and combine them to innovate. By combining two or more preexisting rules, they will more precisely develop new ones. In their work on environmental norms in trade agreements, Morin and his colleagues give the example that the combination of "a norm calling for a broad public participation to the adoption of domestic environmental measures [and] a norm on the regular assessment of the trade agreement's environmental impact [can] give rise to a norm providing for a broad public participation to the impact assessment of the trade agreement" (2017: 378-9).

Importantly, it is understood that the boundaries of a system are open to external influences and that actors can even be part of multiple systems at the same time. Actors that sit on the frontiers of multiple systems indeed have the opportunity to combine ideas coming from the different systems they are part of and can result in giving them a special "arbitrage" role through which they decide what external new ideas come into the regulatory system (Seabrooke and Tsingou 2014). The specific nature and role of actors bridging different systems will not be further investigated here. For this research, it should only be kept in mind that the combination of ideas does not have to only come from inside one regulatory system. As complex systems progressively become more coherent over time as actors exploit known strategies (or similar rules), the inclusion of external ideas can be crucial to innovate. This possibility to draw from external resources was notably made evident in an interviewee's answer to what sources of information had been instrumental in their work to develop new privacy guarantees:

> One was the work of the [Individual Referential Service Group] at the end of the 1990s. [...] The second is really, in the United States, the experience of the stock-market meltdown where security exchange started to require that external non-profit organizations govern the self-regulatory programs and codes of conduct developed by exchanges. (Interview E37, done on May 14th, 2019)

While the former source of inspiration mentioned by the interviewee was the work of an industry organization that developed a code dealing with privacy issues, the latter were changes occurring in the financial sector and not specifically related to privacy. One source was thus from within the privacy regulatory system, while the other was coming from outside. Once created, new rules can finally be exploited by other regulators and serve in the process of forming new ones. In other words, they become the raw materials for other regulatory innovations to emerge.

This relational or systemic view of regulatory innovations should still not be equated to a kind of natural process. Just as the exploitation of preexisting rules, the exploration of new ones is clearly not devoid of politics nor merely driven by the structure of the system. The interests of the regulators are essential to consider in that process, but they need to be looked at and understood in the context of their interactions over time. The fact that the European Commission has been the single most innovative regulator is, for example, due to its constant desire to set a basic framework as seen in chapter 3. At the same time, when and how it ended up promoting regulatory innovations was dependent on its interactions at a specific point in time and what already existed. In other words, its regulatory actions need to be seen as being part of a specific structure that shaped them. Chapter 6 will look deeper into how a specific system's structure interacts with the exploration of new rules by also focusing more on the role of private actors in it.

4.6 Conclusion

Throughout this chapter, I argued that the transatlantic privacy system can be conceptualized as a complex governance system. As opposed to its traditional depiction as being composed of two jurisdictions evolving in isolation up until a formal negotiation or conflict occur every decade or so (Bessette and Haufler 2001; Drezner 2007; Dimitrov et al. 2007; Long and Quek 2002), it emphasizes and takes as a starting point that they have actually been in constant interactions with each other. Even though the European Union

and the United States clearly remain two separate legal entities, their respective public and private regulators have indeed been constantly working together. While not all actors did so equally, all these interactions created bridges between the two jurisdictions and fundamentally changed their respective regulatory processes.

Viewing the United States and the European Union as a complex governance system fundamentally highlights two new dynamics that shaped the evolution of transatlantic data protection rules. There is first a tendency towards greater rule convergence driven by a desire of regulators to exploit preexisting resources and simplify their job. In addition to limiting the investment in time and resources that they have to make when devising new regulations, they also minimize the risks of creating unwanted effects and an increasingly difficult regulatory environment to navigate for private companies. As regulators interact with each other, they quite straightforwardly take inspiration from what their colleagues with whom they had exchanges have previously done. At the same time, there is a second tendency pushing towards greater rule divergence supported by regulators' interest to respond to changes in the real world. By developing new rules, they try to deal with the new information and events that come to challenge how privacy is protected.

Seemingly contradictory, these two processes are what actually keeps the system in a dynamic state of equilibrium (Haas 1982; Morin, Pauwelyn and Hollway 2017; Pauwelyn 2014). While the exploitation of known rules pushes the system towards more order, the exploration of new ones introduces chaos (or diversity) in it. Significantly, it is only possible to simultaneously recognize these two processes because of the multilevel perspective embedded in this research. Indeed, it is by breaking each regulatory system into the public and private regulations constituting them and, in turn, splitting them into their constitutive rules that we can see how these two dynamics operate at the same time. At the level of rules, there is now much more diversity than there used to be. There are nowadays more rules spread across more regulations than ever before. Yet, seen as a whole, all regulations have also never been as close to each other. As these two trends continue to drive the evolution of transatlantic privacy regulation, it should be expected that they will keep themselves in check and impede it from ever becoming a completely fragmented or homogeneous system.

This first set of findings contribute to show the homeorhetic nature of privacy regulation in the transatlantic space. As noted in chapter 2, complex systems tend to evolve following a trajectory (i.e., homeorhesis) rather than going back to a specific state

(i.e., homeostasis). In the present case, new regulations do not tend to move towards the same constant set of data protection principles and rules. As time passes and new connections are formed between public and private regulators, they both tend to explore and exploit new sets of principles and rules. Thomas Oatley similarly defines this as the non-ergodic nature of economic governance, which basically means that "it changes as it moves through time" (Oatley 2019). While most governance scholars would probably recognize that institutions and regulations do not remain the same over their entire lifespan, they would traditionally view them as moving from one state of equilibrium to another. Here, I also distinguish myself from previous studies by pointing out the incremental nature of this process.

The next two chapters will now go deeper into the analysis of these two processes separately and emphasize more clearly the politics behind them. Up to now, the actors' interests in pursuing one of the two strategies behind these two trends (i.e., exploitation and exploration) were highlighted but remained peripheral to the explanation. No difference was moreover drawn between public and private actors. Just discussing these trends in that way can easily leave the unsatisfactory feeling that one of the key questions for political science is left as a blind spot: who benefits from it and how (Kahler 2016: 836)? By focusing on the different forms of interactions between public and private actors as well as their different relations with the broader structure forming this complex governance system, chapter 5 and 6 will highlight how they each attempt to shape the regulation of privacy.

Chapter 5

Transnational Regulatory Networks and Rule Convergence

> *It is remarkable that [the] global profusion of laws has not led to chaotic differences in standards: in fact, it has resulted in a high level of global convergence of standards.*
>
> Graham Greenleaf, 2018

In international privacy debates, convergence is one of the current buzzwords. Speaking at the official events organized by the European Commission back in May 2018 for the launch of the General Data Protection Regulation (GDPR), invited expert Graham Greenleaf cited in epigraph marveled at the "remarkable degree of global convergence" that had been achieved since the European Data Directive had been adopted two decades earlier (2018: 2). One year later, the 41st International Conference of Data Protection and Privacy Commissioners (ICDPPC), a forum connecting 122 privacy and data protection authorities around the world, was specifically organized around the theme *Convergence and Connectivity* as the number of countries with privacy laws reached new heights with the adoption of multiple national laws supposedly modeled after the GDPR like most recently in Nigeria (Chander, Kaminski and McGeveran 2020: 3). While not new (Bennett 1992, 2010), this continuing trend towards greater regulatory convergence

as the regulation of privacy becomes more comprehensive and detailed is truly noteworthy.

Notwithstanding, not everyone embraces the concept of convergence with the same enthusiasm. In the United States, it is most notably viewed as a euphemism for what really is a strategy of regulatory export by the European Union. As one American interviewee quite bluntly argued, "the EU tries to export its framework globally, which I found funny as they only represent 1/4 of the world's population, but, OK, they used to be the centre of the world" (Interview E27, done on April 4th, 2019). As opposed to this, what American regulators often try to promote is the concept of 'interoperability' as noted in chapter 3. The latter supports the use of accountability mechanisms that would "bridge approaches across disparate regulatory systems, by allowing countries to pursue common data protection objectives through very different – but equally reliable – means" (Bennett 2010: 13). While convergence means the adoption of increasingly similar privacy rules and standards, this promotes a form of regulatory coordination where different regulatory frameworks "recognize or accommodate" each other but do not necessarily become closer over time (Drezner 2007: 11). This concept is now at the heart of the Asia-Pacific Economic Cooperation (APEC) Privacy Framework negotiated by the United States in 2015 and was partially incorporated by the European Union in the GDPR. As also discussed in conclusion to chapter 3, the decision to consider private codes of conduct and certification programs as adequate means to transfer personal data across jurisdiction interestingly echoes the American support for interoperability mechanisms rather than the process towards greater legal convergence that adequacy decisions are supposed to support.

In this respect, the finding presented in chapter 4 that privacy regulations adopted in the transatlantic area have actually converged towards one another is even more significant. As this process of convergence was driven by industry self-regulations, it moreover highlights that private forms of regulation have actually ensured that the American and European privacy systems evolved as a whole rather than making them merely 'interoperable'. In the remainder of this chapter, I build on this insight and argue that industry associations acted as pathways for the exchange of data protection rules between both jurisdictions in the two decades following the adoption of the European Data Directive. While supporting the broader adoption of rules originally devised by themselves, they basically became a "new institutional avenue to diffuse public rules" (Green and Auld 2017: 261; see also Turkina and Postnikov 2012, 2014). In doing so, they ended up ex-

tending the influence of public authorities to areas where they would not have normally enjoyed any. As the European Union was particularly active in devising new rules and engaging with private actors, this more often than not meant that European rules were diffused and became the *de facto* standard around which public and private regulators in the transatlantic area converged, a result that the American government had precisely hoped to escape by working with private actors. At the same time, this process was not as unilateral as the recent literature on the Brussels' effect maintained (Bradford 2012, 2020) and, as it will be shown, the United States was never a simple "receiver" or "importer" of European rules. Rules pertaining to the protection of children, the use of passive methods of data collection, and the education of individuals that were first enunciated in the United States have notably made their way in Europe.

In addition to answering recent calls to give more attention to the interactions between public and private forms of authority (Eberlein et al. 2014; Gulbrandsen 2014; Green and Auld 2017) and providing a more nuanced understanding of how the regulation of privacy has evolved than recent work prone to straightforwardly claim Europe's "success in the marketplace of idea" (Schwartz 2019: 146), this will also provide a more in-depth description of the process of convergence by comparing the actual content of privacy regulations adopted in both jurisdictions. In line with the multilevel perspective adopted in this research, convergence will be evaluated based on the content of the rules found in each of them. Up to now, previous studies tended to use the simple rise in the global number of privacy regulations adopted around the world and at most the similarity between their broad principles as a proof of convergence (Bennett 1992, 2010; Greenleaf 2018). By going one step further and breaking down regulations in their constitutive rules, I show more clearly when exactly convergence occurs or not. I am indeed able to highlight that when two regulations share a common principle they may not have really converged.

The next section begins by explaining how the exploitation strategy used by private actors was both driven by hierarchical and network relations, and how the latter importantly ended up reinforcing public authority. It moreover details how a network approach will be used to empirically locate when and how regulatory convergence occurred in the transatlantic regulation of privacy since the adoption of the European Data Directive in 1995. The following sections go on applying this analytical method to four successive time periods ending up just before the European Commission started working on the drafting of the GDPR.

5.1 Public Authority and Private Networks

If anarchy is the traditional starting point in world politics, hierarchy is for national politics. State agencies are in effect considered to have the legal authority to arbitrate any potential conflict of laws and to be the source of all legal obligations that private actors have to respect. In the end, what matters are the principles that national governments have developed and how they are applied. Private rules linearly follow these principles and can be superseded by them at any time. In legal theory, this is famously modeled by Kelsen's pyramid of norms according to which clear relations of superiority or subordination exist between all sources of authority (Benyekhelef 2015: 30). Figure 5.1 depicts it graphically and broadly presents how different norms are hierarchically related. Significantly, not all states would necessarily have the same hierarchy. It is notably contentious where international law fits in it. For most international legal scholars, it would come on top of national laws. Yet, some constitutions only foresee it having an effect after being incorporated in national law in accordance with the constitution and would thus see it coming second in the pyramid presented below. One recent example of such debates appeared when the German constitutional court rejected a previous decision from the European Court of Justice and found that the European Central Bank had exceeded its authority by allowing bond purchases (Karnitschnig 2020). For this research, it is sufficient to point out that industry self-regulations would be seen as a contractual form of law and almost always fall below legal rules in figure 5.1.

Just as the anarchic view of international relations has long been debated (Lake 1996; Onuf and Klink 1989; Zarakol 2017), the pyramid model of norms can, however, be questioned. In line with the literature on private authority reviewed in chapter 2 (Avant, Finnemore and Sell 2010; Braithwaite and Drahos 2000; Cutler, Haufler and Porter 1999; Graz and Nölke 2008; Mattli and Woods 2009), this research indeed holds that principles and rules do not have to follow a simple top-down process nor directly flow from state authority. Private rules can emerge without being directly related to public laws and even end up influencing them. In the absence of clear relations of superiority or subordination, these different sources of law can be conceived of being part of a network of interactions (Benyekhelef 2015: 693).

Adopting a network lens importantly does not mean that all legal sources are equally influential. The network literature has for long pointed out that not all actors are equal even though networks tend to be viewed as flattened structures (Castells 2004).

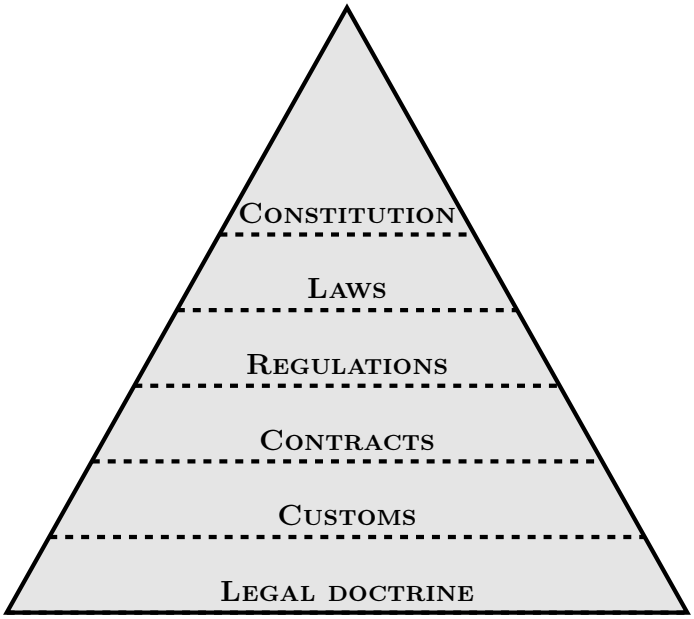

Figure 5.1: Kelsen's pyramid of norms

In networks, influence is understood as deriving from an actor's particular position and set of relations (Hafner-Burton, Kahler and Montgomery 2009). Those with more ties or ties with specific actors are most notably assumed to have more potent resources to draw from to achieve their aims (Carpenter 2011; Puig 2014; Seabrooke and Tsingou 2014). This represents a social form of power where an actor's rules are not adopted by another through direct imposition but freely taken up by actors interacting with each other. This broadly fits with the definition of private authority that assumes influence to be based on consent rather than through coercion (Green 2013*b*: 27-8). In the context of this research, this means that actors will tend to exploit the rules of those with whom they had direct interactions more than those with whom they had no previous contact. Concomitantly, actors with more relations or linking different groups of actors will tend to have more influence over the evolution of data protection rules.

At their core, the pyramid and network models thus represent two modes of organization in which power and influence are expressed differently. While the former focuses on a 'command-type' of power, the latter emphasizes a more 'co-optive' or social-type of power (Lavenex 2014: 889, see also Barnett and Duvall 2005). Unsurprisingly, the network one has been more usual in the international realm as formal hierarchies are often considered to be absent. Meanwhile, the traditional recognition of the existence of such

hierarchies in national legal orders has made the pyramid model the choice to study it. Putting aside the question that these categorizations represent ideal-types that have never been absolute, globalization processes have made them increasingly difficult to separate (Benyekhelef 2015; Davies 2010; Sparke 2013). National legal systems are nowadays permeated by transnational networks creating their own sets of rules (Braithwaite and Drahos 2000). Far from being free of hierarchies, though, public and private actors populating these networks are increasingly embedded in multiple hierarchical relations, and this is also true for all those making the transatlantic regulation of privacy a complex governance system. Exploitation strategies behind the regulatory convergence previously observed were indeed shaped by these two types of interactions between public and private regulators. From here onward, I will specifically emphasize how these two types of interactions came together to shape the choice of the rules that industry associations ended up exploiting and how it sometimes supported the diffusion of public rules.

As shown in figure 5.2, industry associations have progressively formed a collaboration network transcending the jurisdictional boundaries of the United States and the European Union since 1997. The nodes represent industry associations for which a regulation including at least one data protection rule was found (see section 4.2). Ties indicate when two have officially worked together to develop data protection rules, either through shared membership in another organization or collaboration on a specific project. Ties were moreover assumed to last over the years, except when it was specifically indicated that two associations had stopped collaborating. This could notably be because one association disappeared or stopped being an active member of the other. This data was collected from publicly available information found on the website of all industry associations[1].

As it can easily be seen, this network became denser over time. In social network analysis, density represents the proportion of existing ties compared to all potential ones and can be summarized in an index going from 0 (network with no connections) to 1 (fully connected network) (Wasserman and Faust 1994: 101). In the present case, the network densities were respectively 0.06 in 1997 and 0.1 in 2017. The relatively small difference should be understood in light of the different sizes of both networks. As new industry associations joined the network, the number of potential connections rose exponentially, which would generally tend to push towards a lower network density. Previous studies

[1] As for the collection of all data protection regulations used for this study, the Internet archive accessible with the Wayback Machine tool was used to access the websites of all organizations as far back as 1997.

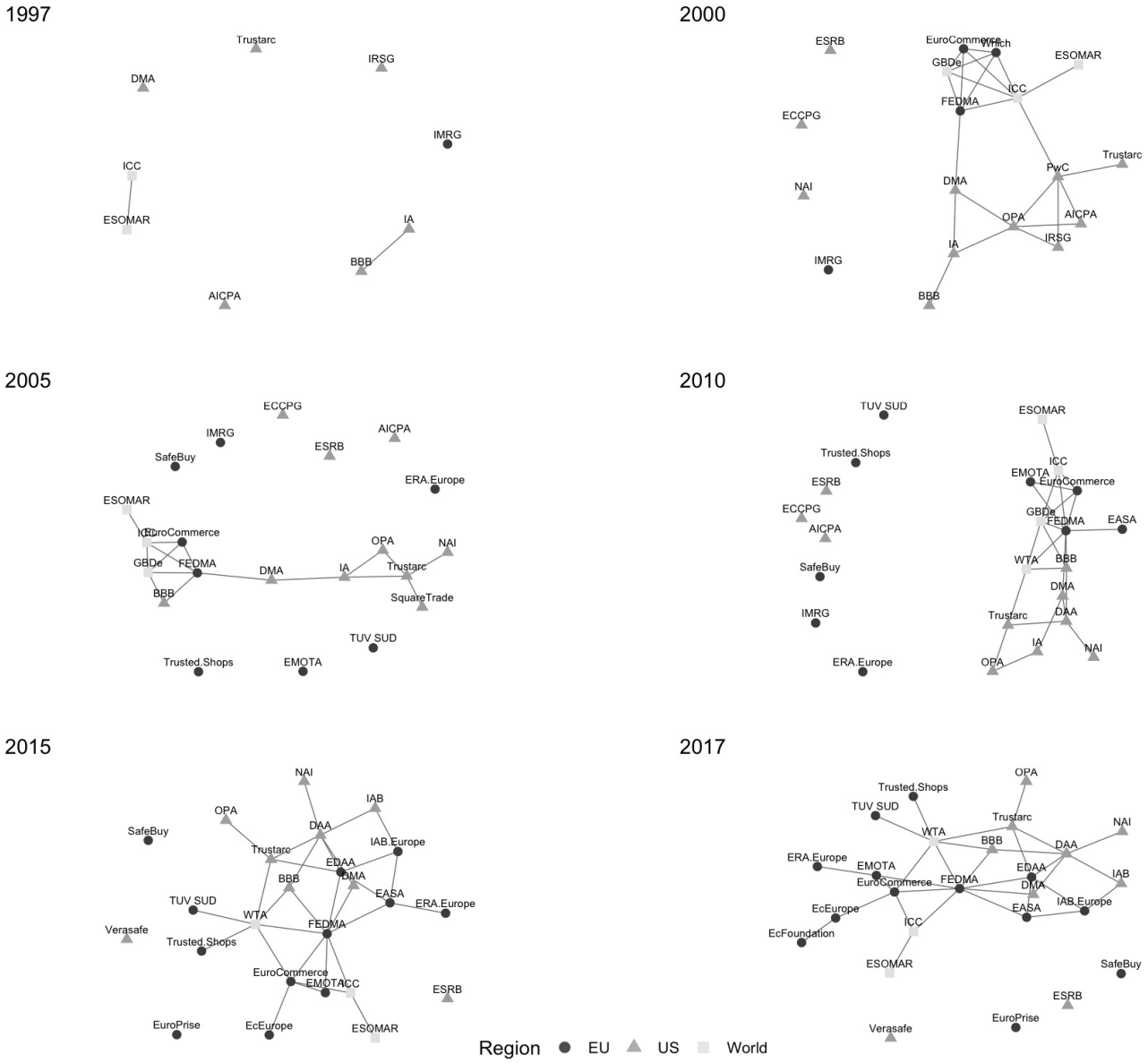

Figure 5.2: The evolution of network of interactions between industry associations (1997 - 2017)

indeed found that the density of many networks tended to become lower over time as new actors joined it (Cunningham, Everton and Murray 2016: 283). The increase is thus more significant than it may seem and indicates that there have proportionally been more new interactions than new actors joining the network over these twenty years.

At the same time, a density of 0.1 in 2017 remains relatively low and reflects the sometimes competitive nature of the interactions between industry associations. It is not uncommon to find that industry associations looked at in this research fight for the same members. As one interviewee stated, there "is always competition. [...] It is sort of like the empires of the antiquities. Everybody claims the same things. We fight for the same members" (Interview E21, done on March 8th, 2019). Another interviewee was also critical of the tendency of another organization to copy their "work for free to monetize it" (Interview E32, done on April 25th, 2019). This, in turn, limited the propensity of these organizations to work with each other as they found themselves selling similar services to the same companies. While this particular relation indeed appears to have had some limitation effects on exchanges between private associations, it has not entirely impeded it. In the end, the tendency of private associations to focus their activities on a specific sector (i.e., marketing, entertainment, e-commerce, etc.) made it easier for most of them to collaborate. By establishing a 'niche' for their regulatory activities, private associations clearly hoped to fend off themselves from direct competition (Abbott, Green and Keohane 2016). Public agencies also sometimes helped private actors to work together by organizing events and even funding their activities as it will be discussed at greater length in chapter 6.

Through these network interactions, industry associations importantly learned and socialized themselves to the rules available and that they could potentially exploit (Auld 2014, Braithwaite and Drahos 2000; more specifically on institutional isomorphism see DiMaggio and Powell 1983). As one interviewee held, "there is always a lot of cross-fertilization when [joint projects] like this happens" (Interview E36, done on May 10th, 2019). Central actors in this network thereby ended up having a greater influence on the evolution of the system. While they could not force others to adopt their rules, they had more opportunities to make them broadly adopted. European associations working with American ones and vice-versa moreover had the very particular capacity to act as bridges between both jurisdictions. Even though their relationships can sometimes be weaker as they may have less regular interactions than with their national counterparts, these specific ties can be particularly influential as they connect different groups of actors.

This echoes the famous claim of network theorist Mark Granovetter (1973) that weak ties can matter even more than strong ties. In his work, he more precisely showed that ties with distant or old friends were often more useful for individuals looking for work as they allowed them to learn about opportunities outside of their close circle of friends. In the present case, industry associations with links to their counterparts in other jurisdictions can play a key role in the convergence previously observed due to their special position, and even though their interactions might not be as strong as with associations active in their jurisdiction of origin.

These private interactions importantly still operated in the "shadow of hierarchy" (Gulbrandsen 2014: 76; see also Newman and Bach 2004, Abbott and Snidal 2009*b* and Graz and Nölke 2008). As one interviewee clearly noted: "When we prepare [our] criteria, we always start with the law" (Interview E19, done on March 5th, 2019). This statement may seem more obvious than it actually is. When industry associations create rules, they certainly cannot contradict what public laws require. Yet, they could also create additional or different rules to the legal obligations their members already have to respect as explained when reviewing the literature on private authority in chapter 2 (see section 2.3). The majority of interviewees for this research nonetheless indicated that the main purpose of their work was to help their members be compliant with national laws, even in the United States where there is not as of now a comprehensive law covering both the public and private sectors.

Various reasons explain this choice. In line with the exploitation strategy, it is less costly and risky to build industry self-regulations using the rules already developed by public actors. Instead of having to create a whole new set of rules that could create a lot of confusion, it is in effect easier to say to their members that companies implementing their rules will be compliant with the law in a given jurisdiction. This provides them with legitimacy and a clear selling point to their potential users (Green 2013*a*; Gulbrandsen 2014). As such, many industry self-regulations are specifically built to demonstrate compliance with national laws. Finally, it must be remembered that private companies pay to say that they respect these industry self-regulations, either directly or through their membership fees. This evidently limits the incentive of these industry associations to move away from already existing legal requirements as they have to find a balance between creating strict requirements and making their services attractive to their members. As one interviewee noted:

> I think that we have developed requirements that go beyond what is required by the law, but our ability to do so is limited by the fact that at the end of the day it is a voluntary program. Not only voluntary, but that companies pay to use. There is thus a limit to what we can ask. [...] It is really important to keep in mind, and it is probably true for any voluntary and paid program, the impact can only be so great and you can only impact the companies that decide to join the program. The more you add requirements that go beyond and above the law the harder you make it to join. This is particularly the case when your competitors do not necessarily recommend them. (Interview E34, done on May 6th, 2019)

In that process, industry associations are evidently not limited to the law of the jurisdiction where they are primarily active. They can combine different sources of law to help their members respect multiple legal frameworks at the same time. Following that line of thought, one interviewee noted that regulation put forward by his organization was "a mix based on a whole variety of things, like the fair information practices, OECD guidelines, global best practices, APEC and others" (Interview E31, done on April 24th, 2019). This is interestingly what the literature on the market power of Europe (Damro 2015) or Brussels' effect (Bradford 2012, 2020) assumes will happen when it argues that companies will find it easier to align themselves with the most stringent rules of jurisdictions with large markets. The previous list of public regulations named by the interviewee yet strikingly misses the ones these theories would have predicted to be included: the European Data Directive or the GDPR.

In line with the broadly held view that the European Union is currently winning privacy debates (Schwartz 2019), most interviewees, including those representing American organizations, in fact mentioned the global influence of European rules in their work. Asked what was the most important regulatory change to have occurred in recent years, almost all also pointed out the adoption of the GDPR in Europe. At the same time, many representatives from non-European associations also maintained that they specifically did not aim to integrate European rules in their regulatory frameworks as they were seen as being too restrictive and unnecessary cumbersome for their members that might not have any ties with Europe. As the interviewee cited above stated, "[w]e try to limit our program to a specific [legal] framework as we don't want to make compliance more difficult for a company that doesn't need it" (Interview E31, done on April 24th, 2019). Interestingly, this phenomenon is not limited to the European Union. Another interviewee specifically indicated that they were both careful of not integrating too many rules coming from Europe as well as the United States:

> We need to mention a lot of the GDPR's content, but then we are getting criticized in other markets. We have to be careful not to be too US or EU. [...] Otherwise, it will be seen as a tool to bring GDPR in other countries. [...] It was the same for the US with COPPA [i.e., the American law on the protection of children privacy online]. (Interview E25, done on March 15th, 2019)

Some privacy commentators have also pointed out that instead of including European rules in their privacy practices, large private companies sometimes prefer to create different categories of users with different data protection guarantees. This is the case of Microsoft and its online service LinkedIn that now indicates that users outside of "designated countries" (i.e., Europe) can be subject to different data collection practices (LinkedIn 2020)[2]. It is thus not a given that either industry associations or private companies will exploit rules emanating from a jurisdiction where they do not find themselves in a hierarchical relation with its public agencies. This directly contradicts the 'Brussels effects' argument that considers that non-divisiblity of a regulatory object (i.e., personal data in this case) as a necessary condition for it to happen.

The transatlantic network relations depicted in figure 5.2 can here supplement and, in a way, further extend these hierarchical relations. As mentioned above, European and American industry associations that have direct interactions with each other can socialize each other to the respective regulations that they promote and exploit rules from their respective primary jurisdiction. In other words, their specific position in the network structure, and concomitant social influence, come to serve public authorities by helping their rules be taken up outside of their original legal realm. In addition, industry associations can amplify the impact of internationally agreed agreements. Both the Safe Harbor and Privacy Shield Agreements negotiated between the United States and the European Union to allow the transfer of personal information between the two jurisdictions foresee that companies will self-certify their compliance with their data protection rules. Originally intended to be limited to companies that needed to move personal data from Europe to the United States, industry associations that exploited these rules in their self-regulations also had the opportunity to more broadly promote these rules in the United States through their own networks. As stated by one interviewee, this all means that through these interactions, companies can end up following "higher requirements than what is foreseen in their national law, which in turn help ensure a consistent application of data protection globally" (Interview E22, done on March 11th,

[2]This was originally identified by Wolfie Christl in a Twitter post on the day that LinkedIn updated its privacy policy (January 6th, 2020).

2019). Significantly, and as will be discussed below, public authority can also play a role in the shaping of the network structure and creation of these bridges. Governments can notably support the work of private organizations working together through financial or administrative means (Gulbrandsen 2014).

This tendency to exploit pre-existing rules relates and yet differs in several ways to the mechanisms identified in the diffusion literature reviewed in chapter 2. It first emphasizes the importance of direct interactions as opposed to indirect ones based on market or social power (Lavenex 2014). Instead of focusing on how a specific socio-economic environment can lead actors to adopt a particular behaviour, it emphasizes the role of direct network or hierarchical relations. This helps avoid the easy slip towards a form of "passive voice functionalism" (Kahler 2016: 828) often intrinsic to market explanations reifying the *natural* logic of the system and making ideas and interests of actors largely irrelevant. Both network and hierarchical relations are moreover viewed as operating together rather than separately. While recognizing the crucial role that public authority plays, it does not see it as linearly imposing its preferences. It can attempt to influence and steer the content of industry self-regulations and how rules move across jurisdictions, but this is partly contingent on how these industry associations decide to work together. Private actors are viewed as having real agency and the capacity to influence the process of rule convergence by both promoting the rules that they develop and the ones of public authorities. Finally, the process of exploitation is not understood as being constant over time. Actors having influence will change as new relations are formed.

Following the argument in chapter 4 that the transatlantic space can be conceived as a complex governance system, this transnational explanation attempts to give a richer representation of how rules have converged. At the same time, it must be reemphasized that this remains a simplification. Not all interactions are hereafter considered. Trans-governmental relations and interactions between individuals are most notably excluded. Various interviewees (e.g., E17, E31, E35) discussed the importance of the International Association of Privacy Professionals (IAPP) in their work and how they sometimes shared their regulatory approaches there. Again, complexity theory does not aim to build a model the replicates the actual world but to emphasize phenomena emerging from the interactions of multiple heterogeneous and interconnected elements making up a system[3].

[3]See section 2.5 on this point.

In this specific case, the emergent phenomenon is the process of exploitation driven by the interactions between public and private actors causing this regulatory convergence.

To demonstrate how private networks have supported the convergence of data protection rules found in the American and European models as well as those developed by industry associations, the next sections will proceed with a careful historical comparison of the content of industry self-regulations adopted in the European Union and the United States with an analysis of the evolution of the network structure. Cases of specific rules adopted following new or repeated interactions between two industry associations will be used as confirmatory evidence of this process of exploitation. As previously mentioned, ties will illustrate situations where two industry associations have officially worked together to develop data protection rules, either through shared membership or specific projects. Information on ties was collected as it was to prepare figure 5.2 above. Time will finally be used "to dissociate [it] from homophily" (Gilardi 2012: 457). When using network data to explain specific outcomes, one needs to be particularly careful about the meaning of the observed relations. Instead of representing a relation of influence ('exploitation'), a tie between two actors can very simply show that two actors had similar preferences in the first place ('homophily'). To account for this, the content of the regulations of two collaborating industry associations will be compared before and after they had their first interactions. Changes occurring after their first direct interactions took place will be taken as a sign of exploitation rather than homophily. When possible, interview data and information from official reports will be supplemented to make the argument stronger.

5.2 Limited Convergence After the Data Directive

From 1995 to 2000, seven private associations put forward a self-regulation dealing with privacy issues in the United States[4]. Next to the sectoral laws adopted at the American federal level and introduced in chapter 3, these contributed to set out the data protection rules in various industries and included: the American Institute of Certified Public Accountants' (AICPA) Webtrust program; the BetterBusinessBureau's (BBB) Online privacy program; the Direct Marketing Association's (DMA) Ethical marketing guidelines; the Internet Alliance's (IA) Code of conduct for online businesses; the Individual

[4]See section 3.3 and 3.5 for a reminder of how these organizations were found as well as those discussed further on in this chapter.

Reference Services Group's (IRSG) Privacy principles; the Online Privacy Alliance's Privacy guidelines; and TrustArc's (then-called TRUSTe) Privacy program. A comparison of all these self-regulations with the European and American models of rules is reported in table 5.1, except for TrustArc as it was impossible to find the text of their self-regulation before 2000. The revised versions of the AICPA Webstrut program in 1999 and IA code in 1998 were included to show the early dynamic nature of these regulations. The OECD guidelines of 1980 were again added as a reference point. Each cell then indicates the number of rules that each industry self-regulation had in common over the total number of rules that they included. The total number of rules present in the OECD guidelines, the European Data Directive, and the FTC guidelines are specified below each one to highlight the actual 'pool' of rules that they could have potentially tapped in. In parenthesis, the thematic similarity index[5] shows the average proportion of rules that two regulations have compared to their respective total number of rules[6].

Table 5.1: Comparison of Number of Shared Rules Between Early Industry Self-Regulation and American and European Rule Models*

	OECD Privacy Guidelines (1980) - 13 Potential Rules	European Data Directive (1995) - 30 Potential Rules	FTC Fair Information Practice Principles (1998) - 20 Potential Rules
AICPA Webtrust 1997	2/8 (0.150)	4/8 (0.32)	4/8 (0.35)
AICPA Webtrust 1999	9/18 (0.60)	13/18 (0.60)	11/18 (0.58)
BBBOnline Privacy Program	8/29 (0.44)	15/29 (0.53)	16/29 (0.68)**
DMA Ethical Guidelines 1997	2/5 (0.158)	4/5 (0.47)	2/5 (0.155)
IA Code 1997	5/14 (0.38)	8/14 (0.45)	12/14 (0.76)**
IA Code 1998	6/18 (0.40)	9/18 (0.42)	14/18 (0.76)**
IRSG Principles 1997	9/23 (0.55)	13/23 (0.53)	13/23 (0.62)**
OPA Guidelines 1999	7/13 (0.54)	11/13 (0.62)**	11/13 (0.70)**

* Thematic similarity index shown in parenthesis; ** Similarity index higher than 0.60

Looking at table 5.1 reveals several things. First, there was an important diversity in the content of these regulations. Some contain very few rules and as little as five for the ethical marketing guidelines adopted in 1997 by the DMA, while others were already more comprehensive like the BBBOnline privacy program or the privacy principles of the IRSG that had even more rules than the FTC guidelines. This broadly reflects the early nature of these self-regulatory attempts and that they were still trying to define what should be acceptable data practices. None is moreover a perfect reflection of the

[5]See section 4.4 for a reminder on how this similarity index is calculated.

[6]In practice, the AICPA Webtrust 1997 similarity index of 0.15 with the OECD guidelines is found by doing the following calculus: 0.5*(2/8 + 2/13).

American or European set of rules, nor even of the OECD guidelines that were adopted close to twenty years before and were supposed to represent a broad consensus. This again points to the fact that many were still experimenting with their codes and were not following one clear model yet. That being said, they generally tend to be closer to the American model as shown by the IA code of conduct, the IRSG principles, and the OPA guidelines having a similarity index with the FTC guidelines of more than 0.6.

This number should be carefully considered and does not mean that they are more than 60% identical. Again, this similarity index calculates the average proportion of rules that two regulations share compared to their respective total number of rules. The OPA guidelines thus have a higher similarity index with the FTC guidelines than with the Data Directive even though they have the same amount of shared rules. This importantly reflects the fact that it could have taken up more rules if it had really embraced the European model rather than the American one. In other words, the index gives weight to the size of the pool of potential rules that a regulation could have exploited. The generally high level of similarity is finally caused by the preexistence of a relatively consensual set of rules. Almost all rules that these industry self-regulations have in common with the European ones are in effect the same ones that they share with the OECD and FTC guidelines. This shows that although none perfectly took on-board the OECD guidelines, they generally tended to use a similar starting point to devise the content of their self-regulation.

At the same time, they practically never contained the new rules introduced in the Data Directive that truly distinguished the European model. None notably included a rule requiring personal data not to be kept for longer than necessary or the requirement to ask for the explicit consent of individuals when dealing with sensitive data. Neither did any included rules specifying that the processing of personal data needs to be fair and in accordance with the law, which has long been a staple characteristic of the European model that comes from their idea that the processing of personal data needs to have a legal basis (Schwartz and Peifer 2017: 127). Only the revision of the AICPA Webtrust program in 1999 moreover included a specification that individuals could ask for wrongful data to be deleted. Yet, it did not add the obligation for companies to communicate any correction or deletion of personal data that they may have shared with third parties. One interesting exception is the inclusion by the AICPA Webtrust program, BBBOnline privacy program, DMA ethical guidelines, and IA code of conduct of rules dealing with the disclosure of personal data to third parties, which were not part of the OECD or

FTC guidelines. This actually explains why the DMA ethical guidelines of 1997 have a much higher similarity index with the European Directive than the other two. Out of the only 5 data protection rules that it had, it included two on the exchange of personal data that were in the Data Directive. One was more specifically requiring private companies to obtain individuals' consent before sharing their personal data with third parties. The other relatedly stated that individuals must be informed of the fact that their personal data may be shared. Far from representing the exploitation of the 'European' rules, though, it actually highlights the influence of American private associations in the development of data protection rules in Europe through private networks before the time period for this research even started.

Since the early 70s, the DMA has operated what is known as a 'suppression list' or 'Robinson list' offering the possibility for individuals to refuse that their personal data be used and shared for direct marketing purposes (Direct Marketing Association 2020; Tempest 2007). Over the years, this practice also became increasingly used in Europe and was even included in the law of some European countries before finally being added to the Data Directive (Art. 14 (b)). Retracing the exact pathway through which these rules on data transfer moved across both jurisdictions is outside the scope of this research as it was before the time period looked at for this research. It is nevertheless significant that private actors in the United States and the European Union have been influencing their regulatory practices before the European Data Directive was even adopted. As a matter of fact, the oldest industry self-regulation dealing with privacy issues found for this research, which is the 1994 code of marketing and social research practice jointly adopted by the International Chamber of Commerce (ICC) and the European Society for Opinion and Marketing Research (ESOMAR), included the same provision. Collaboration between direct marketing associations in both jurisdictions was moreover formalized with the adoption of an agreement on the use of suppression list in 1996 by the International Federation of Direct Marketing Associations (Tempest 2007: 136).

With regards to the self-regulations of the AICPA, BBB, and IA, it is more difficult to be sure if their inclusion of rules on data disclosure was influenced by the Data directive. As they were not specifically marketing associations, it is not clear if it is their previous knowledge of the work of marketing associations or pressure from the European Data Directive that led them to add these rules on disclosure. At the same time, the language used in their self-regulation is very similar to the one used by the DMA. The IA code of conduct even talked of a 'suppression' mechanism. The BBB had also been operating a

self-regulatory program on children advertising developed with an advertising association for years, which specifically included rules on the disclosure of personal data to third parties (Aftab and Savitt 1999: 7). Perhaps more importantly, though, the AICPA and IA's self-regulations did not include other rules found in the European Directive on the disclosure of personal data. The BBB was the sole exception in that respect and included a rule also found in the European Directive requiring companies to ensure subcontractors with whom they share personal do not process it for other purposes than those for which it is shared with them.

In sum, all available industry self-regulations adopted before 2000 in the United States did not show any real sign of convergence with the rules promoted in Europe. Even codes that were revised or adopted after 1998, the year the Data Directive came into force, did not include rules that particularly distinguished the European model from the American one. Overall, they were even lighter than the FTC guidelines as they almost all included significantly fewer rules than the latter. Only the BBBOnline privacy program and the IRSG privacy principles had a more comprehensive set of data protection rules. It is actually noteworthy that they were closely tied to the work of the FTC. In the first case, the BBB was asked by the American administration to develop an online privacy code. It had been identified as a good candidate because of its previous experience in building a code for online advertising to children. The latter had itself been instrumental to the FTC's work leading to the adoption of the law on the protection of children's privacy online in the United States (Hertzel 2000: 437). In the second, the ISRG privacy principles were presented to the FTC at a workshop in 1997 and were explicitly mentioned in its guidelines as a good example of self-regulation (Gellman and Dixon 2016: 55). The main discrepancy between the two interestingly came from the absence of rules on the protection of children's personal data as they were adopted by the American government one year after the IRSG principles were devised. This also explains their absence in other self-regulation adopted before 1998 and supports the idea that all of them were even closer to the American sets of rules promoted by the American federal agencies when they were devised than the similarity index shown above suggests. The BBBOnline privacy program and IRSG principles otherwise included a couple of more detailed rules than the FTC guidelines, but they overall remained largely aligned with it.

This decision of private actors in the United States to mostly exploit rules promoted by American public authorities can be partly explained by the fact that the

European Data Directive only entered into force in 1998. The incentive for industry associations to quickly harmonize their rules with the European ones was not necessarily as strong as it would become in the following years. It is worthwhile to remember that the members of these private associations are not all large corporations with the financial means that we today associate with companies like Facebook or Google. These might thus have preferred to keep their compliance costs down, especially as some of their members did not deal with personal data from Europe at all. It is still noteworthy that not even one engaged with the European rules, which were at the time seen as a significant disruption in the regulation of privacy worldwide. Studies published in the early 2000s in fact repeatedly emphasized the importance of data flows between the United States and the European Union (Farrell 2003; Kobrin 2004; Long and Quek 2002). It could thus have been thought that industry associations developing code in the United States could have been more interested in helping their members to prepare for it, even without the legal obligation to do so.

This lack of exploitation of European rules yet also reflects the lack of counterparts for American private actors to interact with. Although the Data Directive specifically aimed at creating one harmonized set of rules for all its member states, significant discrepancies remained in its application long after it was adopted (Bamberger and Mulligan 2015: 9; see also Korff 2002) and this was especially true in the early days of the Directive. Some countries, for example, continued to rely on different forms of consent for the use of personal data for direct marketing (Tempest 2007). Faced with still diverging national systems and a lot of uncertainty in the application of the Directive, American industry associations did not always know what they should advise their members to do depending on where the personal data was precisely coming from in Europe. Instead of embracing the rules in the Data Directive, they appeared to adopt a wait and see strategy. This was similarly true for associations in Europe. As one interviewee pointed out:

> I don't know how much you know about this, but a directive is not a law or at least a law that directly applies to companies. It needs to be implemented in national laws. [...] Member states need to transpose it in their legislation. [...] The issue is that there is significant legal room in the implementation of a directive. [...] For companies, 28 different sets of rules is unmanageable. (Interview E21, done on March 8th, 2019)

Before 2000, this research identified only one British-based association, the Interactive Media in Retail Group (IMRG), that had developed a code on e-commerce dealing

with privacy issues and that was intended to be used in multiple European countries. Even though national ones existed and had probably interacted with American ones as previously noted, there were yet to have European-wide codes and this obviously limited interactions with American associations.

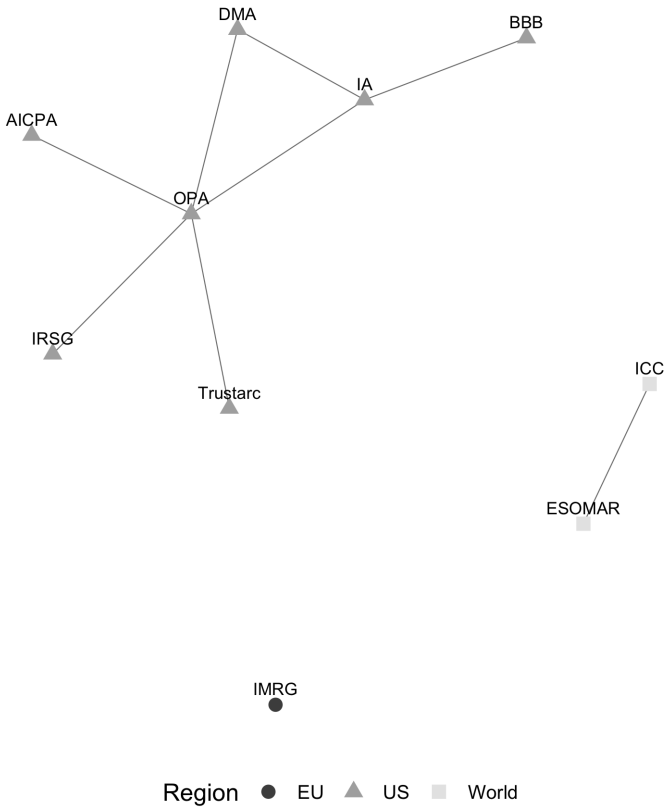

Figure 5.3: Transatlantic private network in 1999

This is depicted in figure 5.3, which presents the state of the interactions between American and European associations that had adopted a code in 1999. While the IMRG was the only private association with an active self-regulation used in multiple European countries, figure 5.3 shows that American associations were already working together and influencing the content of their respective self-regulations. The OPA that clearly stands out as the most central actor was an initiative created by many leading companies in the tech sector or with a strong interest in it (i.e., Apple, Disney, DELL, eBay, HP, Microsoft,

etc.) to develop shared practices[7]. Many associations that had previously adopted self-regulations were also members of it and contributed to its work. In addition to these direct interactions that are illustrated as ties in figure 5.3, some of the companies that founded the OPA were themselves members of other private associations. Acxiom, which is to this day one of the biggest aggregators of personal data for marketing purposes, was, for example, also a member of the IRSG and the DMA. Additional interactions between these organizations thus happened at a level not shown in figure 5.3. These, in turn, help explain the already high level of similarity between their regulations. Except from the earliest adopted in 1997, they all embraced the core set of rules in the FTC guidelines as shown by their respective high level of similarity with it in table 5.1.

In sum, the early years following the adoption of the European Data directive show a relative absence of convergence between the rules promoted in the United States and Europe. Industry self-regulations in the United States remain by far closer to the 'American' model as represented by the FTC guidelines. Interactions between them reinforced this trend and generally pushed them to exploit the same core set of rules. In contrast, they had few clear exchanges with European actors, which then limited even more the potential influence of the Data Directive in the United States. As American associations had no clear counterparts in Europe, they similarly did not have the opportunity to share rules found in the American legal system. Both regulatory systems thus had a minimal influence on the other in the first few years following the adoption of the Data Directive.

5.3 American and European Interactions after the Adoption of the Safe Harbor Agreement

At the turn of the millennium, the regulation of privacy in the United States and the European Union was drastically altered with the adoption of the Safe Harbor Agreement. As just discussed, the adoption of the Data Directive did not right away result in a convergence of rules across European countries. Yet, one important thing that it did achieve is the unification of market access decisions (Bach and Newman 2007). Through its "adequacy decision" procedure (Art. 25 of the Data Directive, now art. 45 of the

[7]Information an the OPA was retrieved from its now-closed webpage (the version of August 2000) through the Internet Archive accessible through the Wayback Machine. These webpages were saved and are on file with the author.

GDPR), the European Union in effect reserved itself the right to block companies from jurisdictions considered to have an inadequate level of protection from using European personal data, except if they relied on additional guarantees like binding corporate rules or an individual's explicit consent. In other words, this mechanism gave the European Union the institutional capacity to leverage its market size and pressure other countries in adopting its data protection rules.

The term 'adequate' obviously left a lot of room for interpretation and was only clarified as meaning 'essentially equivalent' in a recent case (Maximillian Schrems v Data Protection Commissioner, 2015). At the same time, it was pretty clear that the noticeably different regulatory approach and set of rules promoted in the United States made it impossible for it to receive an adequacy decision. Following protracted negotiations, the Safe Harbor Agreement was adopted in place of a full-fledged adequacy decision (Farrell 2003). Instead of recognizing the entire American privacy system as 'adequate', it indicated that companies self-certifying to be abiding by the principles set out in this agreement and being potentially subject to FTC enforcement in case of their violations would be considered to be 'adequate' and allowed to use personal data of Europeans. As the name of the agreement clearly indicates, this new mechanism was directly inspired by the American use of safe harbors and notably by its federal law on the protection of children's privacy online as specifically noted in chapter 3 (see p. 71).

In practice, the Safe Harbor Agreement represented a partial adequacy decision that allowed companies dealing with personal data from Europe to continue to do business as usual. Depending on the authors, this was either a proof of 'no coordination' (Drezner 2007) or 'mutual recognition' (Farrell 2003; Newman and Posner 2015) between the United States and Europe. Without further discussing their slightly diverging understanding of the impact of this agreement (see section 1.2), it is clear that they respectively agreed that it had a limited influence on how these two jurisdictions decided to regulate the use of personal data. Far from supporting a broad convergence, the Safe Harbor Agreement was at most seen as leading them to recognize their respective approaches. On the European side, this meant successfully requiring that private companies using European data to follow the rules found in the Safe Harbor Agreement. Whereas, on the American side, it meant having the European Union accept that privacy guarantees offered by the private sector could be an acceptable form of regulation. According to these authors, none had accepted to broadly embrace the data protection rules of the other through that agreement.

When giving greater attention to the content of industry self-regulation adopted in each jurisdiction, it can however be seen that this agreement spurred a real regulatory convergence between the two jurisdictions. First, it must be noted that various industry associations or companies offering privacy certification services were prone to offer Safe Harbor certifications. This trend was actually reinforced by the fact that the Safe Harbor Agreement required American companies to sign up to an alternative dispute resolution mechanism generally offered by these very same industry associations or private companies. In effect, the AICPA, BBB, DMA, and TrustArc mentioned in the previous section all became Safe Harbor providers. They were additionally joined by the Entertainment Software Rating Board (ESRB), which adopted its first code in 2000 also guaranteeing compliance with the Safe Harbor Agreement[8]. Importantly, instead of promoting multiple regulations or certification services, they almost all included the Safe Harbor principles in the one they offered to all their members or users. The BBB, for example, stated on its webpage promoting its services that "BBBOnLine Privacy Program participants meet the EU 'safe harbor' requirements"[9]. This obviously meant that these different programs, which were supposed to be the prime mode of privacy regulation in the United States, increasingly came to promote the use of 'European' rules by all their members. Only TrustArc decided to offer a different service if a company did not want to self-certify to the Safe Harbor.

Table 5.2 presents all five Safe Harbor providers and show their respective inclusion of rules found in the Safe Harbor Agreement that were not part of the FTC guidelines but were in the European Data Directive. The first revised version of their self-regulation available after the adoption of the Safe Harbor Agreement in 2000 was used. TrustArc's privacy certification service offered to all companies is presented in table 5.2, not the one offered to those wishing to only self-certify with the Safe Harbor principles. Interestingly, almost none included all the rules founds in the Safe Harbor Agreement. This is perhaps normal for TrustArc as it was not aiming to offer a Safe Harbor certification in that specific privacy program. At the same time, they very clearly included more rules than other certifications offered at the same time in the United States.

Table 5.3 shows the inclusion of the same set of rules by non-Safe Harbor providers that had an active self-regulation dealing with privacy issues in the years following the

[8]The list of Safe Harbor providers was found on the now-defunct webpage (the version of August 2003) of the FTC for the Safe Harbor Agreement accessible through the Internet archive offered by Wayback Machine. This specific page is now on file with the author.

[9]Claims made on the BBBOnline service webpage (the version of November 2006) accessed using Wayback Machine tool of the Internet Archive. This specific page is now on file with the author.

Table 5.2: Inclusion of 'European' Data Protection Rules found in the Safe Harbor Agreement by Safe Harbor Providers

Principle	Rule	AICPA Webtrust (2003)	BBBOnline Privacy Program (2002)	DMA Ethical Guidelines (2002)	ESRB Privacy Certified (2001)	TrustArc Privacy Program (2004)*
03. Collection limitations	03.01 Purpose limitations	•		•	•	
04. Use limitations	04.01 Original purposes	•	•	•		•
05. Disclosure	05.01.01 Consent	•	•	•	•	•
	05.03.02 Adequacy of processor policies	•	•			
	05.03.03 Contract	•				
07. Individual participation	07.03 Erasure	•			•	
08. Sensitive data	08.01 Consent	•		•	•	
	08.02 Third-party transfer	•	•	•	•	•
Total		8/8	4/8	5/8	5/8	3/8

* TrustArc's privacy program offered to companies not necessarily wishing to self-certify to the Safe Harbor.

adoption of the Safe Harbor Agreement. As opposed to Safe Harbor providers, they clearly included almost no European rules. When considering the fact that the rule on the need to have the consent of individuals before disclosing their personal data with third parties (05.01.01) was not in the FTC guidelines, but already in most industry self-regulations in the United States before 2000 as discussed in the previous section, the table would actually be practically empty. It is also noteworthy that all these regulations were either adopted before the adoption of the Safe Harbor or one year after at the latest. This evidently made it harder for them to include rules from the Safe Harbor Agreement. Yet, these rules were already in the European Data Directive and, as such, they could have been picked up by them since 1995. More importantly, though, these regulations could have also been revised after the adoption of the Safe Harbor Agreement. Indeed, most industry self-regulations looked at in this research were regularly modified to account for legislative changes or recent events. The fact that in this case they were not should thus be viewed a conscious decision not to include 'European' rules. These finally covered companies that were highly likely to use personal data from Europeans. The Electronic Commerce and Consumer Protection Group (ECCPG) was an association founded by large American companies like Visa, Dell, IBM, Microsoft, America Online, and AT&T clearly having business activities in Europe. SquareTrade was similarly an online service

developed in collaboration with eBay, one of the largest e-commerce platforms at the time.

Table 5.3: Inclusion of 'European' Data Protection Rules found in the Safe Harbor Agreement by non-Safe Harbor Providers

Principle	Rule	ECCPG Guidelines (2000)	IRSG Principles (1997)	NAI Code (2000)	OPA Guidelines (1999)	SquareTrade Seal (2001)	PwC BetterWeb Standard (2000)
03. Collection limitations	03.01 Purpose limitations		•				
04. Use limitations	04.01 Original purposes		•	•			
05. Disclosure	05.01.01 Consent	•			•	•	•
	05.03.02 Adequacy of processor policies						
	05.03.03 Contract						
07. Individual participation	07.03 Erasure						
08. Sensitive data	08.01 Consent						
	08.02 Third-party transfer						
Total		1/8	2/8	1/8	1/8	1/8	1/8

Industry associations or certification companies providing Safe Harbor certification services were also more likely to include in their regulations rules not found in the Safe Harbor Agreement but the European Data Directive. In effect, it should be remembered that the Safe Harbor was a negotiated agreement between the United States and the European Union. As such, it only included a subset of the rules found in the European Data Directive. Notable exclusions included the requirement to indicate the origins of collected personal data (01.04 Data Source), to contact third parties with whom they shared personal data if they correct or delete it (07.04 Notification of third parties), to maintain special security measures for the collection and use of sensitive data (08.03 Special security measures), and to keep personal data for longer than necessary (11. Data Retention). These with all other rules found in the Data Directive, but not the Safe Harbor nor the FTC guidelines are listed in table 5.4.

At first, this table is evidently more sparse than table 5.2. Clearly, private associations were not as prone to adopt rules from the Data Directive that were not in the Safe Harbor. This tends to show that private forms of regulation will generally need to

be subject to the *direct* influence of public authority to further extend it. In other words, it is not only because the government of a country with a large market has adopted some rules abroad that private actors will converge towards them. They will generally need to be directly put in contact with them. As mentioned, associations offering Safe Harbor certification services were not forced to include Safe Harbor rules in their self-regulatory programs offered to all their members. TrustArc is an example of this. Yet, the proximity with these rules created by the direct public influence raised the likelihood of seeing them use or, using the terminology previously introduced, 'exploit' these rules when devising their self-regulatory programs. As previously discussed in chapter 4, it allowed them to save time and resources, as well as minimizing the risks of creating an unwanted conflict of rules.

Table 5.4: Inclusion of 'European' Data Protection Rules outside of the Safe Harbor Agreement by Safe Harbor Providers

Principle	Rule	AICPA Webtrust (2003)	BBBOnline Privacy Program (2002)	DMA Ethical Guidelines (2002)	ESRB Privacy Certified (2001)	TrustArc Privacy Program (2004)*
01. Transparency	01.04 Data source	•	•	•		•
02. Consent	02.06 Right to refuse automated decision-making					
	02.07 Right to object					
03. Collection limitations	03.02 Fair and lawful	•			•	
04. Use limitations	04.02 Fair and lawful	•		•	•	
05. Disclosure	05.03.01 Use limitations		•			
	05.04 Third-country transfer					
07. Individual participation	07.04 Notification of third parties	•			•	
	07.07 Right to be informed of automated practices					
08. Sensitive data	08.03 Special security measures	•	•	•		•
11. Data retention	11. Data retention	•			•	
Total		5/11	3/11	3/11	4/11	2/11

* TrustArc's privacy program offered to companies not necessarily wishing to self-certify to the Safe Harbor.

As their interaction was first with the rules in the Safe Harbor, it is unsurprising that they mostly exploited those found in this agreement and not all those found in the European Data Directive. At the same time, it obviously created a bridge between them

because the Safe Harbor and the Data Directive were obviously closely tied together. Applying the former would have thus generally meant looking at the content of the latter. If the number of rules in table 5.4 included in self-regulations of Safe Harbor providers is not as important as rules found in the Safe Harbor, it is still strikingly more important than by non-Safe Harbor providers. Among the latter, only two included the rule requiring to indicate individuals where their personal data was collected (01.04). It must also be considered that some rules in table 5.4 were specific to the European context and would have been a great proof of convergence. Yet, American private associations probably felt that they did not really need to include them as they did not apply to their context.

This is, for example, the case of the right to object (02.07). The latter foresees that when data collection and use is not based on explicit consent but a legitimate objective, individuals can request that their personal data stop being used for these purposes (art. 14 of the Data Directive and now 21 of the GDPR). This rule makes sense in the context of the consent system established by the European Union, which foresees that the processing of personal data should be primarily based on an individual's explicit consent but often ends being processed on 'legitimate grounds'. The latter has historically been understood very broadly and can even include marketing purposes. Faced with this, the right to object gives the possibility to contest the use of personal data that is often done without the explicit consent of individuals. In the United States, this specific rule is a bit redundant considering their use of an opt-out form of consent. Again, the opt-out form of consent means that individuals are presumed to have accepted the collection and use of their personal data when using the services of a company, but they can at any time opt-out and request that their personal data stop being used. Including the right to object would thus make sense if industry self-regulations in the United States also adopted the European consent system. This would again be a great proof of convergence, but it is also a very high bar to set to observe it as it would practically require an almost complete overhaul of how their privacy regulations function. In practice, both consent systems often moreover work similarly. One interviewee for this research actually noted that the European Union interestingly believed that the European Union was using the same consent system as the United States:

> The primary differentiator before and after [the GDPR] is the move away from explicit consent and the creation of the right to object. They effectively turned themselves into an opt-out regime as in the United States. [...] They moved away from affirmative consent to a kind of opt-out regime, which however limits the

> purposes for which data can be collected and processed. (Interview E27, done on April 4th, 2019)

More accurately, the GDPR did not create the right to object but expanded it by removing the need for an individual to justify its request. It is now the company or any other private entity processing personal data that needs to explain why it has a legitimate ground to do so without the individual's consent. It might thus have effectively moved the European Union closer to the American opt-out system, but private companies in Europe have since the early days of the Directive often operated based on a kind of opt-out mechanism as it is less constraining. This is all to say that it would have been quite surprising to see that specific rule adopted in the United States and that its absence should not preclude us from recognizing that industry associations providing safe harbor certifications have supported a convergence between the 'American' and 'European' rules. A somewhat different but similar explanation could be made for the rules on the transfer of personal data to private entities in third countries (05.04) and automated processing (02.07 and 07.07).

In that vein, the inclusion by the AICPA Webtrust program, ESRB Privacy certified, and DMA guidelines of a rule indicating that the use (04.02) and, for the first two, the collection (03.02) of personal data should be fair and lawful is particularly noteworthy. It might seem quite straightforward that the actions of private companies need to follow the law. In an American context where the overarching principle is that industry self-regulation should lead the way, this is, however, not something that needs pointing out. This rather reflects the European approach, which at its heart requires a legal basis for the processing of personal data (Schwartz and Peifer 2017: 127). This specific mention is thus an important example of a case where American associations converged towards rules that are at the heart of what distinguishes privacy regulation in the European Union and the United States.

By successfully negotiating an international agreement with the American government, the European Commission showed its capacity to use its hierarchical position and legal authority to push private actors in the United States to exploit its rules. Importantly, it does not mean that private actors were all passive in this process. As pointed out, not all private associations decided to embrace the rules found in the Safe Harbor even though many American businesses were already dealing with the personal data of European citizens. More significantly, though, the decision to exploit European rules not found in the Safe Harbor Agreement as well as to promote them to American companies

that did not necessarily need to follow them show how industry self-regulations amplified the reach of European rules. A second way through which they did so is through the formation of private networks allowing for the exchange of their respective practices.

5.4 Transnational Trustmarks and Private Networks in the Early 2000s

Just as the European Union and the United States were actively negotiating the Safe Harbor Agreement, private actors started to increasingly work together as depicted in figure 5.4. In contrast to the 1999 network previously shown in figure 5.3, we can observe that there are now multiple European private actors that had adopted a code dealing with privacy issues. Moreover, most actors have at least one tie, indicating their increasing tendency to collaborate. Unsurprisingly, we can see that American and European associations still tended to work with associations from their home jurisdiction. This reflects the natural and geographical proximity that they share. At the same time, there were already some links between the American and European actors, which created early on opportunities for exchanging practices between these two communities of actors.

Yet, what probably stands out the most when quickly glancing at this figure is the closely tied nature of a small cluster of actors. This importantly exhibits the work being done in the early 2000s to develop an European trustmark to help harmonize protections offered to consumers online. The term trustmark here qualifies an industry self-regulation that specifically aims to allow a company to advertise a seal on its website to raise trust in its services. In practice, most codes of conduct, guidelines, or sets of principles previously discussed allow their members or users to post an online seal. This was notably the case of the BBBOnline and TrustArc privacy programs. The possibility for companies to advertise their goodwill or good data practices remains today one of the main selling points to develop and use industry self-regulations. Importantly, the number of active certifications is often inversely proportional to their success in providing trust. As their number grows, they tend to create confusion and undermine themselves. At the turn of the 2000s, this was notably the case as the number of trustmarks dealing with e-commerce and data protection rose exponentially. It must be remembered that this research only includes associations active at the European level or in multiple European countries. As such, there are almost the same number of European and American private actors

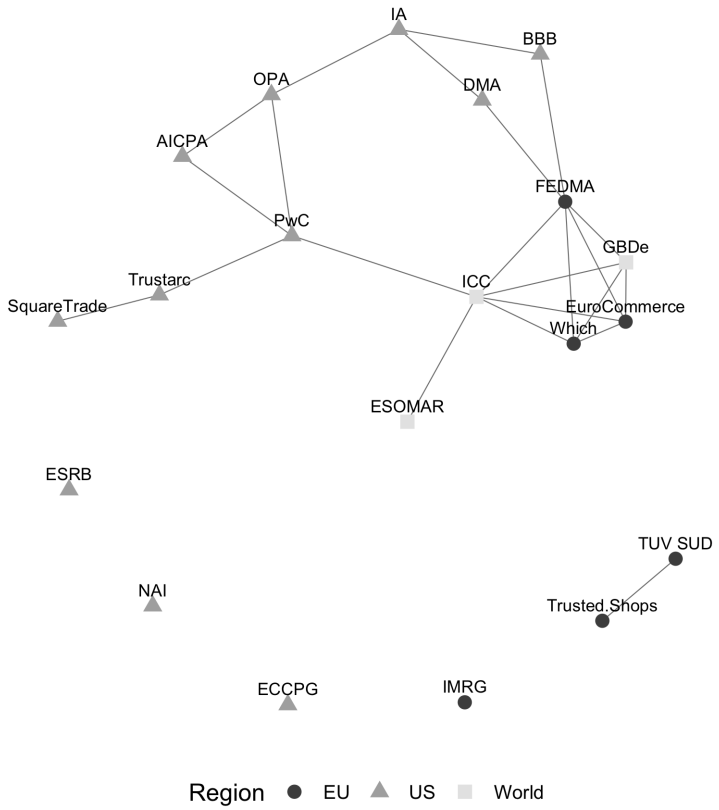

Figure 5.4: Transatlantic private network in 2001

in figure 5.4. There were, however, many more codes and trustmarks at the Member State level in Europe. A preliminary tally for this research found close to 70 codes or trustmarks promoted in Europe and this most likely still missed some. As one interviewee explicitly noted of that situation:

> There were too many logos. Was it helping? Not that much. It was confusing for consumers. (Interview E7, done on February 4th, 2019)

This concern was shared by the European Commission that had early on been adamant that the development of the digital economy should not lead to the creation of new regulatory barriers that would undermine its single market. Back in 1994, a high-level group chaired by then-European Commissioner for the Information Society, Martin Bangemann, specifically stated the need for a "regulatory response [...] at the European level in order to maximize the benefits of the single market for all players" (European

Commission 1994: 21). As mentioned above, the integration process of European data protection rules was not going as smoothly as hoped by the European Commission. The varying application of the Data Directive was moreover being reflected in the development of multiple national trustmarks with different sets of data protection rules. In light of this, the European Commission notably thought it would be good "to examine the potential for drawing up some common guidelines" for the development of codes of conduct and trustmarks at the European level (European Commission 2000).

Following this idea, the European Commission supported the creation of an "e-confidence forum" in 2000 where private associations were expected to work together to build a European trustmark. This specific project more specifically involved important associations like the Federation of European Direct Marketing Association (FEDMA), EuroCommerce, and the consumer organization Which that had previously developed an industry self-regulation or were working on one at the same time (European Commission 2004). They are all part of the small hub of actors presented as interacting in figure 5.4. Importantly, this project also included representatives of businesses outside of the European Union and the United States. As noted in the introduction to the forum, participation was "not limited to European participants [and it specifically welcomed] international participation in order to get a better appreciation of the different initiatives in different countries"[10]. Apart from important American private companies, like AOL, Ford, Intel, and Microsoft, it notably included the Global Business Dialogue on e-Commerce (GBDe) and the International Chamber of Commerce (ICC), two industry associations that adopted international guidelines with data protection requirements in the early 2000s. These can also be seen as part of the small group of actors with close ties to each other in figure 5.4.

By working with private actors, the European Commission was viewing an opportunity to promote a greater level of harmonization than it was able to achieve through its traditional legal means. This interestingly echoes the role that American private associations were at the same time playing in the United States and shows how co-regulation has early on been a feature of both European internal and external regulation of privacy. In the end, the development of a single European trustmark did not bear fruit. The Union of Industrial and Employers' Confederations of Europe (then known as UNICE, now called BusinessEurope) and the European Consumer Organization (BEUC), which were

[10]Information retrieved from the now-closed webpage dedicated to the e-confidence Forum and accessed through the Internet Archive using its Wayback Machine tool. This specific page (July 2000) is now on file with the author.

leading this project, were unable to agree on its implementation. Despite being praised for their collaborative work and actually agreeing on a set of requirements, they were unable to find common ground on the actual enforcement mechanism of the trustmark (European Commission 2004: 8-9).

This failure to create a European trustmark yet does not mean that the e-confidence forum entirely failed to promote greater regulatory convergence. By bringing distant organizations closer to each other, it was an important space where they could influence their respective decisions of which rules to include in their industry self-regulations. For the two non-European associations, it notably meant adopting data protection rules originally found in the European Data Directive. The ICC's 2001 code on direct advertising and the GBDe's 2000 privacy guidelines for e-commerce respectively had a thematic similarity index of 0.68 and 0.55 with it. For the ICC, this was significantly higher than its previous code adopted in 1999 (0.47). While there is not the same point of comparison for the GBDe, its similarity index was generally higher than other industry self-regulations adopted in the United States in the years before (see table 5.1). This European influence can also be seen by looking at their inclusion of 'European' data protection rules found in the Safe Harbor Agreement as presented in table 5.5.

Table 5.5: Inclusion of 'European' Data Protection Rules found in the Safe Harbor Agreement by the ICC and GBDe

Principle	Rule	GBDe Privacy guidelines (2000)	ICC Code on Direct Marketing (2001)
03. Collection limitations	03.01 Purpose limitations		•
04. Use limitations	04.01 Original purposes	•	•
	05.01.01 Consent	•	•
05. Disclosure	05.03.02 Adequacy of processor policies	•	•
	05.03.03 Contract		
07. Individual participation	07.03 Erasure		
08. Sensitive data	08.01 Consent	•	
	08.02 Third-party transfer		
Total		4/8	4/8

As can be seen, both the GBDe and ICC had incorporated many European rules just like the Safe Harbor providers (see table 5.2 above). Just like them, they also included other rules found in the European Data Directive that were not in the Safe Harbor, like the rule requiring not to keep personal data for longer than needed (11. data retention) or the need to have a fair and lawful basis for the collection and use of personal data (03.02 and 04.02). While these two organizations were not purely 'American', this move towards the European model remained significant. The global nature of these organizations meant

that they were in themselves important forums for rule harmonization As a matter of fact, the GBDe was created by private companies primarily based in the United States and the European Union to help minimize their growing divergence of views of how to regulate the electronic marketplace (Green Cowles 2001). Moreover, both represented prominent American companies. Among the representatives of the GBDe during the e-confidence forum were, for example, people from the American computer company Hewlett-Packard.

The participation of these two associations as well as of other American private companies significantly did not only support the exploitation of European data protection rules by American actors. As noted in the official description of the e-confidence forum cited above, the participation of foreign (in practice principally American) private actors was notably aimed at obtaining a better understanding in Europe of the regulatory approach taken in other jurisdictions. This is reflected in the codes adopted by the European associations that took part in the e-confidence forum and included rules found in the FTC guidelines but not the Data Directive. This process of exploitation of American data protection rules is reported in table 5.6.

Just as for American associations exploiting 'European' rules, the exploitation of 'American' rules by European associations was never complete. Indeed, none include all the different data protection rules found in the American industry self-regulation part of the e-confidence forum. This partly reflects the social nature of the process of exploitation. As noted in the first section of this chapter, exploitation indeed does not portray a relation where one straightforwardly imposes its will onto the other. It reflects a more 'co-optive' form of influence where regulators choose to follow rules as they learn about and become socialized to them. These will evidently evolve over time as different regulators gain a better understanding of their respective sets of data protection rules. As these were still early interactions, it should indeed not have been expected that European industry associations would perfectly replicate 'American' rules. It must also be pointed out that the rules with which the European associations were interacting were not directly those developed by the FTC guidelines or other American federal agencies, but those that had been created by the ICC, GBDe, and other American industry self-regulations. In fact, the 1999 ICC direct marketing guidelines only included the rules requiring to notify the use of passive data collection methods (01.09), to limit the collection of personal data from children (09.02), and to gain parental consent before collecting personal data from children (09.04), which are three of the most often taken up by European associations

Table 5.6: Inclusion of 'American' Data Protection Rules by European private associations part of the e-Confidence Forum

Principle	Rule	BEUC-UNICE European Trustmark (2001)*	FEDMA eCommerce Code (2000)	FEDMA Data Protection Guidelines (2003)	EuroCommerce EuroLabel (2000)	Which Webtrader (2000)
01. Transparency	01.09 Automated or Passive Data Collection (Cookie Notice)	•	•			•
03. Collection limitations	03.03 Third-Party Source					
	09.01 Special notification			•		
09. Children data	09.02 Special collection limitations	•	•	•		•
	09.03 Parental control		•	•		
	09.04 Parental consent	•	•	•		•
	09.05 Parental access					
	09.08 Special security measures					
13. Enforcement	13.01 Complaint mechanism	•	•	•	•	•
	13.02 Compliance mechanism	•	•	•	•	•
Total		5/10	6/10	6/10	2/10	5/10

* Text of the European trustmark jointly developed by BEUC and UNICE as part of the e-confidence forum, which ended up never being formally adopted.

in table 5.6. This importantly shows that if private actors can help diffuse public rules, this is always mediated by what private actors actually decide to include in their self-regulatory programs. Private actors can notably exclude some rules that they do not find to be in their interest if they are not mandatory or vague. This seems to be what happened for the requirement to use reputable sources of personal data and cross-verify personal data from a third-party source (03.03), which was a rule found in the FTC guidelines and that can be particularly cumbersome for marketing companies represented by the ICC, GBDe and many European associations part of the e-confidence forum.

Having said that, the exploitation of 'American' rules by the European associations part of the e-confidence forum was generally more substantial than other associations operating trustmarks in Europe at the same time. This research found three associations promoting a trustmark or code of conduct in the early 2000s in at least more

than one European country and that were not actively contributing to the e-confidence forum. Table 5.7 shows how each exploited data protection rules only found in the FTC guidelines and clearly indicates that they did not tend to so. Indeed, they all merely share the rule requiring private companies to notify individuals of the use of cookies or other passive data collection methods before they are being used (01.09). Considering that this requirement became part of the European Directive on privacy in electronic communications in 2002, this might not even be a sign of a direct American influence.

Table 5.7: Inclusion of 'American' Data Protection Rules by European private associations not part of the e-Confidence Forum

Principle	Rule	IMRG Code 2003	Trusted Shops Criteria (2001)	Tuv Sud Safe Shopping Certification (2001)
01. Transparency	01.09 Automated or Passive Data Collection (Cookie Notice)	•	•	•
03. Collection limitations	03.03 Third-Party Source			
09. Children data	09.01 Special notification			
	09.02 Special collection limitations	•		
	09.03 Parental control			
	09.04 Parental consent			•
	09.05 Parental access			
	09.08 Special security measures			
13. Enforcement	13.01 Complaint mechanism			
	13.02 Compliance mechanism		•	
Total		2/10	2/10	2/10

Apart from the initiative to develop a European trustmark, interactions between FEDMA and two American associations presented another important avenue through which private actors supported the exploitation of data protection rules in one jurisdiction by the other. As seen in figure 5.4, FEDMA was more specifically working with two American-based private organizations: the US DMA and the BBB. In the case of the former, FEDMA had long before the e-confidence forum been collaborating with its sister organization in the United States. In addition to working through the International Federation of Direct Marketing Associations on the use of suppression list even before the adoption of the Safe Harbor (see section 4.4), they were notably funding research on how to comply with data protection rules. This included a comparative analysis of codes of conduct on direct marketing around the world in 1997 and a study on the European

data protection rules in 2001[11]. This work with the US DMA can help explain why FEDMA was the association that included the most American rules in table 5.6 and conversely why the DMA became one of the Safe Harbor providers in the United States. Their respective relationship was spurring them to exploit the rules found in each other's primary jurisdictions. This influence importantly persisted after the initial pressure of the negotiation of the Safe Harbor progressively faded away. The US DMA, for one, added the right to request the erasure of personal data (07.03) and the obligation not to maintain personal data for longer than necessary (11) respectively in its 2007 and 2011 version of its code of conduct. These two originally 'European' rules had before then failed to be incorporated in it.

In the early 2000s, FEDMA was working and even signed an official partnership with the BBB to develop a global trustmark. At the time, these two organizations indicated that they hoped to push a greater number of companies around the world to follow "consistently high online standard" based on a "single, internationally recognizable" emblem (Saliba 2001). At this specific point in time, the relation between the two was largely one of homophily. Rather than pushing themselves towards each other, they actually appeared to work together because of their preexisting similarity. In fact, the version of the BBBOnline privacy program in 2000 and FEDMA's code for e-commerce adopted in 2000 had a thematic similarity index of 0.71. Both had thus already moved towards the rules promoted in each of their respective jurisdictions. The BBB was already a Safe Harbor provider and FEDMA had been interacting with American actors, including the US DMA, as just discussed.

If their early collaboration did not in itself led to greater harmonization, it did end up doing so by contributing to the creation of a transnational organization as of today promoting a global trustmark. After presenting their work and launching the Global Trustmark Alliance at a summit organized by the GBDe in 2004, they merged their initiative with the Asia-Pacific Trustmark Alliance in 2007 and contributed to the creation of the World Trustmark Alliance (WTA). The latter helped promote an increasingly unified model of data protection rules for companies doing business online. Besides promoting American and European rules to Asian and Latin American countries, it also created new relations between European and American actors as depicted in figure 5.5.

[11]The list of publications funded by FEDMA and the US DMA was retrieved from FEDMA's website using the Internet archive's Wayback Machine tool. This specific page (April 2001) is now on file with the author.

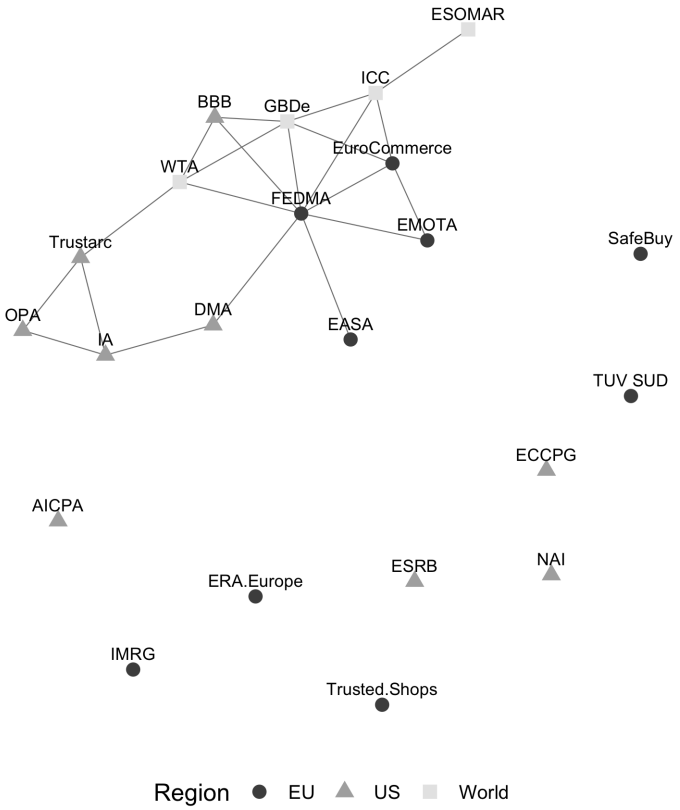

Figure 5.5: Transatlantic private network in 2008

TrustArc was most notably involved in the creation of the WTA. As the United States was working with APEC countries to develop its privacy framework (2005) and cross-border privacy rules system (2011), this provider of Safe Harbor certifications in the United States had already been working with the Asia-Pacific Trustmark Alliance that merged with the initiative of the BBB and FEDMA. While contributing to shaping the rules promoted by the WTA, it created another venue where European rules could influence the work of TrustArc. As a reminder, it was the sole provider of Safe Harbor certifications that had decided to operate different services depending on if companies using its services were planning to deal or not with the personal data of Europeans. Its basic certification program was unsurprisingly the one including the fewest European rules found in the Safe Harbor Agreement. In 2012, its revised version of its most basic privacy program offered to all companies in the United States was significantly closer to European rules than its version of 2004 as shown in table 5.8.

Table 5.8: Inclusion of 'European' Data Protection Rules by TrustArc and the World Trustmark Alliance

Principle	Rule	TrustArc privacy Program (2004)*	TrustArc privacy program (2012)*	WTA Global Trustmark (2008)
03. Collection limitations	03.01 Purpose limitations		•	•
04. Use limitations	04.01 Original purposes		•	•
	05.01.01 Consent	•	•	•
05. Disclosure	05.03.02 Adequacy of processor policies		•	
	05.03.03 Contract			
07. Individual participation	07.03 Erasure		•	•
08. Sensitive data	08.01 Consent			
	08.02 Third-party transfer	•		
Total		2/8	5/8	4/8

* TrustArc's privacy program offered to companies not necessarily wishing to self-certify to the Safe Harbor.

As the revised version of TrustArc's privacy program was not right after the creation of the WTA, it is hard to maintain that it is necessarily this sole event that was the turning point for it. Between 2008 and 2012, there were potentially other sources of influence that could have led TrustArc's representatives to exploit European data protection rules. In the United States, the existence of other American associations that had done so for quite some time clearly raises this likelihood. With that in mind, the fact that TrustArc did not follow its American counterparts for many years tends to indicate that they were probably not the defining factor in its decision. The exploitation of the almost identical set of 'European' rules in the WTA's global trustmark of 2008 and TrustArc privacy program of 2012 moreover sustains the idea that the former played a role in the content of the latter. In the end, it can be assumed that there were probably other sources of influence but working to build a global trustmark with European associations was most likely a contributing factor to the exploitation of European rules by TrustArc.

This work of FEDMA in the early 2000s with the US DMA and the BBB as well as its broader impact on other industry associations is yet another example of how interactions between private actors can become an avenue for rules found in one jurisdiction to be exploited in another and, in turn, amplify the influence of public authorities outside their traditional boundaries. By exchanging and encouraging each other to adopt similar practices, they effectively supported the development of a joint and common set of rules that included what each of their governments had previously set forth. The involvement of the European Commission in the development of the e-confidence forum and the ensuing transnational network moreover highlighted how close the shadow of hierarchy sometimes remain from these private initiatives. While not in a position to legally force

them to include specific rules, the presence of European regulators in the process of devising a potential European trustmark certainly ensured that rules found in its European Data Directive were at the forefront of any discussion. In a way, the internal struggle to ensure that the same set of data protection rules are applied throughout Europe ended up shaping how European rules were exploited globally. This echoes arguments that the diffusion of the European comprehensive model of privacy law was a result of "issues that it faced internally" (Schwartz 2019: 138, see also Newman 2008).At the same time, the creation of these forums allowed American rules to cross over Europe. This also shows that private networks are not tools that public authorities entirely control. Depending on private actors' decisions to create new relations, they will not have the same effects. This can similarly be seen when looking at how deliberate actions taken by American authorities to solve issues raised by the digital advertising industry had similar effects and further supported the exploitation of both European and American data protection rules.

5.5 Self-Regulatory Principles for Digital Advertising and Private Networks in the Late 2000s

Back in 2008, the ad-tech industry was on the rise. After having largely disappeared following "the burst of the dotcom bubble" in the early 2000s, companies were increasingly developing new techniques to track individuals' behaviour online and send them what was increasingly called behavioral (i.e., individualized) advertising, raising many concerns for public authorities (Federal Trade Commission 2009: 7). Following the organization of a Town Hall in 2007 by the FTC, the general agreement was that self-regulatory practices in online advertising were moreover failing to protect the privacy of individuals (Dixon 2007; Federal Trade Commission 2009). The Network Advertising Initiative (NAI) that had adopted a code in 2000 following a previous workshop also organized by the FTC was especially criticized for its promotion of an "opt-out cookie" policy (Gellman and Dixon 2016: 59). The latter allowed companies to place a tracking device on everyone's computers without their explicit consent and often without clearly informing them about it. In this context, the FTC called for the development of new self-regulatory principles for online behavioral advertising, which was first answered by the creation of the Digital Advertising Alliance (DAA) and the adoption of its first industry self-regulation in 2009.

The DAA was in itself the result of the work of various associations already working on these issues and previously mentioned like the BBB, DMA, and NAI (Federal Trade Commission 2009: 14). As such, the DAA helped reinforce and create new links between many previous American associations. Speaking of the DAA, one interviewee noted that it had precisely been a great opportunity to learn "about what some of [its] colleagues were doing" and emphasized the ongoing nature of this project. As opposed to their previous interactions, which had often been a "one-off project", the interviewee mentioned that the work being done at the DAA was still today shaping their own work (Interview E36, done on May 10th, 2019). As of now, it continues to develop new industry self-regulations.

While the result of the collaborative work of many preexisting associations, the DAA's first industry self-regulation was equally inspired by the work of the FTC. The latter had published a set of four principles that they thought should form the core of any self-regulatory initiative, which then formed the core of the DAA's rules for online behavioral advertising (Federal Trade Commission 2008). These more precisely included: (1) transparency and consumer control, (2) security and data retention, (3) affirmative or express consent for material changes to privacy policies, and (4) affirmative or express consent for the use of sensitive data. (Federal Trade Commission 2008). These were all part of the DAA's 2009 code on online behavioral advertising and interestingly reflect some rules that were previously identified as originating from Europe. The requirement to not process sensitive data without the express consent from an individual and to not retain personal data for longer than needed (i.e., data retention) are two examples of rules that were absent of the original guidelines of the FTC but in the Data Directive back in 1995.

It is not entirely clear how these four principles were chosen, but they were clearly written based on discussions that the FTC had with members from the industry and consumer groups. In a transcript of the FTC's 2007 Town Hall organized on this issue, it is evident that the FTC tried to get a good grasp of what were the preexisting self-regulatory initiatives in the marketing space. As such, it notably ended up discussing the work of the DMA, which had been operating a self-regulatory program including many provisions from the Safe Harbor since the beginning of the 2000s (see table 5.2). The DMA privacy guidelines thus seemed to played an important role in the development of these four self-regulatory principles by the FTC. This would also fit the indication by then-NAI's director according to which his organization had been inspired by the work

of the DMA when submitting a revised version of its code of conduct following the FTC' Town Hall (Hughes 2008). In effect, the DMA's guidelines included all the rules found in the FTC's proposed self-regulatory principles and almost all those found in the NAI Revised code of conduct.

The only rule absent from the DMA's guidelines and included by the FTC was the one on data retention. The latter was in fact part of the European Data Directive but had yet to be largely taken up by American private associations. As it was not part of the Safe Harbor Agreement, most associations that had promoted a code including many rules from it did not include it (see table 5.4). This changed with its inclusion in the FTC's proposed principles and then the DAA's code. In effect, most associations that worked on the DAA's program ended up including a rule on data retention in their own codes of conduct or guidelines afterward. Figure 5.6 shows this upsurge in the adoption of this specific rule after 2008.

Besides supporting greater rule harmonization in the United States, the DAA's work was moreover influential in Europe. As similar concerns to those raised during the FTC's Town Hall in 2007 were being voiced towards the marketing industry in Europe, industry associations there decided to develop a similar initiative: the European Digital Advertising Alliance (EDAA). One interviewee that was close to the creation of this new organization in Europe indicated that they knew about the DAA's work through their members that were part of this American initiative (Interview E21, done on March 8th, 2019). The Interactive Advertising Bureau in Europe that took the lead in the creation of the EDAA was similarly exchanging with its sister organization in the United States and thus had the opportunity to learn first-hand about the DAA from one of its founding members. Once created, the EDAA and the DAA moreover started to have direct exchanges with each other and have continued to shape their work since then (Interview E21, done on March 8th, 2019). These new interactions between European and American actors are shown in figure 5.7. It also highlights the central position that the DAA progressively came to have in the United States.

Unsurprisingly, the rules included in the EDAA self-regulation adopted in 2012 are very close to the one of the DAA adopted in 2009. They actually share all the same basic principles and have a very high thematic similarity index of 0.72. The content of their rules actually only slightly differ with regards to the implementation mechanisms and the transfer of personal data to third parties. Apart from this, they are almost a replica of each other. This allowed for the further exploitation of the data protection

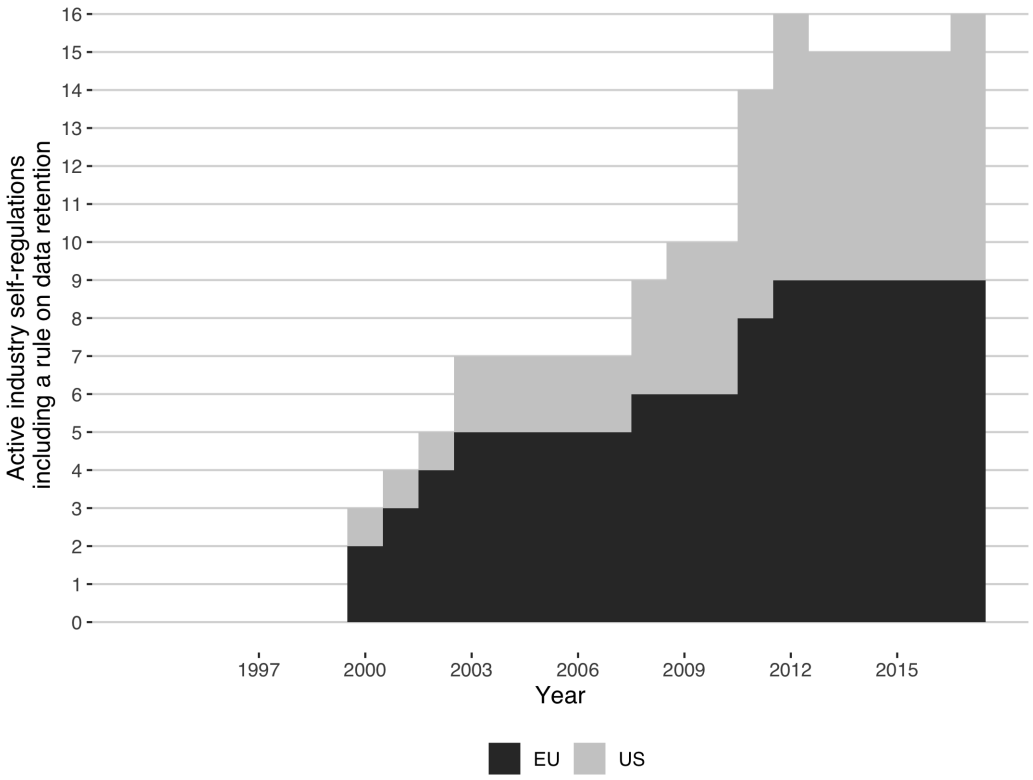

Figure 5.6: Total number of active industry self-regulations including a rule requiring to maintain personal data for no longer than needed

rules promoted in each jurisdiction. This is notably evident when looking at the cases of two rules.

First, the DAA integrated into its original self-regulation the requirement previously found in the codes of other American associations, like the DMA, the IRSG, and the NAI, to educate consumers about their data practices. In addition to transparency rules originally found in the FTC guidelines and European Data directive, these 'education' rules require private companies to make outreach efforts to explain to the public how they use personal data to send targeted advertising. This specific policy became one of the core components of the DAA self-regulatory program in 2009 through its promotion of an AdChoice Icon that is now almost always found in the corner of online advertisements seen on major websites like Google and Facebook. By clicking on this specific icon, users will be briefly explained why they see a specific publicity and what personal information

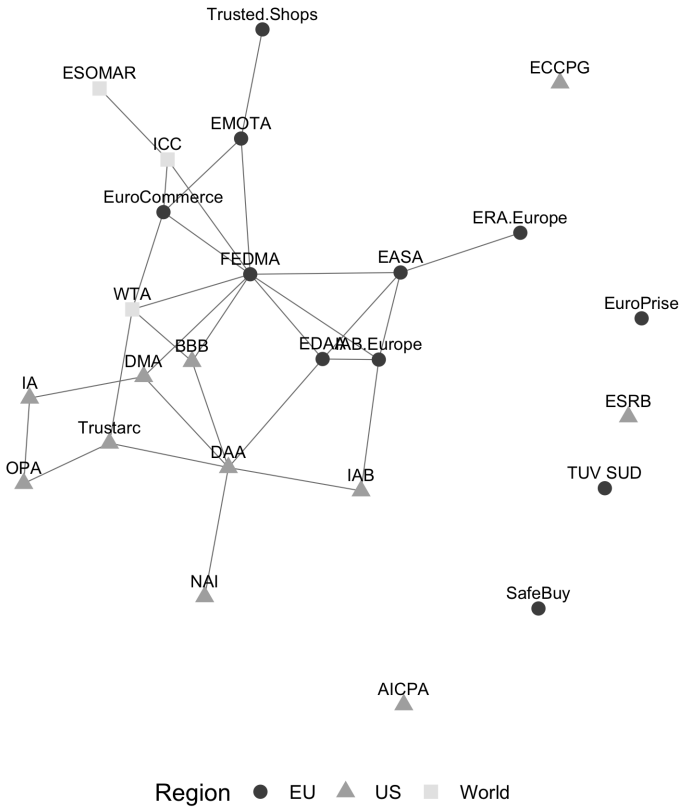

Figure 5.7: Transatlantic private network in 2012

might have been used to identify them. Based on the principles of choice and control, individuals are then allowed to express their wish to remove it and potentially change how their data is used. How the latter is actually implemented, however, varies according to the companies implementing it. For example, Google and Facebook apply the DAA rules but do not offer the same tool to make choices.

With that in mind, the same rule on education was included in the EDAA's self-regulation and has made its way in one of the other European associations that worked with it. Figure 5.8 shows that some of its founding members, like the IAB in Europe, even did so before the EDAA was officially created in 2012. Nowadays, the same AdChoice icon as the one originally developed in the United States is in effect visible by Europeans when receiving online advertising. They can similarly use it to manage the publicity they receive and complement previous privacy guarantees that they had. For many privacy activists, this is not much as it does not impede companies from collecting

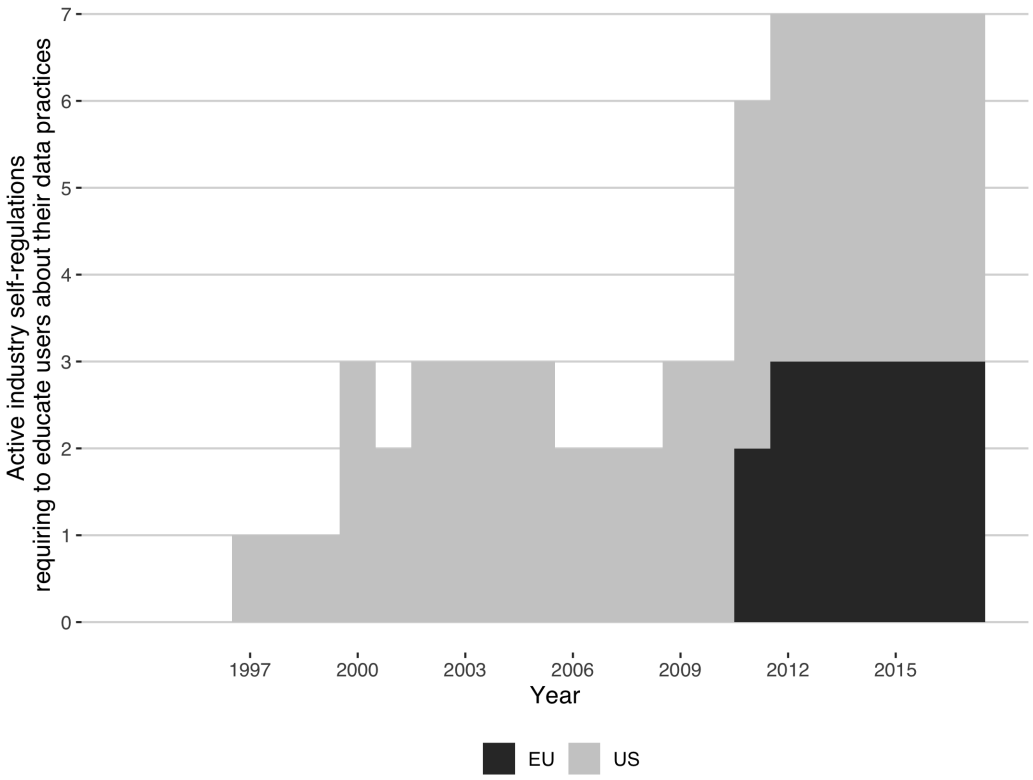

Figure 5.8: Total number of active industry self-regulations requiring companies to educate individuals about their data practices

personal data nor using it to send targeted advertising. Yet, it has forced companies to be more transparent. This is a first essential step to subsequently ensure that individuals actually make use of some of their other privacy protections, like the possibility to object to the use of their personal data for marketing purposes or to request the erasure of their personal data.

A second interesting case is the rule on the need to have affirmative or express consent before collecting or using sensitive data. As previously mentioned, this was a requirement found early on in the Data Directive and, in fact, it had already been included by many of the associations that offered Safe Harbor certifications in the early 2000s (see table 5.4 above). At the time of its inclusion by the DAA, it was thus not so new anymore in the United States. It was similarly not a new rule in Europe, but it had not been widely included in industry self-regulation. In effect, there were significantly

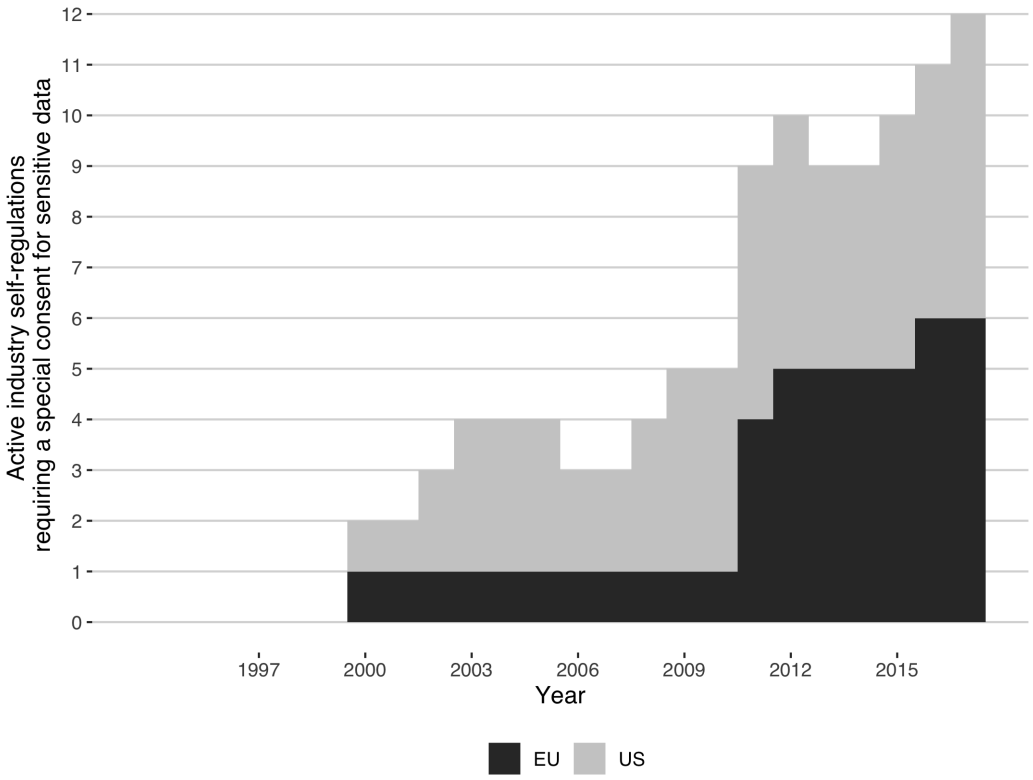

Figure 5.9: Total number of active industry self-regulations requiring to gain the affirmative or express consent before collecting and processing sensitive data

more American associations incorporating this rule in their self-regulatory programs than in Europe before 2011. It can always be said that private companies still had to respect it anyway, but it is still striking that it was not part of the rules that private associations were promoting. This absence of most private regulatory instruments in Europe can help explain why it was not included in the global trustmark created by the World Trustmark Alliance (see table 5.8). The creation of the EDAA and the adoption of self-regulation by some of its founding members largely replicating the original self-regulatory program of the DAA, however, led more European associations to include this rule as shown in figure 5.9.

This finally shows that by interacting with private actors in the United States, European associations were sometimes even led to exploit rules originating from Europe. This reversed influence further demonstrates that when working together, private asso-

ciations do not merely project the rule of the public authority with which they would normally be in direct relation of hierarchy. They promote what they have spent years developing based on their previous interactions with public and private actors. While amplifying the exploitation of public rules, it once again shows the real agency that they have in this process. Recognizing this also helps explain cases where rules have been less likely to be shared between both jurisdictions, which notably includes those covering data breaches. Since 2002, multiple states in the United States have adopted laws requiring private companies to inform their users when they lose their personal data following a security breach. Although this regulatory activity did not originate at the federal level in the United States, it is a prime example of American leadership in privacy regulation. As such, it is striking that only one self-regulation in Europe was found to include rules on data breaches. This, however, mirrors their similar absence in most industry self-regulations in the United States and notably the one of the DAA, which was one the latest cases of direct interactions between American and European industry associations before the European Commission started drafting the GDPR.

5.6 Conclusion

As of today, the United States and the European Union continue to follow different regulatory approaches to privacy protection. While the European Union doubled down on its preference for a comprehensive system with the adoption of the GDPR in 2016, the United States still does not have a federal privacy law covering both the public and private sectors. If the adoption by the state of California of such a comprehensive law in 2018 gave the impression that the United States would soon adopt one, the decision by the Trump administration to abandon the project of a Consumer Privacy Bill of Rights that the previous administration had spent four years developing show how uncertain it is to see it happening in the near future. Despite this lasting difference in their regulatory approaches, I showed that data protection rules in both jurisdictions have in practice became increasingly similar following direct interactions between public and private actors.

Far from a situation of no coordination (Drezner 2007) or even merely mutual recognition (Newman and Posner 2015), there has actually been a regulatory convergence going on. In effect, private companies on both sides of the Atlantic increasingly exploited the same data protection rules in their respective industry self-regulations. Important

divergence remains and not all companies today apply the same set of rules. In fact, it was repeatedly shown that since the adoption of the European Data Directive in 1995, different self-regulatory programs promoted different sets of rules. These have moreover rarely included all those found in the 'American' or 'European' models introduced in chapter 4. At the same time, they generally tended to become increasingly similar and to approximate those of public and private actors with which they previously interacted. In turn, actors creating links between the two jurisdictions have been seen to have a special influence over the choice of which rules are applied in both.

These findings further point out that this is not simply a story of the European Union imposing its standards globally. As it was demonstrated, European rules have been increasingly part of the regulatory framework in the United States. To some extent, the early adoption of a more comprehensive set of rules and its willingness to promote them globally gave the European Union a first-mover advantage. As private actors were deciding which rules to apply, they were naturally drawn towards these preexisting rules, even more so the more actors promoted them. Yet, it is wrong to think that the United States did not play any role in the evolution of data protection rules in the last twenty years. Rules on the protection of children's data, the use of passive data collection methods (i.e., cookies), and the education of users are some examples of rules that were created in the United States and found their way in Europe first through private interactions.

As opposed to previous explanations maintaining that private companies in the United States have embraced European data protection rules (Bradford 2012, 2020), I also maintained that the process of regulatory convergence was never complete. As shown, industry self-regulations never adopted the complete set of data protection rules promoted by either the United States or the European Union. This is notably the cases of rules on data breaches that were first adopted in the United States and that were not included by most industry associations in both jurisdictions. Their inclusion in the GDPR should act as a reminder that private networks are not the sole pathways through which regulatory convergence can occur. Cooperation occurring through transgovernmental networks or between individual experts are two other types of relations that support greater regulatory convergence. As recognized early on, I did not attempt to account for all these potential interactions that took place between European and American actors. I showed that industry associations contributed to this phenomenon by tending to include the rules of their counterparts with which they had previously worked. As entities that themselves represent multiple private companies and are closer to how data

protection rules are applied 'on the ground', this process of regulatory convergence is in itself significant.

In making this last point, I argued that private actors had a real agency in shaping the regulation of privacy in the last twenty years. If public authorities were often key in supporting the creation of forums where private networks came to exist, private actors were free to decide which rules they wanted to exploit and include in their self-regulations. In many ways, they mediated as much as they amplified the impact of public rules in one jurisdiction to the other. Public rules that were more likely to be exploited were indeed those that industry associations from the jurisdiction where they had first been enunciated had integrated in their self-regulations. Similarly, industry associations and certification companies that had a direct interaction with their counterparts from the opposite jurisdiction were more likely to also includes public rules from it. With whom private actors decided to interact thus had important consequences for public authorities.

All these different contributions provided a first detailed account of how the regulation of privacy in the transatlantic has evolved as a complex governance system. They showed how exploitation strategies in practice promoted greater regulatory convergence. Moreover, they emphasized that not all actors were equal in that process. Those that connected the two jurisdictions were seen as having a more influential role. While sharing many insights with the literature on policy diffusion, they highlighted that it was not a linear process. As new connections were formed between industry associations in both jurisdictions, new opportunities for exploitation emerged and progressively supported further regulatory convergence. This even allowed for a reversed influence where rules originally coming from one jurisdiction came back to it through new connections between private actors. The next chapter will now look at greater length at the second main process introduced in chapter 4: exploration. It will more specifically question when and to what extent do private actors also create data protection rules and further contribute to the evolution of data protection rules in the transatlantic area.

Chapter 6

Industry Self-Regulations: Innovation, Implementation or Regulatory Capture?

You put together two things that have not been put together before. And the world is changed. People may not notice at the time, but that doesn't matter. The world has been changed nonetheless.

Julian Barnes, 2013

The convergence of data protection rules in the transatlantic area over the last two decades has been and remains an important trend in the regulation of privacy. Even though the United States has yet to adopt a comprehensive privacy law at the federal level, many American private associations have progressively moved towards exploiting rules first set out by European actors. While being incomplete, this convergence through industry self-regulations is truly significant. As a matter of fact, the recent California Consumer Privacy Act (CCPA) that has been touted by privacy experts as bringing the United States closer to European privacy ideas (Schwartz 2019) and even dubbed as a 'GDPR-lite' by some commentators (Alikhani 2019) lacks many rules that private

associations had already incorporated in their regulations. Rules on collection limitations, purpose limitations, or data retention exploited by private associations in the United States were notably left out of the CCPA (Chander, Kaminski and McGeveran 2020: 19). Moreover, European associations have included rules first devised by American actors and not originally part of the Data Directive. Rules on the protection of children's privacy online that were first enunciated in the United States are one noteworthy example. Years before their inclusion in the General Data Protection Regulation (GDPR), they were indeed part of European industry self-regulations.

This is, however, only one part of the story behind the evolution of privacy regulation in the transatlantic area. In addition to converging towards each other, privacy regulations in the United States and the European Union have grown in terms of the number of privacy rules that they each promote. These have moreover not only came from the exploitation of rules that were originally part of each other's early model, but also from the exploration of new ones as shown in chapter 4. By pushing towards greater diversity, the creation of rules thus brought an important source of dynamism in the evolution of the regulation of privacy. In effect, as new privacy regulations were adopted, they never moved towards one single and definitive model (i.e., one fixed equilibrium) but instead constantly approximated an evolving one. Far from negative, this helped ensure that they kept up with changes in the world and new issues being raised by the growing use of personal data. The absence of regulatory innovations would otherwise mean that the same set of privacy guarantees would be applied to companies using personal data today than in the mid-1990s. Although various regulations nowadays aim and maintain to be 'technology neutral'[1] as stated in recital 15[2] of the GDPR, it is often harder to achieve than to say.

No regulator obviously has a crystal ball to know what technologies will emerge in the future and what new problems they will pose. Even with the best intentions, there can be situations where new data collection or processing techniques can difficulty be addressed by preexisting rules. With that in mind, the disruptive nature of new technologies should still not be overemphasized. It is often easy to fall for the argument that new technologies create unprecedented problems that previous regulations do not cover. The decision of how to apply them can in itself be an innovative act that can even end up

[1]Technological neutrally here means that the application of specific rules or requirements is not dependent on the technology being used.

[2]Recitals provide official information on how the articles of the GDPR should be interpreted and applied.

being codified as a new rule. The recognition of the 'living' nature of privacy regulation and any other regulatory standards may seem evident, but it is actually disregarded in most studies dealing with regulatory cooperation (Krasner 1991; Drezner 2007; Young 2015*a*). Explicitly or implicitly based on the ideas of coordination games, they view different models of regulation as static equilibrium competing with each other. As such, change is observed when an actor adopts the rules of another (i.e., harmonization) or recognizes them as equivalent to its own (i.e., coordination). Change coming from the introduction of new rules in the governance system of a given issue-area falls outside of the scope of their research as noted early on in chapter 2. The complex system approach developed in this research meanwhile brings attention to the endogenous process driving the evolution of a system and innovations that come from within it. By viewing the United States and the European Union as forming a complex governance system, we can more precisely see how interactions between their public and private regulators shaped the process of exploring new data protection rules. Who and what exactly drove this trend is the topic of this chapter.

One common argument is that private associations enjoy more flexibility in developing new rules than public actors (Abbott, Green and Keohane 2016; Overdevest and Zeitlin 2014). The relatively low degree of legalization of industry self-regulations compared to public laws is broadly seen as allowing "private regulators [to] more easily change the rules in response to new information or circumstances than can public regulators" (Green and Auld 2017: 270). Depending on the institutional framework, the adoption of public regulations moreover may be subject to multiple veto points and make the adoption of new rules increasingly difficult by public authorities (Newman 2008). Various studies have highlighted the potential of private authority to complement or fill in gaps in public laws (Auld 2014; Green 2013*b*; Renckens 2020). One interviewee for this research upheld such a line of thought:

> When you look at the GDPR, it adopts a very prescriptive approach. It goes some much into details that it may already need to be updated. You think about blockchain, AI and it's not clear how the GDPR will apply. That's where codes are so important. They can adapt so much faster than the law can. (Interview E15, done on February 19th, 2019)

Depending on the perceived legitimacy of these private regulatory actions (Bernstein and Cashore 2007), this can both be seen positively or negatively. Specifically looking at the digital economy, Spar (1999) and Ibanez (2008) were notably critical of

the risks of seeing large American companies becoming the *de facto* regulators while leaving a limited role to public authorities. In this chapter, I look at this question from a different angle and discuss the extent to which private actors contribute to the regulation of privacy by actually creating new data protection rules. I more precisely examine why the multiplication of private actors adopting data protection rules has actually not led to more regulatory innovations. The latter are once again understood as the inclusion of a rule that prescribes or proscribes a behaviour for the first time in the regulatory system.

Following the argument developed in chapter 4 (see especially section 4.5), I highlight that regulatory innovations are always the result of an assemblage of preexisting components or, in this case, rules. While this normally means that the multiplication of regulatory instruments can help bring more diversity and thereby support a more innovative environment, I will significantly show that fragmentation caused by the multiplication of private regulations actually limited the interest of private actors in experimenting with new rules and thus ended up being a sub-optimal outcome. While public authorities can help by proactively engaging with private actors and notably pushing them to coordinate themselves, I will point out that it will often mean further limiting their role as a regulatory innovator. As public involvement in the development of industry self-regulations can help achieve a greater level of rule compliance, public authorities could nevertheless find it a good trade-off.

This argument is developed throughout the next five sections. The first briefly explains how fragmentation, which is traditionally viewed positively in complexity theory and as a kind of necessary condition for the exploration of new ideas, can actually become an impediment to it and even lead to a form of regulatory capture when considering the role of private regulators. From there, the second section shows how different regulators have created new rules over the years. The third then highlights that despite not being null, regulatory innovations put forward by private regulators were less important than it could have been expected or sometimes even argued. The fourth then details how rather than innovating, many industry self-regulations precisely became tools of regulatory capture. The fifth section shows that the American and European public authorities were able to limit this result through proactive actions. This, however, often meant limiting their creation of new data protection rules as especially seen with the case of the European Union which, tended to adopt a more hands-on approach to industry self-regulation than in the United States.

6.1 Complexity, Regulatory Innovations and Private Rule-Making

As explained in chapter 4, a complex system approach pushes us to rethink the concept of innovation as a relational and systemic phenomenon (Carstensen 2015; Morin, Pauwelyn and Hollway 2017). While individuals or organizations are not inconsequential in that process, the new ideas that they explore are always contingent on what previously existed and became aware through their previous interactions. Again using the example of the iPhone, it basically means that the latter could not have been invented before the Internet, the GPS, and all its other technical components were and came to interact in the work of Steve Jobs and engineers at Apple. In the transatlantic privacy system, new rules can similarly only be based on what regulators behind them were made aware of in their past interactions. As it will be discussed at greater length in the next section, the 'right to be forgotten' could not have been created if the right to erasure had not already existed, which notably allowed to think that it was feasible to request that personal data be destroyed or, at least, be made inaccessible.

An important correlate of this systemic view is that innovating is a non-linear process. As depicted in figure 4.5 (see p. 112), the innovation process takes the form of a cycle where what used to be an innovation can always become a potential component for another. What distinguishes an innovation from a component in one is not their level of complexity nor a hierarchy between them. It is the time of their adoption. As time passes and innovations are created, there is hence an increasingly large set of basic components (i.e., technological parts or rules) that can be used to innovate again. Using data on patents filing in the United States, Hyejin Youn and his colleagues thereby show that the number of patents filed each year grew exponentially as the number of new technologies grew each year (2015: 4). In plain terms, the more innovations there are at a specific point in time, there more potential recombinations and, therefore, innovations there can be later on. A simple calculus can help demonstrate this. The total number of potential connections (p) between two individual components of a system is given by multiplying their total number (n) by the same number minus one (n-*1*) and dividing it by two:

$$p = \frac{n * (n - 1)}{2}$$

When applying this equation to a complex system made up of multiple components, we quickly find out that the number of potential innovations becomes intractable. If we take the present transatlantic privacy system for which this study found 71 rules, there would be 2485 potential combinations. Here, the components are the existing rules and each connection or link represents a possible innovation. As new connections are formed, new rules are added, and the number of potential new recombinations progressively grows larger. This is not even counting potential combinations involving more than two preexisting rules. In all fairness, not all combinations would necessarily make sense. Yet, many that now appear straightforward were not necessarily earlier on. The combination of a mobile phone with a GPS may now seem evident to most people but was certainly not as much in the early days of both technologies. It is often impossible to know what potential combinations will make sense at a future point in time as this will importantly depend on the context creating a demand for the exploration of new ideas or, in this case, rules. As noted in chapter 4 and 5, regulators will generally find it easier to exploit preexisting rules up until being faced with an exogenous shock or negative feedback. An exogenous shock here mainly refers to an event occurring outside of a given regulatory system and a negative feedback to an event occurring inside of it that lead regulators to reconsider how they see their object of regulation (see section 4.5). Depending on what this new information will highlight and the previous interactions of an actor, different new connections will become conceivable.

It is worth noting that this view of innovation closely relates to the concepts of "path dependency" and "increasing returns" that are both central to the historical institutionalist literature (Ma 2007). Indeed, it largely agrees with the idea that choices made today are influenced by those made yesterday and that regulatory changes may have larger effects than their original input[3]. In the latter case, it occurs as one regulatory innovation becomes a component in other ones and thus has a greater impact than the regulator behind it had originally envisioned. Yet, it differs in that it does not look at the political context or institutional characteristics to explain regulatory changes, like the presence of veto points or the room for rule interpretation (Mahoney and Thelen 2010: 19). It instead considers how the pool of existing rules and the interactions between the regulators behind them affect the creation of new ones over time. As such, it does not aim to distinguish between the forms that regulatory change can take (i.e., drift, displacement, layering or, conversion) but rather aims to explain how it relates to the

[3]This should perhaps come as no surprise as one of the main economist, Brian Arthur, credited for the concept of increasing returns in the neo-institutionalist literature in economy is also a leading complexity scholar (Ma 2007: 65).

broader structure of the regulatory system in place. This is in line with the aim of the complexity approach to comprehend the relation between the "whole and the parts" of a system as discussed in chapter 2.

The emphasis on the possibility for one rule to become the source of others (i.e., increasing returns) does not mean that the rate of innovations will constantly accelerate. As clearly seen in figure 4.3 (p. 109), the number of new rules created actually slowed down since the mid-2000s. As opposed to the billiard ball metaphor of linear system, a good metaphor for non-linear systems is the one of a sandpile (Cederman 2003). While the former envisions a system where every input has a proportional effect on the output, the latter sees a system in which small changes might have almost no effect or a much larger one than its creator can even anticipate. In the present case, this notably means that one regulatory innovation could lead to the creation of no other data protection rules, while another one could trigger the creation of many.

In this light, the multiplication of privacy regulations and data protection rules can be seen positively. Far from being a source of disorder or 'chaos', it ensures that a given regulatory system has the internal capacity to keep up with a changing world. As legal scholar J.B. Ruhl rightfully points out,"[r]obust legal systems must evolve" and be "capable of responding to changing context by changing itself", otherwise they are bound to "die" just as any other social or natural systems (2014: 574). By providing more resources that regulators can tap in to explore new ideas, the multiplication of regulations and rules precisely helps ensure this. Indeed, previous research emphasized that institutional redundancy and diversity did not have the negative effects that efficiency proponents will traditionally attribute to it (Kelley 2009; Kellow 2012; Low et al. 2003; May, Levin and Sugihara 2008; Ruhl 2014). More than being a costly repetition of resources, it helps ensure the system is both more flexible and adaptive (Keohane and Victor 2011; Pauwelyn 2014). In the present case, it potentially allows more connections to be made by a more diverse set of regulators than if there were only one regulator and one regulation in charge of setting data protection rules for the whole transatlantic space. With that in mind, it is puzzling that the regulation slowed down as much as it did since the mid-2000s. Although it should not be expected that the rate of innovations remains constant over time, the fact that very few new rules were created still opens up several questions as the collection of personal data became increasingly widespread and its use controversial. As industry self-regulations were moreover supposed to provide an even

more flexible form of regulation, it is quite surprising that there were not more regulatory innovations in recent years.

What actually stands out is that the resulting fragmentation from this multiplication of rules can produce negative effects too. Discussing the growing body of research on regime complexity, Drezner (2009) emphasizes the risks that a fragmented international system can notably pose for weaker states. As he points out, the flexibility provided by the existence of multiple institutions will often work to the advantage of states with sufficient resources to navigate the growing complexity of global governance issues. It may also help powerful states to go around their agreed obligations by allowing them to create and exploit incoherencies among various institutions, thereby undermining the very role that institutions are supposed to play according to liberal scholars: promoting international cooperation (Keohane and Martin 1995). In the rest of this chapter, I emphasize yet another negative outcome of a fragmented system when taking into account the role of private actors. As it will be further discussed below, fragmentation can become a hindrance to the creation of new rules by private actors by producing "second-order information asymmetries" (Renckens 2020: 41).

One of the goals of industry self-regulations is to solve information asymmetries by allowing companies to signal their good practices to consumers or business partners with which they interact (Prakash and Potoski 2012; Vogel 2008). By making use of these tools, they can build up their reputation and attempt to gain or minimally maintain market shares. As noted by one interviewee for this research, "privacy seals main use for consumers is to show that the companies they interact with had their services tested and that they are reliable. It is a bit of a question of prestige too" (Interview E19, done on March 5th, 2019). Similarly, another interviewee explained the choice of developing an industry self-regulation by "the need to preserve public trust" (Interview E22, done on March 11th, 2019). Following this line of thought, various business strategists and representatives from the private sector touts that privacy can be seen as a business opportunity (e.g., Garber 2018; Hoffman 2014). In effect, good data practices can be sold as an added-value to consumers. We see this with the rising number of applications or software that present themselves as being privacy-friendly. As the number of self-regulations and concomitant certifications rise and make the market more fragmented, the signalling value of these private regulatory programs, however, progressively decreases due to 'second-order information asymmetries'. The latter occur when the multiplication of industry self-regulations make it "unclear (or unknown) how [they] compare in

terms of the stringency and scope of their standards, internal governance procedures, or compliance verification processes" (Renckens 2020: 41). In that situation, consumers or businesses are faced with a traditional market for lemons (Akerlof 1970) as they cannot easily distinguish the bad from the good.

Even though the shadow of hierarchy or the threat of regulation (Büthe 2010; Green 2010) may continue to push private actors to develop codes of conduct or other self-regulatory tools, private actors lose their incentive to go beyond legal compliance and innovate (Bartley 2014; Cashore and Stone 2014; Prakash and Potoski 2012) as they will not make any real reputation gains of doing so. When they do create new rules, they can also find it easy to not implement them. By reducing the clarity of one's obligations, the multiplication of regulations and rules dealing with privacy often makes it easier to renege them at the implementation stage (Alter and Meunier 2009). Instead of supporting greater dynamism, fragmentation then ends up limiting it and can lead to regulatory capture. This sub-optimal outcome is here understood as a situation where the regulatory process is controlled " by those whom it is supposed to regulate or by a narrow subset of those affected by regulation, with the consequence that regulatory outcomes favour the narrow 'few' at the expense of society as a whole" (Mattli and Woods 2009: 12). This can more specifically mean the absence of regulation, lenient regulation, or unenforced regulation. As it will be seen, these can occur simultaneously and involve both public and private forms of regulation. While sometimes limiting the positive 'experimenter' role that private regulation can play (Bartley 2011; Green and Auld 2017; Overdevest and Zeitlin 2014), public interventions then appear essential to solve this situation. This was at least the case in both the United States and European Union, even though to different degrees. Before turning to this, the next section will empirically demonstrate how the combination of preexisting data protection rules led to the creation of new ones in the transatlantic area since the adoption of the European Data Directive in 1995.

6.2 Regulatory Innovations in Transatlantic Privacy Regulations

As per the findings of this research, the total number of data protection rules has gone from around 40 in 1995 to 70 today. These include rules on cookie notice and consent

discussed previously and that are now widely adopted, as well as more recent rules on data portability and the 'right to be forgotten' recently added in the GDPR. Going over all these new rules would be too long. Not all are moreover equally interesting. Six regulatory innovations will hereafter be presented to showcase how the innovation cycle introduced in section 4.5 (see p. 112) and just discussed operates. These were selected to reflect the regulatory activity of both public and private actors over time. Special attention was also given to discuss recent rules that have been touted as significant innovations, notably by the European Commission (2015), to highlight their important lineage with previous rules. This specific selection was importantly not meant to allow for a generalization of the process innovation through recombination as the previously cited study on patent could (Youn et al. 2015) but to provide an in-depth understanding of how it practically operates (Della Porta 2008). Table 6.1 summarizes these six innovations, who were behind them, and what were the previous principles or rules that they combined. The rest of this section reviews each of them.

Table 6.1: Six regulatory innovations since 1995

Year	Rule	Creator	Public/Private	Combination
1997	01.09 Automated or passive collection (cookie notice)	AICPA, IA & IRSG*	Private	01.01 Privacy statement & 01.03 Data types and purposes
1997	03.03 Third-party source	IRSG	Private	03 Collection limitations & 06 Data quality
1997	14 Education	IRSG	Private	01.01 Privacy statement & 07 Individual participation
2002	12.03 Data breach notification to the data subjects	California State	Public	01.01 Privacy statement & 10.01 Commitment to data security
2016	07.03.02 Right to be forgotten	European Court of Justice	Public	07.03.01 Right to erasure & 06 Data quality
2016	07.10 Data portability	European Commission	Public	05.01 Sharing with independent controller & 07.01 Access and review &

* All in these organizations adopted the same new rule in their regulations adopted the same year.

The first innovation worthy of mention is the requirement to notify users that their personal data is being passively collected. Again, when visiting a website or using an online application, companies behind them will often collect information about their users (e.g., IP address, geographical location, etc.). As opposed to an active form of data collection, it occurs without the data subject being always aware of it. No forms

or questionnaires are completed. It simply happens in the background as a website or online service is being used. This specific form of data collection is nowadays prevalent and poses a problem to the "privacy as control" dominant paradigm in Europe and the United States introduced in chapter 3. Without knowing that our personal data is being collected, it is evidently hard to control its future use. Following their creation in the mid-1990s, there were repeated calls by various activists to make the use of such tools more transparent (Hill 2001). Interestingly, some industry associations were the ones innovating in this case, not public authorities. In 1997, three industry associations (i.e., the American Institute of Certified Public Accountants (AICPA), Internet Alliance (IA) and Individual Reference Services Group (IRSG) included a rule in their respective privacy regulations requiring that companies notify their users that their personal data is being collected through passive means. The code of the IA was the most straightforward formulating this requirement in the following way:

> In addition to the types of information collected, online operators should make clear how personal information is collected. For example, disclosure should be made as to whether the information ***is collected automatically or affirmatively***. (IA Code 1997: 1; emphasis added)

Here faced with a new technological development, these three private associations used previous transparency requirements to create a new rule. The need to have a privacy statement explaining their data practices (01.01) and to explain what type of data they collect (01.03) are two rules that all three had already incorporated and could have served as a basis for the three associations to indicate that their members should also explain *how* they collect personal data. This is significant and shows that private actors can indeed experiment and go further than their legal requirements. Not all private associations were in effect as prone to do so as this particular form of data collection was at the heart of the business model of many online companies in the early days of the Internet. Chiefly, the Network Advertising Initiative (NAI) that represented some of the biggest users of cookies and other passive data collection methods did not include such rule in their 2000 code of conduct, which already existed at that point. It was nevertheless adopted by the FTC Fair Information Privacy Principles (FIPPs) as noted above and later on became exploited by most public and private regulators. Since 2013, the NAI even includes it in its code of conduct.

A second regulatory innovation that merits attention relates to the source of personal data. Up to now, this research has mostly talked about data collection as being

closely connected with a specific data subject. Private companies have, however, for long exchanged personal data and built up profiles on individuals by using information from third-party sources. An entire industry was actually built around this business interest. Companies named data brokers aggregate personal data from various sources and develop increasingly accurate personal profiles that they then sell to other companies (Pasquale 2015: 30-1). One source of concern is that it was not always clear where the information being exchanged is originally coming from and if it can be trusted. As a matter of fact, mistakes in the combination of personal can end up causing severe harm when such data is used for making sensitive decisions, like credit decisions for a mortgage. To resolve this situation, leading companies in the data brokerage industry represented by the IRSG specifically indicated that they should actively assess the source of personal data before considering it:

> Individually identifiable information shall be acquired from only sources known as reputable in the government and private sectors. ***Reasonable measures shall be employed to understand an information source's data collection practices*** and policies before accepting information from that source. (IRSG Code 1997: 2; emphasis added)

This is a second example of the capacity of private actors to innovate. While still vague[4], this requires to go further than what other public or private regulations were asking at the time. In need to prove to American public authorities that they could self-regulate themselves (Gellman and Dixon 2016), they added this rule by combining two principles that have been at the heart of the protection of privacy since the adoption of the OECD guidelines in 1980: the need to limit data collection (03 Collection limitations) and ensure the quality of personal data (06 Data quality). When going through the code of the IRSG, the rules related to these two principles are presented next to each other and it is clear that a strong link is drawn between the two. Interestingly, this regulatory innovation was not widely exploited. Only 9% of all 124 public and private regulations coded in this research included it. Indeed, not all innovations ended up having a large impact on the complex governance system for privacy. In line with the argument presented in the previous chapter, this depends on the position and the interactions of the actor(s) promoting it. In the case of the IRSG, despite representing important

[4]In fairness, new rules adopted by public authorities also often start by being quite broad and become more precise over time. The early enunciation of the FIPPs by the FTC was very broad and the language was not particularly constraining. Although rules in Europe tend to be defined in more constraining terms, the Data Directive was similarly much vaguer on how many rules should be implemented than the GDPR is today.

companies, it had limited interactions with other public and private regulators following its creation. Its existence was also short-lived as the companies behind this initiative ended it in 2002 and had been inactive for a few years before that (Gellman and Dixon 2016).

A third regulatory innovation by private actors and again introduced by the IRSG relates to the education of individuals about privacy and business data practices. One broad issue with the protection of privacy is that data practices are often obscure to individuals. Just as the sources of personal data are not always clear, the uses and decisions made based on it are also often not obvious for most people. This generally contributes to the broad feeling that we have given up our privacy in this online world. One way to fix this is by educating individuals about data governance and how they can control their information. This is what the members of the IRSG precisely engaged themselves to do back in 1997:

> Individual reference services shall individually and through their industry groups ***make reasonable efforts to educate users and the public about privacy issues associated with their services***, the types of services they offer, these principles, and the benefits of the responsible flow - of information. (IRSG Code 1997: 2)

In this case, this rule builds on the previous obligations of private companies collecting personal data to be transparent about their data policies (01.01 Privacy statement) and offer choices about how personal data is being used to data subjects (02.01 Original consent). In the end, the goal of educating individuals is to inform them about how they can express their preferences and control their information. This is perhaps most evident in how the NAI formulated its own requirement to educate consumers in its code of conduct of 2000, which indicates that its members should educate their users "in [their] privacy statements" to "facilitate consumer awareness and provide a convenient mechanism for consumers to exercise choice regarding such data collection and/or use" (NAI Code 2000: 9). Although both organizations did not officially have direct interactions with each other, the exploitation of this rule seemed possible by the fact that these two organizations still shared similar members (e.g., Acxiom). Since then, many private associations representing advertising companies, like the Direct Marketing Association (DMA) and the Interactive Advertising Bureau, included a rule requiring their members to educate their consumers about their data practices. This ended up being part of the

code of conduct developed by the Digital Advertising Alliance and in turn being exploited by European associations as discussed in chapter 5.

A fourth important novel rule since 1995 is the one requiring private companies to notify individuals on whom they have personal data if they were affected by a security breach. As opposed to the previous three examples, this specific rule was created by a public authority and, more specifically, the government of the State of California. With the rise in the collection of personal data came growing risks of identity theft. Following previous security breach scandals, including one incident involving 265,000 California state employees, Californian legislators decided to adopt a law that would require private entities to be more transparent about security breaches (Burdon 2010; Preston and Turner 2004).

> A person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, ***shall disclose a breach of the security of the system*** following discovery or notification of the breach in the security of the data to a resident of California (1) whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person, or, (2) whose encrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. (California Civil Code s. 1798.82(a))

As made evident by the wording of the obligation, it combined two principles that were at the heart of the regulation of privacy in the United States since the early formulation of fair information practices in the 1970s: notice and security. Up to that point, that minimally meant that private companies would inform consumers of their privacy policies (01.01 Privacy statements) and commit themselves to protect the personal data of their users (e.g., 10.01 Commitment to data security). These were part of the FTC FIPPs and most industry self-regulations in the United States. When put together, they form the basis of the obligation to notify users of potential security breaches affecting their personal data. Since then, few American private associations have, however, included this requirement in their industry self-regulation and limited its exploitation by their European counterparts as pointed out in chapter 5. Nevertheless, it still made its way in Europe first through its Directive specifically aimed for the telecommunications sector (e-Privacy Directive) and then in the GDPR.

Back in 2002, similar concerns than in the United States over identity theft and misuse of personal data led to the inclusion of a requirement in the e-Privacy Directive to inform users of potential security breach risks associated with their services (art.

15(2)). This slightly differs from the rule developed in California as it pertains to "an unrealized contingency, not a realized security breach" (Preston and Turner 2004: 468), and interestingly shows that faced with similar problems and set of original resources, two actors may still not come up with the same innovation. The GDPR has now embraced the American rule and provides that companies should notify the individuals affected by a data breach. It even goes further by defining data breaches more broadly and, notably, including not only the case of a security breach but 'unauthorised disclosure' and 'accidental destruction or loss' that would make it impossible for individuals to access their personal data. In the latter case, it is an example where the new rule became a component of another new one by combining it with the rule requiring companies to allow anyone to have access to their personal information hold by a private entity (07.01 Access and review). This perfectly exemplifies the non-linear process of regulatory innovation.

The fifth regulatory innovation that has attracted a lot of attention in recent years is the famous 'right to be forgotten' included in the GDPR. As previously mentioned (see chapter 4), the Data Directive importantly already provided that data subjects could ask for their personal data to be erased. The big change in the GDPR is that it allows for more grounds to ask for it. Rather than only allowing individuals to ask for the erasure of erroneous data, they can notably require "the controller ***the erasure of personal data***" that "are ***no longer necessary*** in relation to the purposes for which they were collected or otherwise processed" (GDPR art. 17(a)). These two elements that form the new 'right to be forgotten' clearly draw from the previous rule allowing individuals to request the erasure (07.03) and the previous obligation of private companies to only maintain accurate and useful data (06 Data quality). This was actually explicitly said in the decision by the European Court of Justice (ECJ) that drew the contour of the right to be forgotten two years before it was included in the GDPR (Google Spain SL and Google Inc. v AEPD and Mario Costeja Gonzalez, 2014 Case C-131/12). In paragraph 94 of its decision, the ECJ specifically uses article 6 of the Data Directive relating to the principles of data quality to explain that "initially lawful processing of accurate data may, in the course of time, become incompatible with the directive where those data are no longer necessary in the light of the purposes for which they were collected or processed" and make legitimate a request for its erasure.

As a relatively new rule, it has yet to been widely exploited and re-used to create other new rules. At this point, there is notably still few private actors that have moved forward and included it in their own regulation, and especially in the United States.

TrustArc and Verasafe are two exceptions. These two American certification companies have indeed included it in their latest self-regulations (TrustArc 2018 Enterprise certification standards & Verasafe 2017 Privacy Certification Program). This might not be stranger to their known interest to act as certifiers for the GDPR (Interview E31 and E33), a new role that private actors can now play by indicating that specific companies comply with the GDPR. While no private certificators have been recognized by the European Commission or its Member States, the potential interest of being among the first ones to play this potentially lucrative role seems to have led both of them to include the new 'right to be forgotten' in their global certification service as well as other rules found in the GDPR. As a matter of fact, they now both make multiple references to the GDPR in their respective privacy programs. This interestingly highlights a new pathway for the exploitation of European rules by American private actors. Rather than occurring through their interactions with their European counterparts or an international agreement delegating tasks to them, the European Commission can give them an official role in the implementation of its rules globally.

The sixth and last new data protection rule created in the last 20 years and here reviewed is the right to data portability. Just like the 'right to be forgotten', it raised great interest following its inclusion in the GDPR (art. 20). One rising concern in the data economy is the accumulation of data by a few large companies that could lead to competitive bottlenecks (Stucke and Grunes 2016; Srnicek 2017; Zuboff 2019). This issue was specifically recognized by then-Vice President of the European Commission responsible for Competition Policy, Joaquin Almunia, while introducing some of the new rights in the early commission's legislative proposal for the GDPR. In his speech, he noted that a right to data portability specifically aimed to ensure that any individuals de not become "locked in to a particular company just because they once trusted them with their content" (Almunia 2012: 4). To fix this, the right to data portability foresees that:

> [T]he data subject shall have the right to ***receive the personal data concerning him or her***, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have ***the right to transmit those data to another controller***

This specifically builds on two previous rules found in the Data Directive. First, and as duly noted by the participants to the FabLab workshop on the application of the

GDPR by the Article 29 Working Party[5], it extends the preexisting right to access that was part of the Data Directive of 1995 (Article 29 Working Party 2016), which specifically indicated that individuals could require to have communicated to them "in an intelligible form of [the] data undergoing processing" (art. 12). The second part of the right to data portability adds to the right of access by requiring that data subjects received their personal data in a format allowing them to transmit to another controller of their choice. This combines rules on data transfer that had up to then only been applied between data controllers. Interestingly, this novel combination also appears linked to the rule on the portability of phone numbers that was part of the European regulatory framework since the adoption of the Universal Service Directive in 2002 (Article 29 Working Party 2016). The latter foresees that consumers can change service providers and still keep their phone numbers. This represents an example where an outside source of information also contributed to shaping a new rule.

Just like the 'right to be forgotten', the right to data portability is still new, and almost no private actors have added to their industry self-regulation. TrustArc, which again has shown an interest in being a GDPR certifier, is one of the sole exceptions and has included it in the 2018 version of its Enterprise certification standards. It remains to be seen how it will be exploited in the future, but the fact that the right to access is one of the most widely adopted, present in 90 of the 124 coded regulations for this research, is certainly a sign that it could be taken up by many.

These six examples of regulatory innovations each show how the innovation cycle depicted in figure 4.5 (p. 112) operates. Following a negative feedback or an exogenous shock creating a demand for exploring new solutions, regulators combined preexisting rules to create new ones. Once created, these new rules became additional resources that could be exploited by others and be used to produce other regulatory innovations. They also showed that both public and private actors could innovate and actively support the development of privacy regulation. Out of the six innovations reviewed, half were in effect the result of the work of private associations in the United States as displayed in table 6.1. This should, however, not be taken to mean that both have been contributing in the same way to the evolution of data protection rules. The next section will provide more details on the nature of private regulatory innovations and how they relate to public ones.

[5]Once again, the advisory body created by the Data Directive to follow its implementation throughout the Member States (see chapter 3 and more specifically section 3.5.

6.3 Private Regulators: Innovative Rulemakers?

As just seen, the creation of data protection rules has not been the sole purview of public authorities since the European Data Directive was adopted in 1995. At different points in time since then, private actors have been innovative and have gone further than merely exploiting public rules in the development of their industry self-regulations. Varying interviewees for this research representing both the public and private sector have recognized this explicitly. When asked if private actors were going beyond legal compliance, some notably held:

> [Codes] must go a little bit further than the law. [...] There must be an added-value and it cannot be a simple reflection of what the GDPR is requiring. (Interview E12, done on February 11th, 2019; translated from French)

> Every seal has the law as its base, but you always need something on top. You cannot simply repeat the law. (Interview E19, done on March 15th, 2019)

> It does create new obligations. That's why it is called self-regulation. [...] You need to do more than what the law requires you to do. (Interview E21, done on March 21st, 2019)

> I would actually say that this [private] regulatory sandbox is incredibly valuable. It can better keep pace with the technological change that hard law ever can and it brings a flexibility that public authorities lack. (Interview E28, done on April 10th, 2019)

This capacity to innovate is confirmed by the data collected for this research. Figure 6.1 shows that out of all the rules found in this research (i.e., 36) to have been created after the adoption of the European Data Directive, more than half (61%) were created by private actors. When adding the rules found in this research as existing before 1995 and significantly those in the European Data Directive, we get the reverse picture where it is public actors that have been most innovative by the exact same margin (61%). These findings already highlight that industry self-regulations have not been merely applying public laws and confirm previous works that had identified that specific rules, like on the protection of children's privacy online (Lascoutx 2002: 649) or requiring the creation of a data protection officers (Thoma 2012: 277), had first been enunciated by industry groups or private companies. At the same time, they demonstrate that it is far from a given that private actors are necessarily more innovative or experimenting

with more new rules than public regulators are, and this actually varies depending on the time period considered.

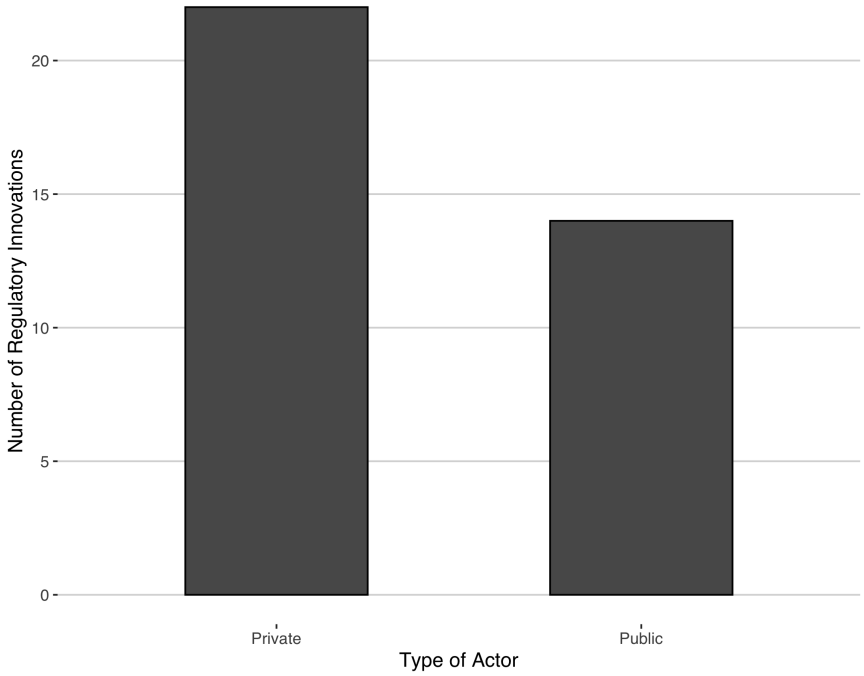

Figure 6.1: Sum of data protection rules first enunciated by public and private actors after 1995

The level of innovativeness of private actors must, however, be further qualified. This broad depiction of their capacity to create new rules in effect does not assess the content of their regulatory innovations nor where and when they tended to innovate. Taking these elements into consideration is essential to evaluate the contribution of private actors to the regulation of privacy and consider and if it indeed supported the development of a more comprehensive regulatory approach in the public interest. In other words, the contributions of public and private actors should be assessed both quantitatively and qualitatively.

A first important specification to make is that the rules created by private actors have largely aimed at bringing clarity on the application of preexisting principles. As noted when introducing the database used for this research in section 4.2, principles are understood as broad expressions of a goal to achieve and rules are more specific prescriptions of how to achieve it. As opposed to technical standards, rules remain, however, vague on how they should be technically implemented. Out of the 14 broad

principles according to which the different data protection rules identified for this research are divided, only three were originally put forward in an industry self-regulation. These are the rules that pertain to the development of private compliance mechanisms, the education of individuals, and the protection of children's privacy. All of the other broad and well-known privacy protection principles, including transparency, consent, individual participation, security, and collection and use limitations, were first found in either a law or public guideline. This was identified by considering which type of actor first put forward a rule for each of these principles and, in many cases, they go back to the adoption of the early report on Fair Information Practices by the United States Department of Health, Education and Welfare in 1973 or the OECD Guidelines in 1980.

This denotes one key characteristic of private forms of regulations, which is that they rarely aim to create broad new principles but instead work to help their members or certified users to respect broad regulatory goals previously set by public authorities. In the United States, where no comprehensive privacy law is in force at the federal level, private actors still largely implement public principles. This is something that constantly came up when discussing the role of private rules with multiple interviewees for this research and even led to sometimes seemingly contradictory answers. Indeed, many interviewees were prone to simultaneously maintain that their industry self-regulations were going further than the law but were not creating new legal obligations. One interviewee, for example, stated that self-regulations "needed to go further than law", but that "they do not create rules" (Interview E12, done on February 11th, 2019). Similar thoughts were held by one interviewee from the private sector who held that industry self-regulations were going "beyond what is required in the law" and still maintained that their "role is to try to implement, not create rules" (Interview E34, done on May 6th, 2019).

This terminology issue is both inconsequential and telling. On the one hand, it speaks to the different understanding that the concept of rule can take and which is understood broadly in this research. Many interviewees tended to equate the concept of rule to 'legal rules' or those enacted by governments. In turn, the regulatory activity of private actors was not seen as the same as rule-making. There are, however, many different and broader ways to understand the concept of rule, and the fact that a requirement aims to operationalize a broader principle or specify another rule does not impede it from being characterized as a rule. For one, the 'right to be forgotten' is here considered to be a rule and is a specification of how private companies should manage the broader right

to erasure that individuals have. On the other hand, it does point to the important fact that if private actors actively contributed to the regulation of privacy, their regulatory innovations were often more limited in scope and generally tended to specify public ones. As another interviewee specifically mentioned, the creation of "principles very broadly, that is for privacy laws. What we do is working with the technical specifics. That's where there is a room to develop new rules" (Interview E40, done on May 14th, 2019).

In line with this, this research found that the specific list of information that private actors need to disclose in their privacy statement was partly determined by industry self-regulations. This reflects the simple fact that governments knew they wanted to promote the principle of transparency, but they did not necessarily know from the onset what were all the different types of information that private companies could and should share with individuals from whom they collect personal data. While being a valuable contribution, these types of innovations can be viewed as being qualitatively less significant than the creation of the requirement to have a privacy statement. Going back to the definition of principles and rules given in chapter 4 (see p. 93), while changes in rules will generally mean a change within the boundaries of the current privacy system and continuity, change in principles are more disruptive and could even lead to a change in the privacy paradigm in place. Previous scholars already emphasized that we are unlikely to see a pure form industry self-regulation system emerging without any state intervention (Börzel and Risse 2010: 116). This additional finding highlights that we are moreover unlikely to see fundamental changes in the regulation of an issue-area being spurred by private actions.

A second element to point out about the regulatory innovations put forward by private regulators relates to the time of their adoption. As previously indicated, one common argument in favour of industry self-regulation is the more flexible form of governance that they can offer to public form of governance (Abbott, Green and Keohane 2016; Overdevest and Zeitlin 2014). This is one of the reason the European Commission in effect has early on decided to give a role to private actors to deal with various issues, including privacy protection that it takes to be a fundamental right (European Commission 2001*b*). Flexibility can significantly mean different things and it was often described by interviewees for this research as allowing private actors to tailor broad principles and rules to specific sectors. This certainly fits the type of regulatory innovations just described.

Offering the opportunity to adapt the way rules should be applied to a specific sector is yet only one way private actors can provide flexibility. Another is by taking stock of negative feedback or changes to adapt their regulations accordingly. As it is well-known, the process of modifying public laws can be long and cumbersome. The GDPR modified a Directive that had been adopted twenty years before[6] and took four years to be adopted after the European Commission (2012*a*) first proposed a comprehensive reform of the European privacy system. In the United States, this assumed flexibility of industry self-regulations has been and remain one of the main selling points for it as discussed in chapter 3 (see especially section 3.3).

Looking at the time when private actors have innovated interestingly tells a different story. Figure 6.2 shows that far from being constantly in the process of exploring new rules and displaying great flexibility, regulatory innovations by private actors have largely been circumscribed to specific time periods where public pressure was particularly high and often close to when regulatory innovations by public regulators appeared. Indeed, most rules created by them was at the end of the 1990s and early 2000s, a time where the European Commission was working hard to ensure its Data Directive was thoroughly applied and the United States was actively trying to push private actors to show they were able to self-regulate themselves as it was negotiating the Safe Harbor Agreement with Europe (Farrell 2003: 290). The organization of workshops by the FTC and the clear threat that public regulations could be adopted in the absence of actions on their part notably led American industry associations to showcase their goodwill. As time passed and public scrutiny diminished, they progressively stopped exploring new rules and mainly relied on exploiting rules that had notably been created in Europe. As discussed in the previous chapter, the cost of doing so was lower and private actors had no real interest in going further.

This is not to say that private actors have done nothing after these first few years. As just indicated, many continued to exploit rules that other public and private organizations had developed. They also sometimes aimed to apply their self-regulations to new technologies or techniques of data collection and use. For example, some developed codes of conduct or certifications specifically for data practices using mobile phones. Yet, they did not create new data protection rules, even though they would regularly hold

[6]Importantly, other directives like the ePrivacy directive were adopted in between contributed to complement the European Data Directive, but it was generally for a specific sector and there was a big change in the European privacy system between the European Data Directive and the adoption of the GDPR.

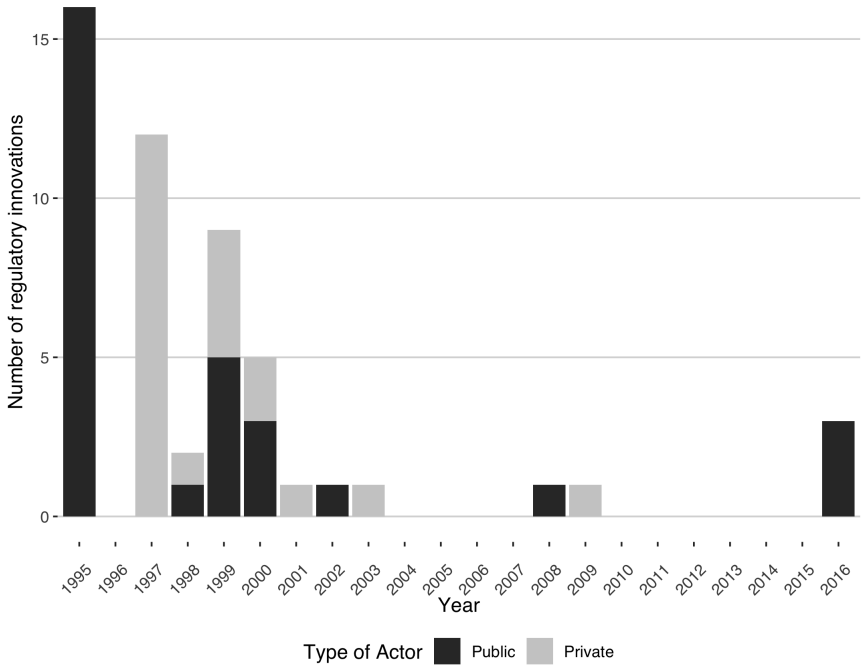

Figure 6.2: Sum of new data protection rules by type of actors and years

to have a better understanding of what are the challenges with protecting the privacy of individuals as many interviewees for this research still held. It is noteworthy that we cannot expect the development of new rules to be continuously high as it depends on the presence of negative feedback or exogenous shocks to spur demand for it. Having said that, the almost complete void of innovations for a decade is quite significant and especially as it goes hand in hand with the rise of the digital economy.

Seen in this light, the contribution of private actors to the creation of new data protection rules is not anything, but certainly not as significant as it may seem at first sight. For one, it does not so much attempt at creating new obligations than specifying those that public authorities have already set forth for them. Moreover, they do not appear to be so flexible and adaptive that they would regularly create new rules. In the ten years before the adoption of the GDPR, almost none did so. Considering that they sell themselves as better to cope with change than public laws, the fact that their role in exploring new rules is not that much more significant is particularly noteworthy. The next section will argue that instead of becoming a potential source of creation, the

multiplication of industry self-regulations and rules actually limited the interest of private actors to explore new rules and even spurred a form of regulatory capture.

6.4 Fragmentation and Regulatory Capture

Despite contributing to the exploration of new data protection rules, industry self-regulations have in many ways not fulfilled their promise of offering a more flexible and adaptive form of governance than public authorities. In addition to having a limited impact on the development of most of the core data protection principles and not being really active for the decade leading to the adoption of the GDPR, many even ended up not truly supporting greater privacy compliance. Over the years, multiple reports indicated that codes of conduct and private certification services were not properly implemented and had not provided the guarantees that they were supposed to. In many ways, various industry self-regulations appeared to act as regulatory decoys used to give a false impression that they make the regulation of privacy more robust while they prevent further regulation by public authorities.

In the United States, one case epitomizing this perfectly is the IRSG, which is actually the most innovative private regulator according to the findings of this research. With the inclusion of eight new rules, its 1997 principles are in effect the industry self-regulation that included the most regulatory innovations (see figure 4.4 on p. 110). Among the three principles first created by an industry self-regulation, it was also behind the one requiring the development of private compliance mechanisms. Indeed, it was one of the first two industry groups to foresee that its members would have to go through an annual 'assurance review' verifying their compliance with their data protection rules. As one interviewee with close knowledge of this early initiative explained, it was supposed to be "the first self-regulatory framework that had teeth behind it" (Interview E37, done on May 14th, 2019). In practice, though, it largely ended up being a tool used by the industry to stop the American government from further regulating -their activities rather than really aiming at improving the regulation of privacy. Following its inception, it did not make public the reports on its members' compliance that it was supposed to do following their assurance review. It was thereby never possible to verify if its principles were actually implemented (Gellman and Dixon 2016: 55). More so, it stopped all its activities five years after it had developed its principles citing the adoption of the Gramm Leach Bliley Act as making its services useless even though none of its members were

financial institutions covered by this law (Gellman and Dixon 2016: 56). In addition to leaving many of its members free to act as they wished with the personal data in their possession, it also limited the broader impact of its regulatory innovations. As it ended up its activities quite quickly and did not build as many interactions with other regulators as others did over the years, some of them were not largely exploited as it was mentioned while discussing the six examples of regulatory innovations given above.

Over the years, many other industry associations or certification companies having put forward a code of conduct or privacy certification less innovative than the IRSG were also found to have failed to enhance the privacy guarantees offered to individuals. As one of the leading providers of privacy certifications in the United States, TrustArc (formerly TRUSTe) has, for example, only produced two regulatory innovations. Yet, on multiple occasions, it made the headlines for its various regulatory failures. Back in 2000, it notably gave its seal to the company RealNetworks, even though the latter was collecting personal information on individuals without them being aware of it (Haufler 2001: 102). The fact of the matter is that TrustArc's certification was limited to RealNetwork's website and, as such, did not apply to the software of the company that was used to collect personal information. Despite extending its program to data collection practices from software following the public outcry, it repeatedly failed to conduct annual re-certifications as its certification program stated it should have been doing (Federal Trade Commission 2014). One interviewee for this research even held that for a long time TrustArc looked as "if it aimed to make things more cloudy for consumers" (Interview E37, done on May 14th, 2019). The NAI is another oft-cited example of the disappointing contribution of industry self-regulations (Dixon 2007: 37; see also Hoofnagle 2005). Since its creation in 2000, this research only found two regulatory innovations in the different codes it adopted over the years. Meanwhile, oversight of its members' data practices was repeatedly found to be lacking. In its early years of activity at the turn of the millennium, reporting on its members progressively stopped and the number of active participants dropped significantly (Gellman and Dixon 2016: 59-60).

While both TrustArc and the NAI underwent changes following these criticisms and now maintain to more adequately check the compliance of their member companies, there are still important concerns to have. TrustArc merely indicates in its certification program that private companies using its services must "monitor, and periodically assess and audit the effectiveness of controls and risk-mitigation initiatives" (TrustArc Certification Assessment Criteria 2018: 33). How and to what extent this is done is not

specified. Meanwhile, the NAI does go further and publish a report assessing its members' compliance with its self-regulatory program every year. There is, however, little information about the actual data practices of its members in it. Most of the time, it indicates that "evaluated members" have fulfilled detailed questionnaires indicating that they were respecting its code of conduct. Taking into account that its 2018 code of conduct still exclude many prominent rules found in other public or private regulations, like that data collection should be limited to specific purposes (03.01 Purpose limitations), that the transfer of personal data to third-parties should be based on an individual's consent (05.01.01 Consent) and that individuals should have the right to request to have their personal data deleted (07.03 Erasure), the NAI's contribution to making the regulation of privacy more robust appears even more questionable.

On the European side, similar instances of such regulatory failures were not as common, but conflicts over how to enforce industry self-regulations also drew a lot of attention and actually led to many never being formally adopted. As previously discussed (see chapter 5), business and consumer representatives that had worked with the support of the European Commission on building a European trustmark that would have established common rules for companies selling online ended up dropping this project as they were unable to agree on how it should be enforced (European Commission 2004: 8-9). One interviewee for this research that had been working on this project specifically noted that disagreement over the need for a third-party verification system was the main source of disagreement (Interview E7, done on February 4th, 2019). More recently, two codes of conduct developed with the financial support of the European Commission and aimed at defining privacy rules in the cloud computing and health sector failed to be adopted for similar reasons. In its opinion on the code of conduct for the cloud computing industry, the article 29 working party specifically raised many issues with the governance structure of the code and how it would check its users' compliance (Article 29 Working Party 2015). These divergences over how industry self-regulations should be enforced are evidently one reason why there has only been one code of conduct officially approved at the European level in the twenty years separating the adoption of the Data Directive in 1995 and the GDPR in 2016.

Overall, many industry self-regulations thus failed to enhance compliance and even did the opposite. This contradicts one key argument in favor of industry self-regulations, which was that they could help ensure better implementation of data protection rules. In being closer to the regulatees (i.e., the very companies they represent or work with), they

were presented as being in a better position to ensure private accountability and were specifically included in the GDPR for that very reason. As one interviewee noted, the European Commission "promoted these types of compliance tools in the GDPR. Again, the keyword was accountability. People in specific sectors know best how to protect privacy." (Interview E23, done on March 14th, 2019). In practice, though, even in cases where they developed new compliance mechanisms like the IRSG did with its annual assurance review, they often did not apply them as they were supposed to and could be seen as a form of 'privacy-washing', an attempt to present a service or product as being more privacy-friendly than it actually is. According to the same interviewee, this is actually evident when looking at how they have been drafted over the years:

> Looking forward, I am however a bit skeptical. What I find is that many codes are written not to protect citizens, but they are mostly written with a defensive attitude towards themselves. It is for their own protection. [...] It is a common weakness that codes are not really made to protect citizens. (Interview E23, done on March 14th, 2019)

This represents a case of regulatory capture where many of these industry self-regulations were developed to benefit those they are supposed to regulate rather than serve the broad public interest. Far from fostering a thriving 'regulatory sandbox' where new data protection rules can be experimented with and explored, many indeed became tools to escape the adoption of stricter data protection rules by public authorities and limit the application of existing ones. The hybrid regulatory process, involving both public and private actors, comes to serve the interests of private companies wanting a more lightly regulated marketplace. The multiplication of regulations and rules that is normally seen as key for regulatory innovations to emerge appears to have played a crucial role in this outcome. By making the regulation of privacy more fragmented, it also made it more opaque and reduced the interest for private actors to spend resources to explore new rules. As one interviewee previously cited (see p. 145) noted, the multiplication of certification marks or seals created a lot of confusion for individuals. In practice, few, if any, would be able to distinguish them and know what each prescribes with regards to the collection of their personal data.

This type of "second-order information asymmetries" (Renckens 2020: 41) was further reinforced by the multiplication of data protection rules over the years. Previous studies have notably pointed out that the text complexity of most privacy policies is too high for most individuals. On average, the privacy policy of many popular companies

requires a college education level to understand (Litman-Navarro 2019). Similar results were in effect found for websites and applications that specifically target children (Calver and Miller 2018). In light of this, there has been a growing push to reduce the use of confusing legalese in privacy policies (Becher and Benoliel 2020). In its transparency requirement, the GDPR specifically tackles this issue, indicating that companies should use "clear and plain language" (art. 12) to describe their data practices. Following this, the length of time needed to read the 2019 version of Google's privacy policy was cut almost in half compared to its version one year before per one journalist from the New York Times (Litman-Navarro 2019).

Despite such attempts at bringing more transparency, the higher number of rules found in today's privacy regulations still tend to make them long and complicated documents to read. The 2019 version of Google's privacy policy is still four times longer (+\- 18 mins) to read than its earlier version of 2004 (+\- 4 mins). This illustrates that as the number of data protection rules grows, the length of public and private regulations necessarily also tends to become longer. A recent study of 194 privacy policies of American private companies in effect found that their overall length had significantly increased between 2014 and 2018 (Davis and Marotta-Wurgler 2019: 695). Although the language used in privacy policies may become simpler and easier to read, the time to read them thus remained the same or even increased. This means that according to previous estimates, individuals with the right reading ability would need on average more than 200 hours per year to read all privacy policies affecting them (McDonald and Cranor 2008: 560). This obviously results in almost none being actually read. A direct consequence of this is that it reduces the value of industry self-regulations' signalling effect. Private companies do not have a real incentive to experiment or go further than what is required of them in the law because they all appear as being equivalent to individuals viewing them.

This is notably made evident by the unfortunate fate of the Webtrust certification program of the American Institute of Certified Public Accountants (AICPA). The latter was an industry self-regulation jointly developed by the American and Canadian association of accountants and widely recognized in the early 2000s for its thoroughness. In one previous research, one representative from a telecom company that joined this certification program explained its choice by specifically emphasizing its comprehensiveness: "The WebTrust criteria were very complicated...The VP at that time said: this is the best one, let's go and get it! Make sure that we get the most impressive seal" (Boulianne and

Cho 2009: 236). This is similarly confirmed by this research, which found that it was the second most innovative private regulator, having enunciated for the first time six rules in the different versions of its industry self-regulation over the years. By 2004, it was also the American industry self-regulation with the highest number of data protection rules (i.e., 41). This is more than twice the average number of rules included in privacy regulations active in the transatlantic area at the same time and ten more than in the European Data Directive of 1995. As a matter of fact, it was the American industry self-regulation that had exploited the most 'European' rules (see 5.2 and 5.4 in chapter 5) by the mid-2000s with close to two-thirds of the rules found in the Data Directive.

Few American companies, however, ended up using the Webtrust certification and it closed down in the United States[7] in 2013 after all that had done so stopped using its services. In contrast, TrustArc became one of the most popular certifications in the United States, even gaining the support of major companies like Microsoft, despite its multiple regulatory failures mentioned above and rarely exploring new data protection rules. According to another representative of the telecom company that had been an early adopter of the Webtrust certification, the high costs associated with operating it and the lack of visibility gain from it were the key reasons behind this outcome (Boulianne and Cho 2009: 239). By exploring new rules and creating an increasingly comprehensive privacy regulation, the Webtrust certification indeed became more costly to implement for companies. Its difficulty to stand out among all other seals visible online and privacy policies disclosed on companies' websites simultaneously made it an unattractive option. Here the multiplication of regulations promoting different rules thus did not become a source for further regulatory innovations, but an impediment to it by making it more difficult for individuals to distinguish them.

To overcome this sub-optimal situation and promote the adoption of private regulations in the broad public interest, both the American federal government and European Commission have engaged with industry associations developing codes of conduct, certification programs, and other forms of self-regulations dealing with privacy. More than simply using the threat of regulation, they took positive steps to ensure that industry groups include a basic set of rules and indeed implement them on multiple occasions. This more specifically included offering funding, feedback, and even official approval in some cases. Interestingly, though, the level of engagement with the development of private regulations has highly differed in the two jurisdictions. The next section will highlight

[7] At the time of writing, the Webtrust certification remains offered to private companies in Canada.

this diverging trend and reflect on how it affected the process of creation of data protection rules by private actors and how different public involvement can produce different results.

6.5 Harnessing Private Regulation in the Shadow(s) of Hierarchy

As argued throughout this research, the American and European approaches to privacy regulation are closer to hybrid forms of regulation than either pure self-regulation or public regulation. On many occasions, representatives from both public agencies and the private sector interviewed for this research in both jurisdictions maintained that they preferred to talk of co-regulation instead of self-regulation (Interview E16, E24, E26, E29, E39, E40). One notably corrected the use of the term self-regulation and indicated that "[w]e don't call these self-regulations anymore. It's really more of a co-regulation or multistakeholder approach" (Interview E37, done on May 14th, 2019). At the same time, they did tend to diverge on the role that they respectively give them as well as how they interacted with them in the rule-making process.

In the United States, the FTC is in many ways the *de facto* privacy regulator. Over the years, this primarily meant that it acted as an enforcer or "backstop" for what would otherwise merely be voluntary obligations that private actors set for themselves. By making use of its statute prohibiting unfair or deceptive acts, it polices the extent to which industry associations and private companies respect what they advertise to their users in their privacy statements. It is notably on this very basis that in 2014 it sued the company TrustArc (then known as TRUSTe) for repeatedly failing to adequately enforce its self-regulatory certification program (Federal Trade Commission 2014). It used the same legal authority to impose a $5 billion fine on Facebook for its role in the Cambridge Analytica scandal (Federal Trade Commission 2019).

While very active at the implementation stage, the FTC has often played a more marginal role in the process of devising rules by industry groups. As noted in chapter 3 (see especially section 3.5), it did sometimes play a role of agenda-setting and even reviewing the content of private regulations, but this was more the exception than the norm. Putting aside the specific case of the safe harbor program under the Children's Online Privacy Protection Act (COPPA) that specifically requires the FTC to evaluate

and approve self-regulations put forward by the industry, one notable exception was in the case of the advertising industry that it pushed twice to self-regulate itself by organizing workshops and events both in 1999 and 2007 (Dixon 2007; Gellman and Dixon 2016). The latter led to the creation of the privacy principles of the NAI in 2000 and both the revision of these principles and the creation of the DAA in 2008. Apart from these two important cases, the FTC did not regularly engage with industry groups to modify the content of their self-regulations. As one interviewee noted, FTC's employees "would not provide a lot of remarks to these programs. When a company that wants to build a trustmark comes to them, they would probably point them to some of the case studies that they have done on these topics, but they would not go in a great level of detail" (Interview E38, done on May 14th, 2019).

In contrast, the European Commission has often been more active early on in the process of rule creation by private actors. In addition to having set a clear legal baseline with the adoption of its Directive and now Regulation, it regularly supported the work of industry groups by offering funding (either directly or indirectly by offering organizational support), detailed feedback, and sometimes even officially approving them. Table 6.2 summarizes the different ways the European Commission has supported self-regulatory programs adopted in Europe and reviewed in this research. This information was retrieved from the websites detailing each of these private regulatory initiatives as well as various studies on the state of self-regulation in Europe over time (European Commission 2001*a*, 2012*b*; European Parliament 2012). In total, it is close to half (42%) of them that received official support from the European Commission in one or multiple forms. Generally speaking, industry groups that saw their self-regulation formally approved also went through a revision process where they received feedback from European officials. Funding and feedback can, however, occur separately and without necessarily leading to a formal approbation by public authorities. It should finally be noted that some of these regulations that were originally developed in one Member state also sometimes received public support from national authorities. This is notably the case of the IMRG and TrustedShops' codes of practice. Many of those that did not receive any form of support from any European institutions finally deal with privacy as one issue posed by the rise of electronic commerce and tend to be less detailed.

Through these different interactions, European regulators have significantly shaped the content of industry self-regulations. Rather than leaving their development to private actors, their early and continuing involvement has often meant that they worked

Table 6.2: European Support of Industry Self-Regulations since 1995

Year	Industry Self-Regulations	Funding	Feedback	Approval
1997	IMRG's Code of Practice			
1999	Which's Webtrader Code of Practice	•	•	•
2000	Eurocommerce's EuroLabel	•		
2001	UNICE - BEUC e-Confidence Project*	•	•	
2001	Clicksure Quality Standard			
2001	TrustedShops' Quality Criteria			
2001	TUV SUD Safe Shopping Standard			
2002	EMOTA's Convention			
2003	SafeBuy's Code of Practice			
2003	FEDMA's Code of practice		•	•
2005	ERA Europe Marketing Guidelines for Electronic Retailers			
2011	EASA's Recommendations on Online Behavioural Advertising			
2011	Europrise's Privacy Seal	•	•	
2011	IAB Europe's Online Behavioural Advertising Framework			
2012	EDAA's Self-Certification Criteria for Online Behavioural Advertising		•	
2015	E-Commerce Europe Code of Conduct			
2016	Code of Conduct for Cloud Service Providers**	•	•	
2016	Code of Conduct for mHealth Applications**	•	•	
2017	E-Commerce Foundation SafeShop Trustmark			

* This self-regulatory program was never formally adopted.
** These codes of conduct were submitted to the Article 29 Working Party, but were never formally approved and adopted.

to ensure that regulations put forward by private actors closely followed their own regulatory standards. As one interviewee from the European side explicitly indicated: "We try to drive them to include what we think should be in [a] code" (Interview E16, done on February 20th, 2019). This is particularly evident when looking at the case of FEDMA's code conduct, which was the only self-regulation formally approved under the Data Di-

rective[8]. After four years of exchanges with the Article 29 working party, its code of conduct for the advertising industry closely approximates almost all the rules found in the European Directive. Both actually have an index of thematic similarity of 80%[9], one of the highest found in this research. The difference mainly comes from the inclusion by FEDMA of additional rules that it copied from its American counterparts, notably on the protection of children's privacy.

The codes of conduct for cloud providers and mobile health applications submitted in 2016 to the article 29 working party were similarly extremely close to the then soon to be adopted GDPR. They both had a thematic similarity higher than 0.75, which is again extremely high and reflects their close interactions with European regulators. In both cases, industry groups even received funding from the European Commission to pay for legal counsel to help them devise their self-regulation. In the end, they were not approved primarily because their enforcement mechanisms were judged insufficient (Article 29 Working Party 2015). As the GDPR was close to enter in force and to change the approval process, these projects were then put on hold. While representing a partial failure for the industry to self-regulate itself, it does show that the European Commission often strictly controls the evolution of industry self-regulations and attempts to limit the risks of seeing them become tools of regulatory capture.

This can notably also be seen when looking at the case of the European Interactive Digital Advertising Alliance (EDAA). As opposed to the previous codes, this self-regulation was never officially submitted to the article 29 working party. Yet, it extensively engaged with the European Commission as noted by one interviewee for this research who was closely involved in the process leading to the creation of this self-regulatory programme:

> We had roundtables organized with the European Commission, 8 to be precise. [...] I don't know how familiar you are with this, but having 2 is already something big. [...] When the commission agrees to do something like this, it is a huge thing. [...] At one point, we were meeting every quarter. They wanted to follow very closely our progress. Up to a point, where we didn't have the time to digest what we were reading anymore. (Interview E21, done on March 8th, 2019)

[8] In table 6.2, the Which's Webtrader Code of Practice appears as having also been officially approved. However, this was not through the process envisioned by the Data Directive. This was rather by the directorate-general for enterprise and industry (DG Enterprise).

[9] For a reminder of how this index is calculated and its exact meaning, see section 4.2.

The close involvement of European regulators played a crucial role in the development of this private initiative. Like the Digital Advertising Alliance (DAA) in the United States, the EDAA primarily operates an 'AdChoices Icon' aiming to educate individuals about how data-driven advertising functions and help them make choices on how their personal data is used. The very specific nature of this industry self-regulation has meant that its content requirement is not as detailed as many others previously discussed. Rather than setting how a comprehensive set of data protection rules for advertising companies, it largely limits itself to explain how to apply a specific set of rules in combination with its 'AdChoices Icon'. As such, it does not include many rules traditionally found in the European regulatory framework and is almost identical in what it requires to the self-regulatory programme of the DAA in the United States. One key difference that precisely came from its interaction with the European Commission is its compliance mechanisms. As the same interviewee indicated:

> They [the representatives of the European Commission] always told us the same thing. Listen, you are not doing the right thing. Unless you can prove that you have grown up, we'll have to regulate. [...] If you don't police yourself, we will police you. (Interview E21, done on March 8th, 2019)

In practice, the European Commission wanted to be sure that any self-regulation would have real teeth and would not become a simple expression of goodwill as it sometimes became the case. In the end, the founding members behind the EDAA listened to the European Commission and adopted a stricter procedure to check compliance early on when a company wishes to join its self-regulatory programme. As of now, any company that wants to self-certify with the EDAA has to go through an audit before being allowed to showcase its trust seal. This significantly reverses how the DAA checks the compliance of its members in the United States, which only occurs after companies have officially joined it. Once admitted, American companies following its rules may be randomly selected for a compliance check, but it is not guaranteed. By directly getting involved in the creation of industry self-regulations, the European Commission thus again tried to limit the risks of seeing it become a tool to avoid public regulations. Its different actions have all contributed to ensuring that self-regulatory programmes created by the industry closely align with its own rules and helped them being enforced throughout its single market.

One consequence of this coordinated approach adopted by the European Commission has been to limit the creation of new data protection rules by private associations

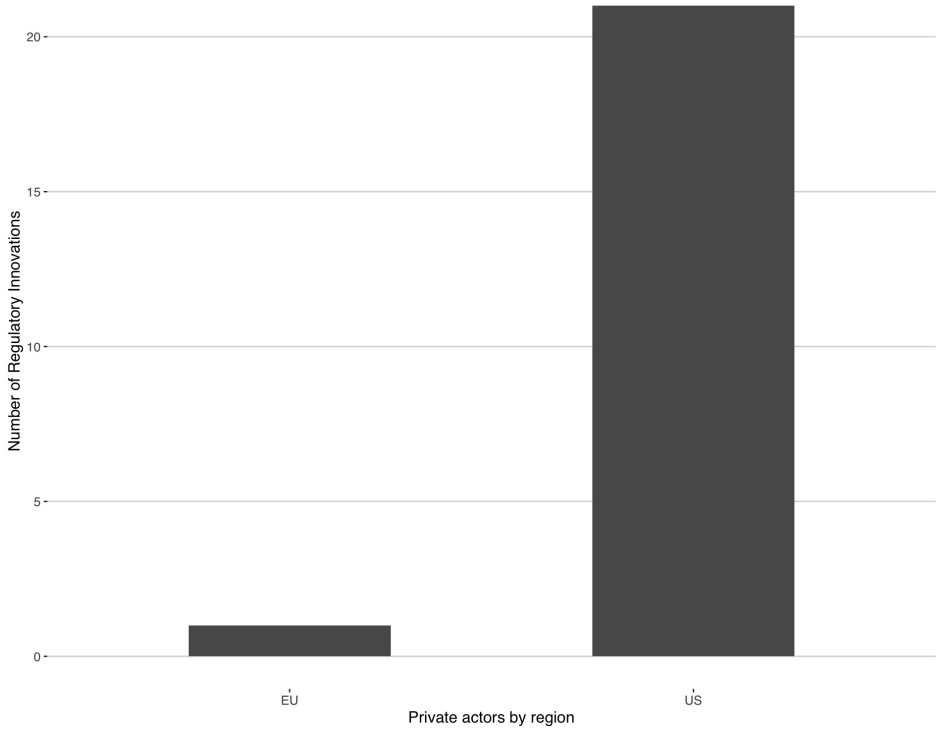

Figure 6.3: Sum of new data protection rules created by private actors in the EU and the U.S. since 1995

in Europe. As figure 6.3 shows, almost all rules (95%) that were found to have been first enunciated by private actors in the last twenty years were also found in a self-regulation created in the United States. In other words, industry groups and companies operating self-regulations in Europe have largely aimed to implement public rules rather than create new ones. While industry self-regulations adopted in Europe can still attempt to innovate when translating data protection rules in their respective "sector lingo" (Interview E22, done on March 11th, 2019), the close involvement of European regulators generally push them to stay as close as possible to the requirements found in the law. This is especially true for those working to be officially approved by European authorities or national data protection authorities. As they are specifically looking to see how public rules have been incorporated, private actors often aim to remain as close to them as possible. As one interviewee straightforwardly argued, it "is just such a big job to decide how to interpret their existing obligations and they do not want to make their jobs harder than it already is." (Interview E26, March 22nd, 2019). What they then often end up doing is providing examples of how specific data protection rules set forth by public authorities should be

applied rather than so much adapt them. One interviewee working for an organization that had specifically worked with European public authorities to develop their code of conduct specifically mentioned that public authorities had praised their inclusion of examples: "What we were told when we were working on the last version of our code was that the examples were very good" (Interview E17, done on February 21st, 2019). Similarly, an interviewee from the public side discussing what industry self-regulation should be doing was not to go "beyond compliance with the law, but [provide] more details, more example of practices" of how to implement it (Interview E20, done on March 3rd 2019). For one interviewee representing an industry group, this was actually seen quite negatively and as leaving almost no room to change anything as it would be seen as an attempt to circumvent their obligations:

> I was once told by the European Commission that if you ask questions [on how to implement their obligations], it meant that you are trying to go around the law and this is problematic. [...] If you want a dialogue, you area already on the edge. (Interview E25, done on March 15th, 2019)

Far from being a defect, though, this reflects the overall view of European public authorities that these private tools can best contribute to the regulation of privacy by making their rules more operational as one interviewee for this research argued:

> Private codes of conduct are there to help compliance. [...] A code translates the rules of public laws for a specific sector. At the same time, they must got a little bit further than the law. [...] Going further can mean different things and it can take different forms. It can be the application of an higher standard, but it doesn't have to be. At a minimum, it must point towards good practices for a specific economic sector or industry. It must clarify for the members of an association how to implement the law by indicating clear steps to do so and offering a more operational approach. (Interview E12, done on February 11th, 2019; translated from French)

This means that there seems to be a trade-off to the involvement of public authorities in the process behind the creation of self-regulations. The more hands-on governments are, the less innovative private actors appear to be. This is not necessarily a negative outcome, though, and depends on how we define the role that private actors should play. If it is expected as it sometimes argued that companies working in a specific area know best how to regulate themselves, this is certainly unfortunate that private actors are becoming less adaptive and flexible. As previously explained, this specific argument has often been more assumed than empirically verified. Indeed, private actors have often not been as prone to explore new data protection rules in that process as

they often seem to maintain. Time and again, they also failed to implement the rules they had set for themselves or even entirely stopped their activity when public scrutiny disappeared. This was notably the case of the IRSG, which is the private association that was found to be the most innovative and to have created the highest number of new rules in the last twenty years. As one interviewee pointed out, this can even raise competition issues as private actors can attempt to reinforce their market position by establishing rules to their own benefit:

> What we see is authors of a code that sometimes try to regulate themselves. This can be problematic and even raise competition issues. The main players will try to block access to the market to smaller players by institutionalizing their practice. (Interview E16, done on February 20th, 2019)

In sum, codes and other softer forms of regulations created by private actors work best when they complement the work of public agencies rather than try to replace them. As the same interviewee maintained, it is precisely when the industry attempts to do the latter that it becomes problematic:

> [Data Protection Authorities] are enthusiast about codes because they know how difficult it is for the market to implement data protection rules. It is good for the operationalization of data protection principles. [...] During the GDPR, the industry requested that European regulators do not over-regulate. Their argument was that they knew how to regulate, much better than [data protection authorities] and legislators do, and it is partly true. In my case, I am not an energy specialist and I would have never thought that my work would lead me to study the energetic sector, but it did. I did it, but I can't do 70 sectors. [...] Co-regulation is private regulation, which uses national or European laws as background for their codes. We need co-regulation, but it sometimes end up as self-regulation.

This is clearly the approach that has been preferred in Europe where the European Commission and other public agencies, like the Article 29 working party, specifically worked to impede the adoption of industry rules that would not sufficiently engage with national and European laws. In the United States, they tend to promote something closer to a pure form of industry self-regulation, even though relying on the backstop enforcement of the FTC. Yet even there, public authorities sometimes ended up having to take action if they wanted private actors to do something as previously mentioned.

6.6 Conclusion

Since the European Data Directive was adopted in 1995, the regulation of privacy in the transatlantic area has gone through significant changes. In addition to the European and American model of privacy regulation becoming closer to each other, I highlighted throughout this chapter that each grew in terms of their complexity. The exploration of new data protection rules in effect ensured that each became more comprehensive and covered more data practices. Far from only being driven by public authorities, private associations and certification companies developing various forms of industry self-regulations also contributed to this trend. New rules on the use of cookies and how personal should be collected were notably first enunciated by American associations. At the same time, the number of new rules put forward by these private actors has remained limited and was particularly low in the last ten years. Rather than becoming a source of regulatory innovations, the multiplication of regulations and rules early on appeared to have the opposite effect. By creating more fragmentation and making it hard for individuals to know which companies follow which rules, it reduced the interest of private actors to go much beyond what they are already required. While the rise in complexity can often be seen positively by complexity scholars, this emphasizes one potentially negative outcome and points out the importance of always considering how interactions between the structure of a given system differently affect actors depending on their preexisting interests. Indeed, it shows that although a more fragmented system can offer opportunities to innovate for actors looking to do so, it can also diminish the value of innovating for others and support a form of regulatory capture. The latter here does not result from a public regulation that comes to represent specific vested interests. It rather represents a case where stringent public regulations are replaced with lenient or unenforced industry self-regulations.

At the same time, this should not be seen as an inevitable outcome. Due to their hierarchical position and their capacity to proactively engage with the regulatory work of private actors, public authorities can ensure that industry self-regulations are adopted in the public interest. The European Commission was indeed seen as successfully having pushed them to exploit its data protection rules by adopting a more hands-on or coordinated approach towards industry self-regulations. While limiting the role of European industry self-regulations in exploring new data protection rules, it also limited the risks of them being used to avoid compliance as it sometimes became the case in the United States. This finding concurs with previous studies (Cashore and Stone 2014; Gulbrand-

sen 2014; Renckens 2020) showing that public interventions in the development of private regulatory initiatives can help achieve better regulatory outcomes and emphasizes that exploration of new rules and the concomitant flexibility that it can bring are not the only benefit nor necessarily the most important one that industry self-regulations can provide to the regulation of an issue-area. Making more operational public rules might actually be a better contribution.

On a more analytical note, I also showed in this chapter the importance of going further than merely looking at the emergence of private authority (Hall and Biersteker 2002) and of adopting a multilevel perspective. In effect, the multiplication of industry self-regulations could have given a false sense of a thriving environment providing ever more privacy guarantees to individuals when actually a comparison of the content of these regulations would show that few bring anything new and many largely repeat what you would find in public regulations. This moreover demonstrates that instead of being a sign of a 'retreat of the state' (Strange 1996), the rise of private authority can enhance the influence of public authorities either by potentially raising compliance as discussed in this chapter or promoting greater regulatory convergence as discussed in the previous one. It finally shows the difficulty to distinguish between 'entrepreneurial' and 'delegated' form of private authority as Green (2013*b*) recently tried to do. Even though industry associations can show entrepreneurial signs in deciding by themselves to develop a private form of regulation, they might exploit public rules more than explore new ones and, in practice, be closer to a delegated form of authority. This is without mentioning that the line becomes even more blurry as public actors become more and more active in their drafting process.

Together with chapter 5, the contributions of this chapter help better appraise the dynamic nature of the evolution of the transatlantic regulation of privacy as a complex system. It again shows the crucial role that private actors have played in it and how they affected the system's capacity to adapt over time. Throughout this research, I significantly talk of complex systems or complex governance systems. Another expression often found in the literature on complexity theory is, however, the one of "complex *adaptive* systems" (Harrison 2006; Holland 1998, 2006; Miller and Page 2007; emphasis added). I consciously decided to forgo the qualitative adaptive as I do not consider adaptation to be one of the necessary characteristics of complex systems but one of their potential outcome. In other words, I see it as an empirical rather than a theoretical question (Morçöl 2012: 42); see also Axelrod and Cohen 2000). As detailed throughout

this chapter, a complex environment can in fact limit the adaptation capacity of a system depending on the logic of the actors in it.

Conclusion

We have never hidden that we want to see more convergence when it comes to the framework for data protection [in the U.S.]. [...] We would like to see on the American side a federal law that would be equivalent or similar to the General Data Protection Regulation.

Věra Jourová, EU Vice-President in charge of values and transparency, 2020

On July 16, 2020, the European Court of Justice (ECJ) struck down the Privacy Shield Agreement in a decision reminiscent of the one it had reached four years before in invalidating the Safe Harbor Agreement. According to the ECJ, the Privacy Shield did not offer sufficient guarantees that the personal data of Europeans would be protected from being accessed by American authorities, notably through one of its surveillance programs revealed by Edward Snowden. Discussing this outcome, the European Commissioner for Justice from 2014 to 2019 and now EU Vice-President in charge of values and transparency, Věra Jourová, pleaded for more convergence between the two transatlantic partners and for the United States to adopt a comprehensive federal privacy law as cited in epigraph. According to her, the absence of such a law was impeding any real integration of their respective data realms.

Both the Safe Harbor and the Privacy Shield Agreements were always second-best options for two jurisdictions that diverged over how the use of personal data should

be regulated. It is because the United States did not have sufficient legal guarantees in place and thereby could not get an adequacy decision that these agreements had to be negotiated in the first place. With this in mind, I contended in chapter 3 that both jurisdictions are not irreconcilable and have more in common than it often seems. In addition to starting from a similar liberal or 'privacy as control' paradigm, they both actually involve private actors. Even in Europe, where public authorities are expected to set a basic framework of how private companies can collect and use personal data, industry associations have been repeatedly encouraged to develop codes of conduct and certification programs. Following the demise of the Privacy Shield, these are one of the remaining tools for data transfer in the United States allowed by the General Data Protection Regulation (GDPR). Companies that will abide by a certified code of conduct or certifications will indeed be permitted to transfer personal data between the United States and the European Union.

Looking at these private forms of regulation being created in the European Union and the United States, I argued in chapter 4 that before even becoming tools for data transfers, they created new connections between these two regulatory systems that contributed to forming a complex governance system. As opposed to the traditional 'system clash' view embedded in the citation of Věra Jourová above, this led me to maintain that the content of the regulations adopted in both jurisdictions was constantly being shaped by decisions taken in the other. I more specifically maintained that this occurred through two joint processes: exploitation and exploration. Exploitation was first defined as the tendency to use preexisting resources, or rules in the present case, to achieve efficiency gains. Exploration was meanwhile presented as the tendency to create new rules when preexisting resources proved insufficient.

Using a combination of network and content analyses, I then demonstrated in chapter 5 how the exploitation of preexisting rules by industry associations supported a form of regulatory convergence. Even though the European Union and the United States still do not share the same regulatory approach, the set of data protection rules that they actually promote grew increasingly similar over the years. Codes of conduct, certification programs, and other forms of private regulations here notably support the exploitation of public rules and become an institutional avenue through which public authorities' influence can be expressed. Way before California adopted the first American comprehensive privacy law in 2018, many provisions originally found in the European Data Directive had indeed made their way to the United States through interactions

between industry associations and firms developing these private regulations. Similarly, rules first found in American sectoral laws at both the federal and state levels had been integrated by private actors in Europe before they were taken up in the GDPR.

I finally showed in chapter 6 that convergence is only one part of the story. More than simply sharing an increasingly large set of data protection rules, public and private actors behind regulations dealing with privacy issues also tended to explore new data protection rules by combining preexisting ones. In itself, this is one of the factors that limited their regulatory convergence as new rules were obviously not instantly shared by all. Far from a defect, though, this ensured that the regulation of privacy remained dynamic and kept up with changes in data practices over the years. I then pointed out that private actors played a role in that process and thereby contributed to providing a more flexible regulatory environment. At the same time, their contribution was not as substantial as it was sometimes argued. Industry associations and firms developing codes of conduct or certification programs in effect tended to stay close to public requirements and only go further at times of close scrutiny by public authorities. In the United States, their regulatory initiatives even appeared to be about avoiding regulation more than really making it more robust. I maintained that this was, in many ways, a by-product of the rising of complexity that created information asymmetries and limited the public interest in these private forms of regulation. Greater involvement of public authorities, as regularly seen in the European Union, could help limit this sub-optimal outcome, but it did seem to reduce the interest of private actors to explore and experiment with new rules.

7.1 Original Contributions

Throughout this research, I show that the integration of national economies does not merely, nor even primarily, lead to a clash of systems where one jurisdiction merely attempts to make its regulatory standard adopted globally. As they become increasingly interdependent, interactions between their regulators also become more prevalent and progressively upend the process of rule formation. In that process, public authorities are importantly joined and complemented by private actors that act as regulators in their own right. The interaction between the United States and the European Union over the regulation of privacy depicts this perfectly. Since the adoption of the European Data Directive in 1995, neither straightforwardly exported its regulatory preference to

the other. Yet, their exchanges, notably through private actors, continuously shaped the content of the rules adopted in each jurisdiction, and it will most likely continue to be the case as their respective models continue to evolve in the years to come. While making this broad argument, I contribute to the literature on data privacy, global regulation, and private authority.

First, I provide one of the most in-depth analyses of how the regulation of privacy and, more precisely, data protection rules have evolved since the adoption of the European Data Directive in 1995. The multilevel approach that I use to look at regulations as collections of principles and rules instead of coherent policy documents specifically allows me to go further than the so-called 'American' and 'European' privacy models up-to-now distinguished in the literature (Long and Quek 2002; Newman 2008; Solove and Schwartz 2011; Schwartz and Peifer 2017). I actually show that despite agreeing on some broad principles, they diverged over what should be their practical requirements. If this leads me to point out that the European Commission indeed continuously aimed to be more comprehensive in the content of the rules that it includes, I also highlight that the United States is not simply lagging behind the European Union. As a matter of fact, it developed rules that the European Union ended up integrating later on. This importantly provides a more nuanced picture than the story of European global leadership or influence currently dominating privacy debates (Bradford 2020; Greenleaf 2018; Schwartz 2019). My fine-grained analysis of the content of privacy regulations in the United States and the European moreover emphasizes the existence of both change and continuity in their regulatory frameworks. While previous studies tended to focus on the continuity in the regulatory approach preferred by the United States and the European Union (i.e., their continuous reliance on different regulatory approaches), I point out that important changes still occurred over the years as new rules were created and adopted. At the same time, I make clear that there is an important lineage in the content of regulations over time.

Second, I offer a renewed understanding of how globalization and economic interdependence are transforming national regulatory processes. I specifically move past traditional distributive arguments that see states as either cooperating or fighting over the share of the economic gains of globalization through regulation (Krasner 1991; Bach and Newman 2007; Drezner 2007) and show that growing interactions between a diverse set of actors fundamentally affect the process of rule formation itself. Rather than being purely driven by domestic actors, the decision to adopt or create rules is informed

by what others have done in other jurisdictions. As opposed to the traditional view of globalization as an exogenous shock that puts pressure on governments, it presents it as a source of regulatory change in itself. In that regard, it complements the recent literature charting a "new interdependence approach" (Farrell and Newman 2014, 2016, 2019*a*). While the latter emphasized that transnational connections were offering new pathways for a variety of actors to assert their influence globally, I present how it shapes the evolution of the "rules of the game" that define the behaviour of these very actors in the first place.

This also leads me to complement the literature on policy diffusion by outlining the interactive and incremental nature of regulatory change. Once again, my multilevel perspective allows me to demonstrate that even though the United States and the European Union stuck with their original 'comprehensive' or 'limited' policies, they both grew more alike over the years. This finding echoes those in the literature on policy convergence that had previously pointed out the actual similarities in the content of privacy policies in both jurisdictions over the years (Bennett 1992, 2010). Yet, I maintain that this is not merely the result of a tendency driven by the emergence of a common understanding of the issues raised by new technologies, but exchanges between public and private actors that made them approach their object of regulation in a similar fashion. I also go further by illustrating how these interactions do not only promote greater convergence but also become a source of innovation as they become the basic components of new data protection rules.

Third, my findings illustrate the complex relationship that exists between public institutions and private authority. The point that I here try to convey is not that states are in 'retreat' (Strange 1996). As repeatedly discussed, it has never been a story of either one or the other. They actively build on each other. Even in the United States, which is supposedly more inclined towards the use of market-based mechanisms to regulate the digital economy, industry self-regulations were never the whole story. The Federal Trade Commission and other regulatory agencies, like the Department of Commerce, played a crucial role in enforcing the rules that private companies set out for themselves. While not as commonplace as in Europe, these same agencies also openly interacted with industry associations to shape the content of data protection rules in public workshops or through direct exchanges. Meanwhile, in the European Union, public laws were early on supplemented by self-regulatory tools. Going back to the early days of the Data Directive, these were notably seen as potentially contributing to harmonizing the European

regulatory framework. Since the adoption of the GDPR, they are now also considered to be potential tools to allow for international data flows to take place and ensure greater accountability. The extent to which public and private actors interacted with each other even blurs the boundaries between the 'delegated' and 'entrepreneurial' form of private authority described by Green (2013*b*). In practice, it often happens that public actors enroll or give regulatory tasks to industry self-regulations that originally 'entrepreneurially' emerged. This is notably what the United States and the European Union did when promoting the use of private mechanisms to solve their divergence of regulatory approaches, and what the European Union did when attributing new regulatory tasks to private forms of regulation in the GDPR. What can also sometimes appear as an entrepreneurial form of authority can have in fact been actively influenced by public authorities through the receipt of public feedback or funding, as especially seen in the case of the European Union.

If it is not always clear if industry self-regulations draw their authority from public institutions or themselves, they clearly tend to be layered upon public rules (Bartley 2011). The legal authority of governments means that their principles and rules will be the (mandatory) starting point for private actors when devising their own sets of rules. The fact remains that if these tools can sometimes be aimed at helping companies differentiate themselves in the marketplace, they are also used to help them achieve greater legal compliance and navigate complex legal environments. Codes of conduct and certification services thus aim to include rules that will help companies say that they respect their requirements in the various jurisdictions where they operate. Such integration of public rules in industry self-regulations should matter for governments. They can first help extend their own legal authority by promoting their rules outside of their jurisdictions. As private actors exploited the rules of their counterparts, those in Europe started to integrate rules originally devised in the United States and vice versa. By combining these same rules and their knowledge of how personal data is being collected and used, they can moreover provide some flexibility to public rules. At the same time, my analysis cautions against ideas of "simply 'let 1,000 flowers bloom' and see which rules appear robust" (Green 2013*b*: 174). The multiplication of private forms of regulation can actually end up undermining their supposed flexibility while at the same time giving a false impression that they make the regulation of privacy more effective.

Looking more specifically at the European Union, I then indicate that public contributions to the development of private regulatory initiatives contributed to solving this

sub-optimal outcome. I show that by providing funding, feedback, and even officially approving or certifying industry self-regulations, the European Commission limited the number of apparent cases of lax or unenforced rules by the industry. Its actions moreover supported the creation of links between American and European associations, which led to some of its data protection rules to be exploited by private actors in the United States. While reinforcing them and more closely incorporating them in a public regulatory framework, my evidence suggests that these European actions further limited the interest of industry associations to explore new rules. In effect, almost no European industry associations created new rules, and most attempted to closely approximate European public rules. This apparent trade-off is not necessarily negative. While innovation is often highly valued in our societies, the actual enforcement and implementation of existing rules is in itself a crucial contribution.

7.2 Complexity and International Political Economy

All these different contributions are significantly tied together by the complex system approach that I developed in dialogue with my empirical findings. The recognition that we live in a complex world is hardly new (Keohane and Nye 1974, 1977). In this work, I, however, join recent scholarship promoting the use of complexity as an analytical lens rather than a mere metaphor (Bousquet and Curtis 2011; Kavalski 2007, 2012; Oatley 2019; Orsini et al. 2019). The term complexity was indeed not meant to describe a complicated phenomenon, but a system made of multiple parts displaying emergent properties. To put it differently, viewing the transatlantic regulation as a complex governance system was not used to point out that it was becoming more difficult to manage, but that it created dynamics that could not be fully understood without considering the system as a whole. These were in this case the exploitation and exploration processes analyzed throughout chapter 4 to 6.

These are not necessarily the sole emergent properties that complex systems can display. Nor will they present themselves similarly across all complex systems. In fact, this research has shown that the exploration of new rules was not necessarily as significant as it could have been thought. The multiplication of regulators and regulations in effect did not significantly support the growth of data protection rules. The regulation of privacy was in turn not found to be as adaptive as other complex systems were sometimes argued to be (Mitchell 2009). This importantly points out the highly contingent nature

of complex systems. Depending on the actors (or units) involved as well as previous interactions, two different systems will not evolve in the same way. In this case, the specific logic of action of private actors was seen as limiting their interest in creating new rules when the system was actually becoming increasingly complex.

A complex system approach thus does not necessarily offer a straightforward indication of what will happen in the future. As noted in chapter 2, it forces us to recognize that context and time matter (Cilliers 2001; Oatley 2019). For the broader fields of international relations and international political economy, it presents a call to be more sensitive to "uncertainty and unexpected consequences" (Kavalski 2007). The diffusion of data protection rules across the United States and the European Union was never entirely planned by the American government or the European Commission. The creation of new rules like the 'right to be forgotten' was similarly not foreseen by regulators creating the rules that would be later on used to constitute it. These are, however, part of broad trends that both practitioners and researchers can recognize and attempt to act upon.

Looking at the governance of socioecological systems, Oran Young (2017) chiefly argues that governing them as complex systems should specifically involve using new "steering mechanisms". Pointing out that institutional arrangements are also complex systems that can change in unexpected ways as socioecological systems themselves change, he maintains that one overarching goal of policymakers should be to devise institutions that minimize the risks of a potential "problem of fit" over time (Young 2017: 113). To ensure this, he favours the use of "goal setting strategies" and a "principled form of governance". In both cases, the point is to leave more leeway in how broad goals or principles are achieved as circumstances change. This somewhat echoes previous ideas expressed in the literature on experimentalist governance interested in building institutional environments prone to learning and capable to improve over time (De Búrca, Keohane and Sabel 2014; Overdevest and Zeitlin 2014; Sabel and Zeitlin 2010).

While not disagreeing with this view, the present work has pointed out that it should not be expected that implementation will straightforwardly follow from the expression of broad principles. Industry associations and certification companies devising self-regulations again did not always appear so much interested in making the regulation of privacy more robust or adaptive. Close attention should thus also be paid to building capacities to monitor and spur various actors to continuously aim to respect the goals or principles set out early on, something again already hinted at in the literature on

experimentalist governance. The involvement of European authorities in the development of industry self-regulations was one example of such actions. Another not discussed in the context of this research is the newly given possibility in the GDPR (art. 80) for non-governmental organizations (NGOs) to submit complaints in place of data subjects. One recurring problem with the liberal or "privacy as control" paradigm espoused by the United States and the European Union and discussed in chapter 3 is the continuous difficulty for data subjects to monitor how their personal data is being collected and used. NGOs working in the privacy space will now be able to act as kinds of watchdogs and put pressure on private companies to improve their practices by filing lawsuits against them. This mechanism could interestingly contribute to provide additional information to regulators and help spur regulatory innovations. As noted in chapter 6, the right to be forgotten was indeed originally enunciated following a lawsuit filed in Spain against Google.

7.3 Practical Implications

My findings moreover have important practical implications for the regulation of privacy and global regulatory debates. They notably show the importance for public authorities to engage with private actors. Here, I do not want to plead in favor of a specific regulatory approach. The different level of involvement of American and European authorities in the development of private mechanisms used to regulate the use of personal data is obviously no stranger to their preference for a more comprehensive or limited form of regulation. At the same time, I argued that these very differences become more blurry when looking at how privacy is protected in practice. One of my aim in this work was specifically to move past these broad dichotomies and call attention to how interactions between a diverse set of actors in the United States and the European Union was shaping the regulation of privacy. No matter their preference for having a public law setting out the requirements for the private use of personal data or primarily leaving companies to self-regulate themselves, they can indeed both benefit from a greater engagement in the development of private rules as this can notably end up promoting a more coherent and enforceable regulatory framework. This is in line with recent arguments in favor of rejecting an adversarial view of regulation or one solely based on the formal enforcement power of the state (McGeveran 2016). By adopting a more supportive and coordinating role, governments can harness the influence of private authority in the public interest and

limit the risks of seeing it becoming a tool of 'privacy washing' or for merely avoiding public regulation.

More broadly, it emphasizes the role of "intermediaries" in achieving regulatory outcomes in a complex and global economy. The concept of intermediary very simply relates to actors or institutions that operate between public regulators and their final subject of regulation. As previous scholars have hinted at in the regulation of finance and information technologies, these are actually quite common (Benkler 2011; Goldsmith and Wu 2006; Farrell and Newman 2019*b*; Judge 2015; Tusikov 2016). Internet service providers, online platforms, online payment companies, and clearing houses are just a few examples. While all can sometimes be viewed as regulatees in their own right, they also all have close interactions with other regulatees. These can be individuals (e.g., Internet users, investors, etc.) or institutional actors (e.g., Internet companies, banks, etc.). In the present work, industry associations and certification companies are yet another form of intermediary that operates between public regulators and private companies using personal data. Their role is again recognized both in the United States and in the European Union where adherence to their rules can offer several benefits to private companies. In the United States, companies following an approved code of conduct will be assumed to respect the Children's Online Privacy Protection Act (COPPA). Under the GDPR, companies abiding by approved codes of conduct or certification programs could also more easily transfer personal data.

Due to their close connection with the subjects of regulation, these intermediaries can offer many advantages to public authorities. They notably tend to know better how rules are or not applied as well as what are the potential practical issues of implementing specific sets of rules. In the present case, industry self-regulations are indeed sold as tools that can help translate public rules in a specific business context or economic sector (i.e., advertising, research, e-commerce, etc.). The transnational nature or connections of intermediaries with regulatees based in multiple jurisdictions can additionally help public enforcement efforts across jurisdictional boundaries. Once again, the evidence reviewed throughout this work does suggest that industry self-regulations dealing with privacy issues in the transatlantic area contribute by pushing each jurisdiction to include the same set of data protection rules through their interactions. This network argument should, in turn, push public authorities to closely consider the position of these different intermediaries in the regulatory system when engaging with them. By targeting those that are particularly central or that have particular ties could help them promote their

own regulatory framework. They can moreover actively contribute to the evolution of the network structure by bringing potentially distant actors to work together. Examples of such coordination were notably seen to have helped the European Union promote a common set of data protection rules in chapter 5.

7.4 Prospects for Future Research

As the citation in epigraph highlights, the evolution of the regulation of privacy in the transatlantic area is very much an ongoing process. As opposed to what the European Commission would perhaps hope for, this will not necessarily only be towards greater convergence around European data protection rules. As public and private actors continue to interact with each other, new data protection rules are bound to emerge and change how the personal data from Europeans and Americans are protected. While keeping track of how these broad trends will play out, future work could build and expand on the present findings in three ways.

In this analysis, I consciously focus on two types of actors: public authorities and industry associations (or certification companies) that create rules for other private companies. While emphasizing how interactions between these two types of actors shaped the regulation of privacy, a next step could be to add private companies to this picture as I actually pointed out on a number of occasions. In the end, these are the ones that apply and interpret the data protection rules described in this research. Just as industry associations can contribute to refining the meaning of principles and rules devised by public authorities, private companies can similarly do so through the final terms of use or community rules that they adopt. What this addition of governance layer actually means for the regulation of privacy and how it interacts with the other two are important avenues for future research. The recent literature looking at 'privacy on the ground' (Bamberger and Mulligan 2015) has significantly started to look at what the move from the law on the books to actual data privacy practices can mean, and they actually point out that there are signs of convergence at this level too. How this fits with the trends that I outlined in this work would be interesting to further investigate. There is also the question of how the different levels relate to each other. Do they necessarily contribute to bring themselves into balance or agreement, or could one tend to supersede or circumvent the others? On this point, recent work on the interactions between multiple networks or

layered networks could be a valuable starting point (Hollway and Koskinen 2016; Lazega and Snijders 2016).

Additional research could moreover explore how public and private rules are layered upon each other. In this work, I show that private rules tend to be layered on top of public rules. Another way to frame this is that the production of rules still follows a kind of top-down process, starting with public actors and ending with industry associations refining them. The reverse relationship where public rules are developed out of privates ones is not truly investigated. As I duly point out, industry associations can, however, create rules, which can even end up being taken up by public authorities. The GDPR notably includes rules that were both first devised or that were at least first promoted in Europe by industry associations. When does this occur and under which conditions remain open questions at this stage. This reversed relationship (i.e., where public actors learn from the regulatory activities of private actors) is an area that has still not received a lot of attention in the literature on private authority (Schmid et al. 2020).

Future work could finally attempt to unpack how interactions between public and private actors affect the formation of rules by distinguishing the different forms that they take. As it was most clearly highlighted for the European Commission, its involvement in the development of industry self-regulations has indeed varied over time. On different occasions, it provided funding, feedback, and official approval to them. Others in the literature on private authority also find other forms of involvement by public authorities, including benchmarking and procedural regulation (Gulbrandsen 2014; Renckens 2020). Meanwhile, among private actors, it was seen that their interactions could be through shared memberships or collaboration on a specific project. For the purposes of this research, these two different forms of interactions were both considered to offer an opportunity for information exchange. Nonetheless, it could be hypothesized that depending on the nature of the relation, the flow of information will not be the same. This could importantly provide a more fine-grained understanding of when informational exchanges are likely to matter. In the specific case of public authorities getting involved in the development of a private regulatory framework, it could moreover help identify if there are actually forms of interactions that could lead private regulations to act as 'regulatory sandboxes' and explore new rules while ensuring greater compliance with public rules.

Once again, the core claim that I made in this research is that interactions between heterogeneous actors active in multiple jurisdictions have upended the process of rule

formation. Public and private regulators in effect tend to exploit the rules of those with whom they had previously interacted and, when insufficient, to explore new ones based on these very same interactions. These processes moreover do not respect traditional jurisdictional boundaries, which offers new opportunities for transnational influence. By engaging with one or more of the sets of questions that I just highlighted, researchers can improve our understanding of these important dynamics by providing a more detailed picture of the actors involved, the direction of the relations of influence, and the nature of the interactions. This will help further demonstrate that the distinctions between national and international politics are often fuzzier than they seem and that national regulatory systems need to be appraised in light of their connections just as much as their differences.

Bibliography

Aaronson, Susan A. 2015. "Why Trade Agreements are not Setting Information Free: The Lost History and Reinvigorated Debate over Cross-Border Data Flows, Human Rights, and National Security." *World Trade Review* 14(4):671 – 700.

Aaronson, Susan A. and Patrick Leblond. 2018. "Another Digital Divide: The Rise of Data Realms and its Implications for the WTO." *Journal of International Economic Law* 21(2):245–272.

Abbott, Kenneth W. 2012. "The Transnational Regime Complex for Climate Change." *Environment and Planning C: Government and Policy* 30(4):571–590.

Abbott, Kenneth W. and Duncan Snidal. 2009*a*. "Strengthening International Regulation Through Transnational New Governance: Overcoming the Orchestration Deficit." *Vanderbilt Journal of Transnational Law* 42:501–577.

Abbott, Kenneth W. and Duncan Snidal. 2009*b*. The Governance Triangle: Regulatory Standards Institutions and the Shadow of the State. In *The Politics of Global Regulation*, ed. Walter Mattli and Ngaire Woods. Princeton: Princeton University Press pp. 44–88.

Abbott, Kenneth W. and Duncan Snidal. 2010. "International Regulation Without International Government: Improving IO Performance Through Orchestration." *Review of International Organizations* 5(3):315–344.

Abbott, Kenneth W., Jessica F. Green and Robert O. Keohane. 2016. "Organizational Ecology and Institutional Change in Global Governance." *International Organization* 70(2):247 – 277.

Abbott, Kenneth W., Robert O. Keohane, Andrew Moravcsik, Anne-Marie Slaughter and Duncan Snidal. 2000. "The Concept of Legalization." *International Organization* 54(3):401 – 419.

Aftab, Parry and Nancy L. Savitt. 1999. "Children's Legal Rights Journal Protecting Children's Privacy and Regulating Cybertot Marketing Practices Online." *Children's Legal Rights Journal* 19(2):2–13.

Akerlof, George A. 1970. "The Market for "Lemons": Quality Uncertainty and the Market Mechanism." *The Quarterly Journal of Economics* 84(3):488 – 500.

Alikhani, Kayvan. 2019. "Regulatory Disruption: Is Your Business Ready to Comply with the CCPA?" *Forbes* .
URL: *https://www.forbes.com/sites/forbestechcouncil/2019/06/06/regulatory-disruption-is-your-business-ready-to-comply-with-the-ccpa/*

Allee, Todd, Manfred Elsig and Andrew Lugg. 2017. "Is the European Union Trade Deal with Canada New or Recycled? A Text-as-data Approach." *Global Policy* 8(2):246–252.

Almunia, Joaquin. 2012. *Speech for the Privacy Platform Event: Competition and Privacy in Markets of Data*. Brussels: European Commission.
URL: *https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_12_860*

Alschner, Wolfgang and Dmitriy Skougarevskiy. 2016. "Mapping the Universe of International Investment Agreements." *Journal of International Economic Law* 19(3):561–588.

Alschner, Wolfgang, Joost Pauwelyn and Sergio Puig. 2017. "The Data-Driven Future of International Economic Law." *Journal of International Economic Law* 20(2):217–231.

Alter, Karen J. and Sophie Meunier. 2009. "The Politics of International Regime Complexity." *Perspectives on Politics* 7(01):13–24.

Amoore, Louise. 2014. "Security and the Claim to Privacy." *International Political Sociology* 8(1):108–112.

Armborst, Andreas. 2017. "Thematic Proximity in Content Analysis." *SAGE Open* 7(2):1–11.

Arthur, Brian W. and Wolfgang Polak. 2006. "The Evolution of Technology Within a Simple Computer Model." *Complexity* 11(5):23–31.

Article 29 Working Party. 2015. *Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing*. Brussels: European Commission.
URL: *https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2015/wp232_en.pdf*

Article 29 Working Party. 2016. *Fablab "GDPR/from concepts to operational toolbox,DIY" - Results of the Discussion*. Brussels: European Commission.
URL: *https://ec.europa.eu/justice/article-29/documentation/other-document/files/2016/20160930_fablab_results_of_discussions_en.pdf*

Ashby, William R. 1960. *Design for a Brain*. 2 ed. New York: John Wiley & Sons.

Atikcan, Ece O. and Adam W. Chalmers. 2019. "Choosing Lobbying Sides: The General Data Protection Regulation of the European Union." *Journal of Public Policy* 39(4):543–564.

Auld, Graeme. 2014. *Constructing Private Governance: The Rise and Evolution of Forest, Coffee, and Fisheries Certification*. New Haven and London: Yale University Press.

Avant, Deborah D., Martha Finnemore and Susan Sell. 2010. *Who Governs the Globe?* Cambridge: Cambridge University Press.

Axelrod, Robert and Michael Cohen. 2000. *Harnessing Complexity: Organizational Implications of a Scientific Frontier*. New York: Basic Books.

Bach, David and Abraham L. Newman. 2007. "The European Regulatory State and Global Public Policy: Micro-Institutions, Macro-Influence." *Journal of European Public Policy* 14(6):827–846.

Bach, David, Abraham L. Newman and Steven Weber. 2006. "The International Implications of China's Fledgling Regulatory State: From Product Maker to Rule Maker." *New Political Economy* 11(4):499–518.

Baldwin, Richard E. 2016. *The Great Convergence: Information Technology and the New Globalization*. Cambridge: Harvard University Press.

Bamberger, Kenneth A. and Deirdre K. Mulligan. 2015. *Privacy on the Ground: Driving Corporate Behavior in the United States and Europe*. Massachussets: MIT Press.

Barnett, Michael and Raymond Duvall. 2005. "Power in International Politics." *International Organization* 59(01):39–75.

Bartley, Tim. 2011. "Transnational Governance as the Layering of Rules: Intersections of Public and Private Standards." *Theoretical Inquiries in Law* 12(2):517–542.

Bartley, Tim. 2014. "Transnational Governance and the Re-Centered State: Sustainability or Legality?" *Regulation and Governance* 8(1):93–109.

Bartley, Tim. 2018. "Transnational Corporations and Global Governance." *Annual Review of Sociology* 44:145–165.

Bauman, Zygmunt, Didier Bigo, Paulo Esteves, Elspeth Guild, Vivienne Jabri, David Lyon and R. B. J. Walker. 2014. "After Snowden: Rethinking the Impact of Surveillance." *International Political Sociology* 8(2):121–144.

Becher, Shmuel and Uri Benoliel. 2020. Law in Books and Law in Action: The Readability of Privacy Policies and the GDPR. In *Consumer Law and Economics*, ed. Klaus Mathis and Avishalom Tor. Berlin: Springer.

Bell, Stephen. 2011. "Do We Really Need a New 'Constructivist Institutionalism' to Explain Institutional Change?" *British Journal of Political Science* 41(4):883–906.

Bellanova, Rocco and Paul De Hert. 2009. "Protection des données personnelles vers une perspective transatlantique." *Cultures et Conflits* 74:63–80.

Benkler, Yochai. 2011. "Wikileaks and the PROTECT-IP Act: A New Public-Private Threat to the Internet Commons." *Daedalus* 140(4):154–164.

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

Bennett, Colin J. 2010. "International Privacy Standards: A Continuing Convergence." *Privacy Laws & Business International Newsletter* 105:13–15.

Bennett, Colin J. and Charles Raab. 2006. *The Governance of Privacy: Policy Instrumentst in Perspective*. Massachussets: MIT Press.

Benyekhelef, Karim. 2015. *Une possible histoire de la norme: Les normativités émergentes de la mondialisation*. Montreal: Editions Themis.

Bernstein, Steven and Benjamin Cashore. 2007. "Can Non-State Global Governance Be Legitimate? An Analytical Framework." *Regulation & Governance* 1(4):347–371.

Bessette, Randi and Virginia Haufler. 2001. "Against All Odds: Why There Is No International Information Regime." *International Studies Perspectives* 2(1):69–92.

Betts, Alexander. 2009. "Institutional Proliferation and the Global Refugee Regime." *Perspectives on Politics* 7(1):53–58.

Borke, Robert. 1978. *The Antitrust Paradox*. New York: Free Press.

Börzel, Tanja A. and Thomas Risse. 2010. "Governance Without a State: Can it Work?" *Regulation and Governance* 4(2):113–134.

Boulianne, Emilio and Charles H. Cho. 2009. "The Rise and Fall of Webtrust." *International Journal of Accounting Information Systems* 10(04):229–244.

Bousquet, Antoine and Simon Curtis. 2011. "Beyond Models and Metaphors: Complexity Theory, Systems Thinking and International Relations." *Cambridge Review of International Affairs* 24(1):43–62.

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

Bradford, Anu. 2012. "The Brussels Effect." *Northwestern University Law Review* 107(1):1–68.

Bradford, Anu. 2020. *The Brussels Effect: How the European Union Rules the World*. Oxford: Oxford University Press.

Braithwaite, John. 2008. *Regulatory Capitalism: How it Works, Ideas for Making it Work Better*. Northampton: Edward Elgar.

Braithwaite, John and Peter Drahos. 2000. *Global Business Regulation*. Cambridge: Cambridge University Press.

Burdon, Mark. 2010. "Contextualizing the Tensions and Weaknesses of Information Privacy and Data Breach Notification Laws." *Santa Clara Computer & High Technology Law Journal* 27(1):63–129.

Büthe, Tim. 2010. "Private Regulation in the Global Economy: A (P)Review." *Business and Politics* 12(3):1–38.

Bygrave, Lee A. 2004. "Privacy Protection in a Global Context - A comparative Overview." *Scandinavian Studies in Law* 47:319–348.

Calver, Tom and Joe Miller. 2018. "Social Site Terms Tougher than Dickens." *BBCNews* .

URL: *https://www.bbc.com/news/business-44599968*

Campbell, John L., Charles Quincy, Jordan Osserman and Ove K. Pedersen. 2013. "Coding In-depth Semistructured Interviews: Problems of Unitization and Intercoder Reliability and Agreement." *Sociological Methods and Research* 42(3):294–320.

Cappocia, Giovanni. 2015. Critical Junctures and Institutional Change. In *Advances in Comparative Historical Analysis in the Social Sciences*, ed. James Mahoney and Kathleen Thelen. Cambridge: Cambridge University Press pp. 149–179.

Carpenter, R. Charli. 2011. "Vetting the Advocacy Agenda: Network Centrality and the Paradox of Weapons Norms." *International Organization* 65(1):69–102.

Carrington, Peter J., John Scott and Stanley Wasserman. 2005. *Models and Methods in Social Network Analysis*. Cambridge: Cambridge University Press.

Carstensen, Martin B. 2015. "Conceptualising Ideational Novelty: A Relational Approach." *British Journal of Politics and International Relations* 17(2):284–297.

Cashore, Benjamin. 2002. "Legitimacy and the Privatization of Environmental Governance: How Non-State Market-Driven (NSMD) Governance Systems Gain Rule-Making Authority." *Governance: An International Journal of Policy, Administration, and Institutions* 15(4):503–529.

Cashore, Benjamin, Deanna Newsom and Graeme Auld. 2004. *Governing Through Markets: Forest Certification and the Emergence of Non-State Authority*. New Haven: Yale University Press.

Cashore, Benjamin and Michael W. Stone. 2014. "Does California Need Delaware? Explaining Indonesian, Chinese, and United States Support for Legality Compliance of Internationally Traded Products." *Regulation and Governance* 8(1):49–73.

Castells, Manuel. 2004. *The Power of Identity*. Malden: Blackwell Publishers.

Cate, Fred H. 2000. "Principles of Internet Privacy." *Connecticut Law Review* 32(3):877–896.

Cavoukian, Ann and Malcolm Crompton. 2000. *Web Seals: A Review of Online Privacy Programs*. Venice: 22nd International Conference on Privacy and Data Protection. **URL:** *https://www.ipc.on.ca/wp-content/uploads/Resources/up-seals.pdf*

Cederman, Lars-Erik. 2003. "Modeling the Size of Wars: From Billiard Balls to Sandpiles Modeling the Size of Wars." *The American Political Science Review* 97(1):135–150.

Chander, Anupam, Margot E. Kaminski and William McGeveran. 2020. "Catalyzing Privacy Law." *Minnesota Law Review* Early view:1–55.

Checkel, Jeffrey T. 2005. "International Institutions and Socialization in Europe: Introduction and Framework." *International Organization* 59(4):801–826.

Christl, Wolfie, Katharina Kopp and Patrick Riechert. 2017. *How Companies Use Personal Data Use Against People*. Vol. October Vienna: Cracked Labs.

Christou, George and Seamus Simpson. 2007. *The New Electronic Marketplace: European Governance Strategies in a Globalising Economy*. Cheltenham: Edward Elgar.

Cilliers, Paul. 2001. "Boundaries, Hierarchies and Networks in Complex Systems." *International Journal of Innovation Management* 5(2):135–147.

Cohen, Julie E. 2000. "Examined Lives: Informational Privacy and the Subject as Object." *Stanford Law Review* 52(5):1373 – 1438.

Cudworth, Erika and Stephen Hobden. 2015. Complexifying International Relations for a Posthumanist World. In *World Politics at the Edge of Chaos: Reflections on Complexity and Global Life*, ed. Emilian Kavalski. New York: SUNY Press chapter 6, pp. 169–187.

Cunningham, Daniel, Sean Everton and Philip Murray. 2016. *Understanding Dark Networks*. Lanham: Rowman & Litttlefield.

Cutler, Claire A. 2002. Private International Regimes and Interfirm Cooperation. In *The Emergence of Private Authority in Global Governance*, ed. Rodney Bruce Hall and Thomas J. Biersteker. Cambridge: Cambridge University Press pp. 23–42.

Cutler, Claire A., Virginia Haufler and Tony Porter. 1999. *Private Authority and International Affairs*. Albany NY: State University of New York Press.

Damro, Chad. 2015. "Market Power Europe: Exploring a Dynamic Conceptual Framework." *Journal of European Public Policy* 22(9):1336–1354.

Davies, Margaret. 2010. Legal Pluralism. In *The Oxford Handbook of Empirical Legal Research*, ed. Peter Cane and Herbert M. Kritzer. Oxford: Oxford University Press pp. 805–824.

Davis, Christina L. 2009. "Overlapping Institutions in Trade Policy." *Perspectives on Politics* 7(1):25–31.

Davis, Kevin E. and Florencia Marotta-Wurgler. 2019. "Contracting for Personal Data." *New York University Law Review* 94(4):662–705.

De Búrca, Grainne, Robert O. Keohane and Charles Sabel. 2014. "Global Experimentalist Governance." *British Journal of Political Science* 44(3):477–486.

de Goede, Marieke. 2012. "The SWIFT Affair and the Global Politics of European Security." *Journal of Common Market Studies* 50(2):214–230.

de Goede, Marieke. 2014. "The Politics of Privacy in the Age of Preemptive Security." *International Political Sociology* 8(1):100–104.

De Hert, Paul, Vagelis Papakonstantinou, Gianclaudio Malgieri, Laurent Beslay and Ignacio Sanchez. 2018. "The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services." *Computer Law and Security Review* 34(2):193–203.

Della Porta, Donatella. 2008. Comparative Analysis: Case-Oriented Versus Variable-Oriented Research. In *Approaches and Methodologies in the Social Sciences: A Pluralist Perspective*, ed. Donatella Della Porta and Michael Keating. Cambridge: Cambridge University Press pp. 198–222.

DeNardis, Laura. 2009. *Protocol Politics: The Globalization of Internet Politics*. Cambridge: MIT Press.

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

Der Derian, James. 2003. "The Question of Information Technology in International Relations." *Millennium* 32(3):441–456.

DiMaggio, Paul J. and Walter W. Powell. 1983. "The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields." *American Sociological Review* 48(2):147–160.

Dimitrov, Radoslav S., Detlef F. Sprinz, Gerald M. DiGiusto and Alexander Kelle. 2007. "International Nonregimes: A Research Agenda." *International Studies Review* 9(2):230–258.

Direct Marketing Association. 2020. "DMA Consumer Choice Services.".
URL: *https://thedma.org/resources/compliance-resources/dma-consumer-choice-services/*

Dixon, Pam. 2007. *The Network Advertising Initiative: Failing at Consumer Protection and at Self-Regulation.* Washington D.C.: World Privacy Forum.

Dobbin, Frank, Beth Simmons and Geoffrey Garrett. 2007. "The Global Diffusion of Public Policies: Social Construction, Coercion, Competition, or Learning?" *Annual Review of Sociology* 33(1):449–472.

Drahos, Peter. 2017. Regulatory Globalisation. In *Regulatory Theory*, ed. Peter Drahos. Sydney: ANU Press.

Drezner, Daniel W. 2001. "Globalization and Policy Convergence." *International Studies Review* 3(1):53–78.

Drezner, Daniel W. 2007. *All Politics Is Global: Explaining International Regulatory Regimes.* Princeton: Princeton University Press.

Drezner, Daniel W. 2009. "The Power and Peril of International Regime Complexity." *Perspectives on Politics* 7(1):65–70.

Duit, Andreas and Victor Galaz. 2008. "Governance and Complexity - Emerging Issues for Governance Theory." *Governance* 21(3):311 – 335.

Dutton, John M. and William H. Starbuck. 1971. *Computer Simulation of Human Behavior.* New York: Wiley.

Eberlein, Burkard, Kenneth W. Abbott, Julia Black, Errol Meidinger and Stepan Wood. 2014. "Transnational Business Governance Interactions: Conceptualization and Framework for Analysis." *Regulation and Governance* 8(1):1–21.

EDRi. 2019. *EDPB Confirms: Privacy Shield is Still a Shame.* Brussels: European Digital Rights' Association.
URL: *https://edri.org/our-work/edpb-confirms-privacy-shield-is-still-a-shame/*

Elkins, Zachary, Andrew T. Guzman and Beth A. Simmons. 2006. "Competing for Capital: The Diffusion of Bilateral Investment Treaties, 1960-2000." *International Organization* 60(4):220–260.

Elkins, Zachary and Beth Simmons. 2005. "On Waves, Clusters, and Diffusion: A Conceptual Framework." *The Annals of of the American Academy of Political and Social Science* 598:33–51.

Elman, Colin and Miriam F. Elman. 2003. *Progress in International Relations Theory: Appraising the Field*. Cambridge (Massachussets): MIT Press.

Espinoza, Javier and Mehreren Khan. 2019. "UK at 'End of Queue' for Data Deal with Brussels." *Financial Times* .
URL: *https://www.ft.com/content/875a903e-2313-11ea-b8a1-584213ee7b2b*

Ess, Charles. 2005. ""Lost in translation"?: Intercultural dialogues on privacy and information ethics (Introduction to special issue on privacy and data privacy protection in Asia)." *Ethics and Information Technology* 7(1):1–6.

European Commission. 1994. *Europe and the Global Information Society*. Brussels: Official Publications of the European Communities.

European Commission. 2000. "Principles for E-Commerce Codes of Conduct.".
URL: *http://econfidence.jrc.it/default/show.gx?Object.objectid=ECFORUM0000000000000088*

European Commission. 2001*a*. *E-Commerce and Consumer Protection - A Survey of Codes of Practices and Certification Processes*. Luxembourg: Publications Office of the European Union.

European Commission. 2001*b*. *European Governance - A White Paper*. Brussels: Official Publications of the European Communities.
URL: *https://ec.europa.eu/commission/presscorner/detail/en/DOC0110*

European Commission. 2004. *Consumer Confidence in E-Commerce: Lessons Learned from the e-Confidence Initiative*. Brussels: Commission Staff Working Document SEC(2004) 1390.

European Commission. 2012*a*. *Commission Proposes a Comprehensive Reform of Data Protection Rules to Increase Users' Control of their Data and to Cut Costs for Businesses*. Brussels: Press Corner.
URL: *https://ec.europa.eu/commission/presscorner/detail/en/IP_12_46*

European Commission. 2012*b*. *EU Online Trustmarks: Building Digital Confidence in Europe*. Luxembourg: Publications Office of the European Union.
URL: *https://ec.europa.eu/digital-single-market/en/news/eu-online-trustmarks-—building-digital-confidence-europe-smart-20110022*

European Commission. 2015. *Questions and Answers - Data Protection Reform MEMO/15/6385*. Brussels: Press Corner.
URL: *https://ec.europa.eu/commission/presscorner/detail/en/MEMO_15_6385*

European Data Protection Board. 2019. *Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679*. Brussels: European Data Protection Board.
URL: *https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-20190219_guidelines_coc_public_consultation_version_en.pdf*

European Parliament. 2012. *A Pan-European Trustmark for E-Commerce: Possibilities and Opportunities*. Brussels: Directorate General for Internal Policies.
URL: *https://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL-IMCO_ET(2012)492433*

Ezrachi, Ariel and Maurice E. Stucke. 2016. *Virtual Competition: The Promise and Perils of the Algorithm-Driven Economy*. Cambridge: Harvard University Press.

Facebook. 2016. *BTO Meeting with Gerard De Graaf*. Brussels: Politico.
URL: *https://images.politico.eu/wp-content/uploads/2019/01/36-BTO-Meeting-GdG-03.16.pdf*

Farrell, Henry. 2003. "Constructing the International Foundations of E-Commerce: The EU - U.S. Safe Harbor Arrangement." *International Organization* 57(02):277 – 306.

Farrell, Henry. 2006. "Regulating Information Flows: States, Private Actors, and E-Commerce." *Annual Review of Political Science* 9:353–374.

Farrell, Henry and Abraham Newman. 2010. "Making Global Markets: Historical Institutionalism in International Political Economy." *Review of International Political Economy* 17(4):609–638.

Farrell, Henry and Abraham Newman. 2014. "Domestic Institutions Beyond the Nation State: Charting the New Interdependence Approach." *World Politics* 66(2):331–363.

Farrell, Henry and Abraham Newman. 2016. "The Transatlantic Data War: Europe Fights Back Against the NSA." *Foreign Affairs* 95:124 – 133.

Farrell, Henry and Abraham Newman. 2018. "Linkage Politics and Complex Governance in Transatlantic Surveillance." *World Politics* 70(4):515–554.

Farrell, Henry and Abraham Newman. 2019*a*. *Of Privacy and Power*. Princeton: Princeton University Press.

Farrell, Henry and Abraham Newman. 2019*b*. "Weaponized Interdependence." *International Security* 44(1):42–79.

Federal Trade Commission. 1998. *Privacy Online: A Report to Congress*. Washington D.C.: Federal Trade Commission.
URL: *https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf*

Federal Trade Commission. 2008. *Online Behavioral Advertising: Moving the Discussion Forward to Possible Self-Regulatory Principles*. Washington D.C.: FTC Staff Report.

Federal Trade Commission. 2009. *Self-Regulatory Principles for Online Behavioral Advertising*. Washington D.C.: FTC Staff Report.

Federal Trade Commission. 2010. *Protecting Consumer Privacy in an Era of Rapid Change*. Washington D.C.: Federal Trade Commission.
URL: *https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf*

Federal Trade Commission. 2014. *TRUSTe Settles FTC Charges it Deceived Consumers Through Its Privacy Seal Program*. Washington D.C.: FTC Press Release.
URL: *https://www.ftc.gov/news-events/press-releases/2014/11/truste-settles-ftc-charges-it-deceived-consumers-through-its*

Federal Trade Commission. 2019. *FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook*. Washington D.C.: FTC Press Release.
URL: *https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions*

Franda, Marcus. 2001. *Governing the Internet: The Emergence of an International Regime*. Boulder: Lynne Rienner Publishers.

Garber, Joe. 2018. "GDPR - Compliance Nightmare or Business Opportunity?" *Computer Fraud & Security* 6:14–15.

Gasser, Urs. 2016. "Recoding Privacy Law: Reflections on the Future Relationship Among Law, Technology, and Privacy." *Harvard Law Review Forrum* 130(2):61–70.

Geller, Anja. 2020. "How Comprehensive Is Chinese Data Protection Law? A Systematisation of Chinese Data Protection Law from a European Perspective." *GRUR International* Early View:1–14.

Gellman, Robert and Pam Dixon. 2016. Failures of Privacy Self-Regulation in the United States. In *Enforcing Privacy: Regulatory, Legal and Technological Approaches*, ed. David Wright and Paul De Hert. Springer pp. 53–77.

Gilardi, Fabrizio. 2010. "Who Learns from What in Policy Diffusion Processes?" *American Journal of Political Science* 54(3):650–666.

Gilardi, Fabrizio. 2012. Transnational Diffusion: Norms, Ideas, and Policies. In *Handbook of International Relations*, ed. Walter Carlsnaes, Thomas Risse and Beth Simmons. Thousand Oaks: SAGE Publications pp. 453–477.

Goldsmith, Jack and Tim Wu. 2006. *Who Controls the Internet? Illusions of a Borderless World*. Oxford: Oxford University Press.

Gordon, Sarah and Aliya Ram. 2018. "Information Wars: How Europe Became the World's Data Police." *Financial Times* .
URL: *https://www.ft.com/content/1aa9b0fa-5786-11e8-bdb7-f6677d2e1ce8*

Gourevitch, Peter. 1978. "The Second Image Reversed : The International Sources of Domestic." *International Organization* 32(4):881–912.

Grabs, Janina. 2020. *Selling Sustainability Short? The Private Governance of Labor and the Environment in the Coffee Sector*. Cambridge: Cambridge University Press.

Grande, Edgar and Louis W. Pauly. 2005. *Complex Sovereignty : Reconstituting Political Authority in the Twenty-First Century*. Toronto: Toronto University Press.

Granovetter, Mark S. 1973. "The Strength of Weak Ties." *American Journal of Sociology* 78(6):1360–1380.

Gray, Virginia. 1973. "Innovation in the States: A Diffusion Study." *American Political Science Review* 67(4):1174–1185.

Graz, Jean-Christophe and Andreas Nölke, eds. 2008. *Transnational Private Governance and its Limits*. Abingdon: Routledge.

Green Cowles, Maria. 2001. "Who Writes the Rules of e-Commerce? A Case Study of the Global Business Dialogue on e-Commerce." *AICPA Policy Papers* 14:1 – 35.

Green, Donald and Ian Shapiro. 1996. *Pathologies of Rational Choice Theory: A Critique of Applications in Political Science*. New Haven and London: Yale University Press.

Green, Jessica F. 2010. "Private Standards in the Climate Regime: The Greenhouse Gas Protocol." *Business and Politics* 12(3):1–37.

Green, Jessica F. 2013*a*. "Order out of Chaos: Public and Private Rules for Managing Carbon." *Global Environmental Politics* 13(2):1–25.

Green, Jessica F. 2013*b*. *Rethinking Private Authority: Agents and Entrepreneurs in Environmental Governance*. Princeton (NJ): Princeton University Press.

Green, Jessica F. and Graeme Auld. 2017. "Unbundling the Regime Complex: The Effects of Private Authority." *Transnational Environmental Law* 6(2):259–284.

Greenleaf, Graham. 2018. "Global Convergence of Data Privacy Standards and Laws: Speaking Notes for the European Commission Events on the Launch of the General Data Protection Regulation (GDPR) in Brussels & New Delhi, 25 May 2018." *UNSW Law Research Paper* 18-56:1–5.

Grimmer, Justin and Brandon M. Stewart. 2013. "Text as data: The promise and pitfalls of automatic content analysis methods for political texts." *Political Analysis* 21(3):267–297.

Guagnin, Daniel, Leon Hempel, Carla Ilten, Inga Kroener, Daniel Neyland and Hector Postigo, eds. 2012. *Managing Privacy through Accountability*. Basingstoke: Palgrave Macmillan.

Gulbrandsen, Lars H. 2014. "Dynamic governance interactions: Evolutionary effects of state responses to non-state certification programs." *Regulation and Governance* 8(1):74–92.

Haas, Ernst B. 1980. "Why Collaborate?: Issue-Linkage and International Regimes." *World Politics* 32(3):357–405.

Haas, Ernst B. 1982. "Words can hurt you; or, who said what to whom about regimes." *International Organization* 36(2):207–243.

Haas, Peter M. 1992. "Epistemic Communities and International Policy Coordination." *International Organization* 46(1):1–35.

Hafner-Burton, Emilie M., Miles Kahler and Alexander H. Montgomery. 2009. "Network Analysis for International Relations." *International Organization* 63(3):559–592.

Haggard, Stephan and Beth A. Simmons. 1987. "Theories of International Regimes." *International Organization* 41(3):491–517.

Hall, Peter. 1993. "Policy Paradigms, Social Learning, and the State: The Case of Economic Policymaking in." *Comparative Politics* 25(3):275–296.

Hall, Rodney Bruce and Thomas J. Biersteker, eds. 2002. *The Emergence of Private Authority in Global Governance*. Cambridge: Cambridge University Press.

Hannan, Michael T. and John Freeman. 1977. "The Population Ecology of Organizations." *American Journal of Sociology* 82(5):929 – 964.

Hannan, Michael T. and John Freeman. 1989. *Organizational ecology*. Cambridge: Harvard University Press.

Harcourt, Alison, George Christou and Seamus Simpson. 2020. *Global Standard Setting in Internet Governance*. Oxford: Oxford University Press.

Harrison, Neil. 2006. *Complexity in World Politics*. Vol. d Albany (NY): State University of New York Press.

Haufler, Virginia. 2001. *A Public Role for the Private Sector: Industry Self-Regulation in a Global Economy*. Washington D.C.: Brookings Institution Press.

Hayek, Friedrich. 1984. *Law, Legislation and Liberty: A New Statement of the Liberal Principles of Justice and Political Economy*. London: Routledge.

Hertzel, Dorothy A. 2000. "Don't Talk to Strangers: An Analysis of Government and Industry Efforts to Protect a Child's Privacy Online." *Federal Communications Law Journal* 52(2):429–451.

Hill, Jessica T. 2001. "The Cookie Monster: From Sesame Street to Your Hard Drive." *South Carolina Law Reivew* 52(4):921–954.

Hirsch, Dennis D. 2011. "The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?" *Seattle Univeristy Law Review* 34(2):439–480.

Hoffman, David A. 2014. "Privacy is a Business Opportunity." *Harvard Business Review* .

URL: *https://hbr.org/2014/04/privacy-is-a-business-opportunity*

Hoffmann, Matthew J. and John Riley Jr. 2002. "The Science of Political Science: Linearity or Complexity in Designing Social Inquiry." *New Political Science* 24(2):303–320.

Holland, John H. 1998. *Emergence: From Chaos to Order*. New York: Basic Books.

Holland, John H. 2006. "Studying complex adaptive systems." *Journal of Systems Science and Complexity* 19(1):1–8.

Hollway, James and Johan Koskinen. 2016. "Multilevel Embeddedness: The Case of the Global Fisheries Governance Complex." *Social Networks* 44:281–294.

Hoofnagle, Chris. 2005. Privacy Self Regulation: A Decade of Disappointment. In *Consumer Protection in the Age of the 'Information Economy'*, ed. Jane K. Winn. London and New York: Routledge pp. 379–402.

Hughes, Trevor J. 2008. *Network Advertising Initiatitve Written Comments in Response to the Federal Trade Commission Staff's Proposed Behavioral Advertising Principles*. Washington D.C.: Federal Trade Commission.

Ibáñez, Josep. 2008. Who Governs the Internet? The Emerging Regime of E-Commerce. In *Transnational Private Governance and its Limits*, ed. Jean-Christophe Graz and Andreas Nölke. Abingdon: Routledge pp. 142 – 155.

Information Commissionner's Office. 2019. *Guide to the General Data Protection Regulation*. Cheshire: Information Commissionner's Office.
URL: *https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf*

Jervis, Robert. 1997. *System effects: Complexity in Political and Social Life*. Princeton: Princeton University Press.

Jordana, Jacint and David Levi-Faur. 2005. "The Diffusion of Regulatory Capitalism in Latin America: Sectoral and National Channels in the Making of a New Order." *Annals of the American Academy of Political and Social Science* 598:102–124.

Judge, Kathryn. 2015. "Intermediary Influence." *University of Chicago Law Review* 82(2):573–642.

Kahler, Miles. 2016. "Complex Governance and the New Interdependence Approach (NIA)." *Review of International Political Economy* 23(5):825–839.

Karnitschnig, Matthew. 2020. "German Court Lays Down EU Law." *Politico* .

Kavalski, Emilian. 2007. "The Fifth Debate and the Emergence of Complex International Relations Theory: Notes on the Application of Complexity Theory to the Study of International Life." *Cambridge Review of International Affairs* 20(3):435 – 454.

Kavalski, Emilian. 2012. "Waking IR Up from its 'Deep Newtonian Slumber'." *Millenium* 41(1):137 – 150.

Keck, Margaret E. and Kathryn Sikkink. 1999. "Transnational Advocacy Networks in International and Regional Politics." *International Social Science Journal* 51(159):89–101.

Kelemen, Daniel R. and Giovanni Cappocia. 2007. "The Study of Critical Junctures: Theory, Narrative, and Counterfactuals in Historical Institutionalism." *World Politics* 59(3):341–369.

Kelley, Judith. 2009. "The More the Merrier? The Effects of Having Multiple International Election Monitoring Organizations." *Perspectives on Politics* 7(1):59–64.
URL: *http://sites.duke.edu/kelley/files/2012/03/POP.pdf*

Kellow, Aynsley. 2012. "Multi-Level and Multi-Arena Governance: The Limits of Integration and the Possibilities of Forum Shopping." *International Environmental Agreements: Politics, Law and Economics* 12(4):327–342.

Keohane, Robert O. 1984. *After Hegemony: Cooperation and Discord in the World Political Economy*. Princeton (NJ): Princeton University Press.

Keohane, Robert O. and David G. Victor. 2011. "The Regime Complex for Climate Change." *Perspectives on Politics* 9(1):7 – 23.

Keohane, Robert O. and Joseph S. Nye. 1974. "Transgovernmental Relations and International Organizations." *World Politics* 27(1):39–62.

Keohane, Robert O. and Joseph S. Nye. 1977. *Power and Interdependence: World Politics in Transition*. 4 ed. Boston: Longman.

Keohane, Robert O. and Lisa L. Martin. 1995. "The Promise of Institutionalist Theory." *International Security* 20(1):39–51.

Khan, Lina M. 2017. "Amazon's Antitrust Paradox." *Yale Law Journal* 126(3):710–805.

Kim, Rakhyun E. 2013. "The emergent network structure of the multilateral environmental agreement system." *Global Environmental Change* 23(5):980–991.

King, Gary, Robert O. Keohane and Sidney Verba. 1994. *Designing Social Inquiry.* Princeton: Princeton University Press.

Kitiyadisai, Krisana. 2005. "Privacy Rights and Protection: Foreign Values in Modern Thai Context." *Ethics and Information Technology* 7(1):17–26.

Knill, Christoph. 2005. "Introduction: Cross-National Policy Convergence: Concepts, Approaches and Explanatory Factors." *Journal of European Public Policy* 12(5):764–774.

Kobrin, Stephen J. 1998. "Back to the Future: Neomedievalism and the Postmodern Digital World Economy." *Journal of International Affairs* 51(2):361 – 386.

Kobrin, Stephen J. 2004. "Safe Harbours are Hard to Find: The Trans-Atlantic Data Privacy Dispute, Territorial Jurisdiction and Global Governance." *Review of International Studies* 30(1):111–131.

Korff, Douwe. 2002. EC Study on the Implementation of Data Protection Directive (2001/B5-3001/A/49). Technical Report September European Commission.
URL: *https://gegevensbeschermingsrecht.nl/onewebmedia/douwe.pdf*

Krasner, Stephen D. 1982. "Structural Causes and Regime Consequences: Regimes as Intervening Variables." *International Organization* 36(02):185–205.

Krasner, Stephen D. 1991. "Global Communications and National Power: Life on the Pareto Frontier." *World Politics* 43(3):336–366.

Lake, David A. 1996. "Anarchy, Hierarchy, and the Variety of International Relations." *International Organization* 50(1):1–33.

Lake, David A. 2009. "TRIPs Across the Atlantic: Theory and Epistemology in IPE." *Review of International Political Economy* 16(1):47–57.

Lascoutx, Elizabeth L. 2002. "Children's Advertising Review Unit." *Journal of Civil Rights and Economic Development* 16(3):649–653.

Lavenex, Sandra. 2014. "The Power of Functionalist Extension: How EU Rules Travel." *Journal of European Public Policy* 21(August 2015):885–903.

Lavenex, Sandra and Frank Schimmelfennig. 2009. "EU Rules Beyond EU Borders: Theorizing External Governance in European Politics." *Journal of European Public Policy* 16(6):791–812.

Lazega, Emmanuel and Tom A.B. Snijders, eds. 2016. *Multilevel Network Analysis for the Social Sciences*. New York: Springer.

Lazer, David. 2005. "Regulatory Capitalism as a Networked Order: The International System as an Informational Network." *Annals of the American Academy of Political and Social Science* 598:52–66.

Legro, Jeffrey W. 1997. "Which Norms Matter? Revisiting the "Failure" of Internationalism." *International Organization* 51(1):31–63.

Levi-Faur, David. 2017. Regulatory Capitalism. In *Regulatory Theory*, ed. Peter Drahos. Canberra: ANU Press.

Levi-Faur, David and Jacint Jordana. 2005*a*. "Globalizing Regulatory Capitalism." *The Annals of the American Academy of Political and Social Science* 598(1):6–9.

Levi-Faur, David and Jacint Jordana. 2005*b*. "The Rise of Regulatory Capitalism: The Global Diffusion of a New Order." *The Annals of the American Academy of Political and Social Science* 598(1):200–217.

LinkedIn. 2020. "Privacy Policy.".
URL: *https://www.linkedin.com/legal/privacy-policy*

Lipton, Eric and Danny Hapkim. 2013. "Lobbying Bonanza as Firms Try to Influence European Union.".
URL: *https://www.nytimes.com/2013/10/19/world/europe/lobbying-bonanza-as-firms-try-to-influence-european-union.html*

Litman-Navarro, Kevin. 2019. "We Read 150 Privacy Policies. They Were an Incomprehensible Disaster." *New York Times* .
URL: *https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html*

Long, William J. and Marc P. Quek. 2002. "Personal Data Privacy Protection in an Age of Globalization: The US-EU Safe Harbor Compromise." *Journal of European Public Policy* 9(3):325–344.

Low, Bobbi, Elinor Ostrom, Carl Simon and James Wilson. 2003. Redundancy and Diversity: Do they Influence Optimal Management? In *Navigating Social-Ecological Systems: Building Resilience for Complexity and Change*, ed. Fikret Berkes, Johan Colding and Carl Folke. Cambridge: Cambridge University Press pp. 83 – 114.

Lütz, Susanne. 2011. "Back to the Future? The Domestic Sources of Transatlantic Regulation." *Review of International Political Economy* 18(4):iii–xxii.

Ma, Shu-Yun. 2007. "Political Science at the Edge of Chaos? The Paradigmatic Implications of Historical Institutionalism." *International Political Science Review* 28(1):57–78.

Macenaite, Milda and Eleni Kosta. 2017. "Consent for Processing Children's Personal Data in the EU: Following in US Footsteps?" *Information and Communications Technology Law* 26(2):146–197.

Mahoney, James and Kathleen Thelen. 2010. *Explaining Institutional Change: Ambiguity, Agency, and Power*. Cambridge: Cambridge University Press.
URL: *http://library1.nida.ac.th/termpaper6/sd/2554/19755.pdf*

Majone, Giandomenico. 1994. "The Rise of the Regulatory State in Europe." *West European Politics* 17(3):77–101.

Manyika, James, James Chui, Brad Brown, Jacques Bughin, Richard Dobbs, Charles Roxburgh and Angela Hung Byers. 2011. *Big Data: The Next Frontier for Innovation, Competition, and Productivity*. New York: McKinsey Global Institute.

Manyika, James, Susan Lund, Jacques Bughin, Jonathan Woetzel, Kalin Stamenov and Dhruv Dhingra. 2016. *Digital Globalization : The New Era of Global Flows*. New York: McKinsey Global Institute.

March, James G. 1991. "Exploration and Exploitation in Organizational Learning." *Organization Science* 2(1):71–87.

Martins dos Santos, Bruna and Joana Varon. 2018. *Data and Politics - Brazilian Country Report*. Berlin: Coding Rights.
URL: *https://cdn.ttc.io/s/ourdataourselves.tacticaltech.org/ttc-data-and-politics-brazil.pdf*

Mattli, Walter and Ngaire Woods. 2009. In Whose Benefit? Explaining Regulatory Change in Global Politics. In *The politics of global regulation*, ed. Walter Mattli and Ngaire Woods. Princeton: Princeton University Press pp. 1–43.

Mattli, Walter and Tim Büthe. 2003. "Setting International Standards: Technological Rationality or Primacy of Power?" *World Politics* 56(1):1–42.

Mattli, Walter and Tim Büthe. 2005. "Accountability in Accounting? The Politics of Private Rule-Making in the Public Interest." *Governance* 18(3):399–429.

May, Robert M., Simon A. Levin and George Sugihara. 2008. "Ecology for Bankers." *Nature* 451(21):893–894.

Mayer-Schönberger, Viktor and Kenneth Cukier. 2013. *Big Data: A Revolution that Will Transform how We Live, Work and Think*. New York: Houghton Mifflin Harcourt.

Mazzucato, Mariana. 2011. *The Entrepreneurial State: Debunking Public vs. Private Sector Myths*. New York: PublicAffairs.

McDonald, Aleecia M. and Lori F. Cranor. 2008. "The Cost of Reading Privacy Policies." *I/S: A Journal of Law and Policy for the Information Society* 4(3):543–568.

McGeveran, William. 2016. "Friending the Privacy Regulators." *Arizona Law Review* 58(4):959–1026.
URL: *https://heinonline.org/HOL/License*

Meseguer, Covadonga. 2005. "Policy Learning, Policy Diffusion, and the Making of a New Order." *Annals of the American Academy of Political and Social Science* 598:67–82.

Meseguer, Covadonga. 2009. *Learning, Policy making and Market Reforms*. Cambridge: Cambridge University Press.

Meseguer, Covadonga and Fabrizio Gilardi. 2009. "What is New in the Study of Policy Diffusion?" *Review of International Political Economy* 16(3):527–543.

Meunier, Sophie and Jean-Frederic Morin. 2015. No Agreement is an Island: Negotiating TTIP in a Dense Regime Complex. In *The Politics of Transatlantic Trade Negotiations: TTIP in a Globalized World*, ed. Jean-Frederic Morin, Tereza Novotna, Frederik Ponjaert and Mario Telo. Farnham: Ashgate pp. 145–155.

Meyer, John W. 2000. "Globalization: Sources and Effects on National States and Societies." *International Sociology* 15(2):233–248.

Meyer, John W. and David Strang. 1993. "Institutional Conditions for Diffusion." *Theory and Society* 22(4):487–511.
URL: *https://link.springer.com/content/pdf/10.1007/BF00993595.pdf*

Miller, John H. and Scottt E. Page. 2007. *Complex Adaptive Systems: An Introduction to Computational Models of Social Life*. Princeton: Princeton University Press.

Mitchell, Melanie. 2009. *Complexity A Guided Tour*. Oxford: Oxford University Press.

Mitchener, Brandon. 2002. "Rules, Regulations of the Global Economy are Increasingly Being Set in Brussels." *The Wall Street Journal* .
URL: *https://www.wsj.com/articles/SB10195212402628453 60*

Modelski, George. 1996. "Evolutionary Paradigm for Global Politics." *International Studies Quarterly* 40(3):321–342.

Moore, Barrington. 1984. *Privacy: Studies in Social and Cultural History*. New York: Almonde.

Moravcsik, Andrew. 1997. "Taking Preferences Seriously : A Liberal Theory of International Politics." *International Organization* 51(4):513–553.

Morçöl, Goktug. 2012. *A Complexity Theory for Public Policy*. New York: Routledge.

Morin, Edgar. 1990. *Introduction à la complexité*. Paris: Le Seuil.

Morin, Edgar. 2007. Restricted Complexity, General Complexity. In *Science and us: Philosophy and Complexity*, ed. Carlos Gershenson, Diederik Aerts and Bruce Edmonds. Singapore: Word Scientific Publishing pp. 6–29.

Morin, Jean-Frederic, Joost Pauwelyn and James Hollway. 2017. "The Trade Regime as a Complex Adaptive System: Exploration and Exploitation of Environmental Norms in Trade Agreements." *Journal of International Economic Law* 20(2):365–390.

Murphy, Craig N. and Roger Tooze. 1991. Getting Beyond the "Common Sense" of the IPE Orthodoxy. In *The New International Political Economy*, ed. Craig N. Murphy and Roger Tooze. Boulder: Lynne Rienner Publishers pp. 11 – 31.

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

Newman, Abraham and Elliot Posner. 2015. "Putting the EU in its Place: Policy Strategies and the Global Regulatory Context." *Journal of European Public Policy* 22(9):1316–1335.

Newman, Abraham and Elliot Posner. 2016*a*. "Structuring Transnational Interests: The Second-Order Effects of Soft Law in the Politics of Global Finance." *Review of International Political Economy* 23(5):768–798.

Newman, Abraham and Elliot Posner. 2016*b*. "Transnational Feedback, Soft Law, and Preferences in Global Financial Regulation." *Review of International Political Economy* 23(1):123–152.

Newman, Abraham L. and David Bach. 2004. "Self-Regulatory Trajectories in the Shadow of Public Power: Resolving Digital Dilemmas in Europe and the U.S." *Governance: An International Journal of Policy, Administration, and Institutions,* 17(3):387–413.

North, Douglass. 1990. *Institutions, Institutional Change and Economic Performance.* Cambridge: Cambridge University Press.

Nye, Joseph S. and Robert O. Keohane. 1971. "Transnational Relations and World Politics: An Introduction." *International Organization* 25(3):329 – 349.

Oatley, Thomas. 2019. "Toward a Political Economy of Complex Interdependence." *European Journal of International Relations* pp. 1 – 22.

O'Connor, Nuala, Alethea Lange and Ali Lange. 2015. "Privacy in the Digital Age." *Great Decisions* pp. 17–28.

Onuf, Nicholas and Frank F. Klink. 1989. "Anarchy, Authority, Rule." *International Studies Quarterly* 33(2):149–173.

Orsini, Amandine, Jean-Frederic Morin and Oran Young. 2013. "Regime complexes: A buzz, a boom, or a boost for global governance?" *Global Governance* 19(1):27 – 39.

Orsini, Amandine, Philippe Le Prestre, Peter M. Haas, Malte Brosig, Philipp Pattberg, Oscar Widerberg, Laura Gomez-Mera, Jean-Frederic Morin, Neil E. Harrison, Robert Geyer and David Chandler. 2019. "Complex Systems and International Governance." *International Studies Review* pp. 1–30.

Overdevest, Christine and Jonathan Zeitlin. 2014. "Assembling an Experimentalist Regime: Transnational Governance Interactions in the Forest Sector." *Regulation and Governance* 8(1):22 – 48.

Padgett, John F. and Walter W. Powell. 2012. The Problem of Emergence. In *The Emergence of Organizations and Markets*, ed. John F. Padgett and Walter W. Powell. Princeton: Princeton University Press pp. 1 – 32.

Pagliari, Stefano and Meredith Wilf. 2020. "Regulatory Novelty after Financial Crises: Evidence from International Banking and Securities Standards, 1975 - 2016." *Regulation and Governance* Early View:1–19.

Parkins, David. 2017. "The world's most valuable resource is no longer oil, but data." *The Economist* .
URL: *https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data*

Pasquale, Frank. 2015. *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge: Harvard University Press.

Pauwelyn, Joost. 2014. "At the Edge of Chaos? Foreign Investment Law as a Complex Adaptive System, How It Emerged and How It Can Be Reformed." *ICSID Review* 29(2):372–418.

Posner, Elliot. 2009. "Making Rules for Global Finance: Transatlantic Regulatory Cooperation at the Turn of the Millennium." *International Organization* 63(4):665–699.

Posner, Richard A. 1978. "The Right of Privacy." *Georgia Law Review* 12(3):393–422.

Poulsen, Lauge and Emma Aisbett. 2016. "Diplomats Want Treaties: Diplomatic Agendas and Perks in the Investment Regime." *Journal of International Dispute Settlement* 7(1):72 – 91.

Powers, Shawn M. and Michael Jablonski. 2015. *The Real Cyber War*. Champaign: University of Illinois Press.

Prakash, Aseem and Matthew Potoski. 2012. "Voluntary Environmental Programs: A Comparative Perspective." *Journal of Policy Analysis and Management* 31(1):123–138.

Preston, Ethan and Paul Turner. 2004. "The Global Rise of a Duty to Disclose Information Security Breaches." *The John Marshall Journal of Computer and Information Law* 22(2):457–492.

Privacy International. 2012. *A New Dawn: Privacy in Asia*. London: Privacy International.
URL: *https://www.privacyinternational.org/reports/a-new-dawn-privacy-in-asia*

Puig, Sergio. 2014. "Social Capital in the arbitration market." *European Journal of International Law* 25(2):387–424.

Putnam, Tonya L. 2009. "Courts Without Borders: Domestic Sources of U.S. Extraterritoriality in the Regulatory Sphere." *International Organization* 63(3):459–490.

Radin, Margaret Jane. 1982. "Property and Personhood." *Stanford Law Review* 34(5):957–1015.

Raustiala, Kal. 2009. *Does the Constitution Follow the Flag? The Evolution of Territoriality in American Law*. Oxford: Oxford University Press.

Raustiala, Kal and David G. Victor. 2004. "The Regime Complex for Plant Genetic Resources." *International Organization* 58(2):277–309.

Raymond, Mark and Laura DeNardis. 2015. "Multistakeholderism: Anatomy of an Inchoate Global Institution." *International Theory* 7(03):572 – 616.

Recio, Miguel. 2017. "Data Protection Officer: The Key Figure to Ensure Data Protection and Accountability." *European Data Protection Law Review* 3(1):114–118.

Reidenberg, Joel. 1992. "Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?" *Federal Commnications Law Journal* 44(2):195–243.

Renckens, Stefan. 2020. *Private Governance and Public Authority. Regulating Sustainability in a Global Economy*. Cambridge: Cambridge University Press.

Risse-Kappen, Thomas. 1995. *Bringing Transnational Relations Back In*. Cambridge: Cambridge University Press.

Rodrigues, Rowena and Vagelis Papkonstantinou, eds. 2018. *Privacy and Data Protection Seals*. Berlin: Springer.

Rosenau, James N. 1990. *Turbulence in World Politics: A Theory of Change and Continuity*. Princeton: Princeton University Press.

Rosenau, James N. 1995. "Governance in the Twenty-first Century." *Global Governance* 1(1):13–43.

Rosenau, James N. 1997. *Along the Domestic-Foreign Frontier: Exploring Governance in a Turbulent World*. Cambridge: Cambridge University Press.

Rosenau, James N. 2003. *Distant Proximities: Dynamics beyond Globalization*. Princeton: Princeton University Press.

Rosenau, James N. 2005. Global Governance as Disaggregated Complexity. In *Contending Perspectives on Global Governance: Coherence and Contestation and world order*, ed. Matthew J. Hoffmann and Alice D. Ba. London and New York: Routledge pp. 131–153.

Rothchild, John A., ed. 2016. *Research Handbook on Electronic Commerce Law*. Cheltenham: Edward Elgar.

Ruggie, John G. 1975. "International Responses to Technology: Concepts and Trends." *International Organization* 29(3):557–583.

Ruggie, John G. 2004. "Reconstituting the Global Public Domain - Issues, Actors, and Practices." *European Journal of International Relations* 10(4):499–531.

Ruhl, J. B. 2014. "Managing Systemic Risk in Legal Systems." *Indiana Law Journal* 89(2):559–603.

Ruhl, J. B., Daniel Martin Katz and Michael J. Bommarito. 2017. "Harnessing Legal Complexity." *Science* 355(6332):1377–1378.

Rule, James B. 2009. *Privacy in Peril*. Oxford: Oxford University Press.

Sabel, Charles and Jonathan Zeitlin, eds. 2010. *Experimentalist Governance in the European Union: Towards a New Architecture*. Oxford: Oxford University Press.

Saliba, Clare. 2001. "Global E-Commerce Conduct Code in the Works." *E-Commerce Times* .
URL: *https://www.ecommercetimes.com/story/9172.html*

Satariano, Adam. 2018. "G.D.P.R., A New Privacy Law, Makes Europe World's Leading Tech Watchdog." *New York Times* .
URL: *https://www.nytimes.com/2018/05/24/technology/europe-gdpr-privacy.html*

Satariano, Adam. 2019. "Google Is Fined $57 Million Under Europe's Data Privacy Law.".
URL: *https://www.nytimes.com/2019/01/21/technology/google-europe-gdpr-fine.html*

Schmid, Nicolas, Leonore Haelg, Sebastian Sewerin, Tobias S. Schmidt and Irina Simmen. 2020. "Governing Complex Societal Problems: The Impact of Private on Public Regulation through Technological Change." *Regulation and Governance* Early View:1–16.

Schwartz, Paul M. 2019. "Global data privacy: The EU way." *New York University Law Review* 94(4):771–818.

Schwartz, Paul M. and Karl Nikolaus Peifer. 2017. "Transatlantic Data Privacy Law." *Georgetown Law Journal* 106(1):115–179.

Scott, Colin. 2003. Regulation in the Age of Governance: The Rise of the Post- Regulatory State. In *The Politics of Regulation*, ed. Jacint Jordana and David Levi-Faur. Cheltenham: Edward Elgar pp. 145–175.

Seabrooke, Leonard and Eleni Tsingou. 2014. "Distinctions, Affiliations, and Professional Knowledge in Financial Reform Expert Groups." *Journal of European Competition Law & Practice* 21(1):389 – 407.

Seawright, Jason. 2016. *Multi-Method Social Science: Combining Qualitative and Quantitative Tools*. Cambridge (UK): Cambridge University Press.

Shearing, Cifford D. 1993. A Constitutive Conception of Regulation. In *Business Regulation and Australia's Future*, ed. Peter Grabosky and John Braithwaite. Canberra: Australian Institute of Criminology pp. 67–80.

Shulz, Wolfgang and Thorsten Held. 2004. *Regulated Self-Regulation as a Form of Modern Government: An Analysis from Case Studies from Media and Telecommunications Law*. Bloomington: Indiana University Press.

Simitis, Spiros. 1995. "From the Market to the Polis : The EU Directive on the Protection of Personal." *Iowa Law review* 80(3):445–470.

Simmons, Beth A. and Zachary Elkins. 2004. "The Globalization of Liberalization: Policy Diffusion in the International Political Economy." *The American Political Science Review* 98(1):171–189.

Singleton, Solveig. 2002. *Privacy as a Trade Issue: Guidelines for U.S. Trade Negotiators*. Washington D.C.: Heritage Foundation.

Slaughter, Anne-Marie. 2004. *A New World Order*. Princeton: Princeton University Press.

Solove, Daniel J. 2004. *The Digital Person*. New York: New York University Press.

Solove, Daniel J. and Paul M. Schwartz. 2011. *Information Privacy Law*. Fourth ed. New York: Wolters Kluwer.

Spar, Debora L. 1999. Lost in (Cyber) space: The Private Rules of Online Commerce. In *Private Authority and International Affairs*, ed. Claire Cutler, Virginia Haufler and Tony Porter. Albany NY: State University of New York Press pp. 31–51.

Sparke, Matthew. 2013. *Introducing Globalization: Ties, Tensions, and Uneven Integration*. Malden: Blackwell Publishers.

Spencer, Shaun B. 2016. Predictive Analytics, Consumer Privacy, and E-commerce Regulation. In *Research Handbook on Electronic Commerce Law*, ed. John A. Rothchild. Cheltenham: Edward Elgar pp. 492–518.

Spruyt, Hendrik. 2001. "The Supply and Demand of Governance in Standard-Setting: Insights from the Past." *Journal of European Public Policy* 8(3):371–91.

Srnicek, Nick. 2017. *Platform Capitalism*. Cambridge: Polity.

Strange, Susan. 1994. "Wake up, Krasner! The World Has Changed." *Review of International Political Economy* 1(2):201 – 219.

Strange, Susan. 1996. *The Retreat of the State*. Cambridge: Cambridge University Press.

Stucke, Maurice E. and Allen P. Grunes. 2016. *Big Data and Competition Policy*. Oxford: Oxford University Press.

Tempest, Alastair. 2007. Robinson Lists for Efficient Direct Marketing. In *International Direct Marketing*, ed. Manfred Krafft, Jurgen Hesse, Jurgen Hofling, Kay Peters and Diane Rinas. Berlin: Springer pp. 129–154.

Tene, Omer and Trevor J. Hughes. 2014. "The Promise and Shortcomings of Privacy Multistakeholder Policymaking: A Case Study." *Maine Law Review* 66(2):438–465.

Thoma, Florian. 2012. How Siemens Assesses Privacy Impacts. In *Privacy Impact Assessment*, ed. David Wright and Paul De Hert. Berlin: Springer pp. 275–284.

Trzaskowski, Jan. 2006. *E-Commerce Trustmarks in Europe - An Overview and Comparison of Trustmarks in the European Union, Norway and Lichtenstein*. Copenhagen: European Consumer Centre of Denmark.

Turkina, Ekaterina and Evgeny Postnikov. 2012. "Cross-Border Inter-firm Networks in the European Union's Eastern Neighbourhood: Integration via Organizational Learning." *Journal of Common Market Studies* 50(4):632–652.

Turkina, Ekaterina and Evgeny Postnikov. 2014. "From Business to Politics: Cross-Border Inter-Firm Networks and Policy Spillovers in the EU's Eastern Neighbourhood." *Journal of Common Market Studies* 52(5):1120–1141.

Tusikov, Natasha. 2016. *Chokepoints: Global Private Regulation on the Internet*. Oakland: University of California Press.

UNCTAD. 2020. *Data Protection and Privacy Legislation Worldwide*. Geneva: United Nations Conference on Trade and Development.

U.S. Department of Health Education and Welfare. 1973. *Records, Computers and the Rights of Citizens*. Washington D.C.: U.S. Department of Health Education and Welfare.

Valentino-Devries, Jennifer, Natasha Singer, Michael H. Keler and Aaron Krolik. 2018. "Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret." *The New York Times* .
URL: *https://www.nytimes.com/2018/12/10/technology/location-tracking-apps-privacy.html*

Varoufakis, Yanis. 1998. *Foundations of Economics: A Beginner's Companion*. London: Routledge.

Vogel, David. 1995. *Trading Up: Consumer and Environmental Regulation in a Global Economy*. Cambridge: Harvard University Press.

Vogel, David. 2003. "The Hare and the Tortoise Revisited: The New Politics of Consumer and Environmental Regulation in Europe." *British Journal of Political Science* 33(4):557–580.

Vogel, David. 2005. *The Market for Virtue*. Washington D.C.: Brookings Institution Press.

Vogel, David. 2008. "Private Global Business Regulation." *Annual Review of Political Science* 11(1):261–282.

Vogel, David. 2012. *The Politics of Precaution: Regulating Health, Safety and Environmental Risks in Europe and the United States*. Princeton: Princeton University Press.

Waltz, Kenneth. 1979. *Theory of International Politics*. Reading: Addison-Wesley.

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

Wasserman, Stanley and Katherine Faust. 1994. *Social Network Analysis: Methods and Applications*. Cambridge: Cambridge University Press.

Waterson, Jim. 2018. "UK Fines Facebook £500,000 for Failing to Protect User Data.". **URL:** *https://www.theguardian.com/technology/2018/oct/25/facebook-fined-uk-privacy-access-user-data-cambridge-analytica*

Weiss, Linda. 2014. *America Inc.? Innovation and Enterprise in the National Security State*. Ithaca: Cornell University Press.

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

White & Case. 2019. *GDPR Handbook: Unlocking the EU General Data Protection Regulation*. New York: White & Case LLP.
URL: *https://www.whitecase.com/publications/article/gdpr-handbook-unlocking-eu-general-data-protection-regulation*

Wu, Tim. 2018. *The Curse of Bigness: Antitrust in the New Gilded Age*. New York: Columbia Global Reports.

Yao Huai, Lu. 2005. "Privacy and Data Privacy Issues in Contemporary China." *Ethics and Information Technology* 7(1):7–15.

Youn, Hyejin, Deborah Strumsky, Luis M.A. Bettencourt and Jose Lobo. 2015. "Invention as a Combinatorial Process: Evidence From US Patents." *Journal of the Royal Society Interface* 12(106):1–8.

Young, Alasdair R. 2003. "Political Transfer and "Trading Up"?: Transatlantic Trade in Genetically Modified Food and U.S. Politics." *World Politics* 55(4):457–484.

Young, Alasdair R. 2015*a*. "Liberalizing Trade, not Exporting Rules: The Limits to Regulatory Co-ordination in the EU's 'New Generation' Preferential Trade Agreements." *Journal of European Public Policy* 22(9):1253–1275.

Young, Alasdair R. 2015*b*. "The European Union as a Global Regulator? Context and Comparison." *Journal of European Public Policy* 22(9):1233–1252.

Young, Oran R. 1980. "International Regimes: Problems of Concept Formation." *World Politics* 32(3):331–356.

Young, Oran R. 2017. *Governing Complex Systems.* Cambridge: MIT Press.

Zarakol, Ayse, ed. 2017. *Hierarchies in World Politics.* Cambridge: Cambridge University Press.

Zuboff, Soshana. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power.* New York: PublicAffairs.

Appendices

Appendix A

List of interviewees

Name	Organization	Title
Marty Abrams	The Information Accountability Foundation	Executive Director
Carlos Almaraz	Business Europe (then called UNICE)	Deputy Director (2000-2010)
Razvan Antemir	European eCommerce and Omni Channel Trade Association	Legal Advisor
Rosa Barcelo	DG Connect	Deputy Head of Unit – Cybersecurity and Privacy (2016 - 2018)
Senny Boone	Direct Marketing Association	General Counsel, SVP, Compliance & Ethics
Thomas Boué	Business Software Association	Director General for EMEA Policy
Jasmin Battista	DG Connect	Head of Sector – E-Commerce
Isabelle Chatelier	DG Justice	Legal and Policy Advisor – Data Protection Unit
Willem Debeuckelaere	European Data Protection Board	Vice-Chair
Michael Donohue	Organisation for Economic Co-operation and Development	Senior Policy Analyst
John Falzone	Entertainment Software Rating Board	Vice-President of Privacy Certified
Caitlin Fennessy	International Trade Administration – U.S. Department of Commerce	Privacy Shield Director (2018 - 2019)
Bruno Gencarelli	DG Justice	Head of Unit – Data Protection
Andrea Gil	eCommerce Foundation	Trustmark Coordinator
Alisha Guhr	Datenschutz	Legal Counsel
Hans Graux	Timelex	Legal Advisor

Continued on next page

Continued from previous page

Name	Organization	Title
Oliver Gray	European Digital Advertising Alliance	Director-General
Josh Harris	TrustArc	Director, International Regulatory Affairs
Frances Henderson	BetterBusinessBureau	Vice President and National Director, Privacy Initiatives
Markus Heyder	Centre for Information Leadership	Vice President and Senior Policy Counselor
Matt Joseph	VeraSafe	Managing Director and Data Protection Leader
Sara Lone	eCommerce Foundation	Senior Research Analyst and Coordinator
Joanna Lopatowska	Eurocommerce	Advisor on Consumer Policy
Robert Madelin	DG Connect	Director-General (2010 - 2015)
Anthony Matyjaszewski	Network Advdertising Initiative	Vice President, Compliance and Membership
David Martin	The European Consumer Organisation (BEUC)	Head of Digital Unit
Ionel Naftanaila	European Digital Advertising Alliance	Programme Development Director
Jules Polonetsky	The Future of Privacy Forum	Chief Executive Officer
Geraldine Proust	Federation of European Direct Marketing Associations	Director of Legal Affairs
Guilherme Roschke	Federal Trade Commission	Counsel for International Consumer Protection
Michael Rose	International Trade Administration – U.S. Department of Commerce	Advisor for the Global Data Policy Team
Kim Smouter-Umans	European Society for Opinion and Marketing Research	Head of Public Affairs
Malin Strandell-Jansson	McKinsey & Co.	Consultant
John P. Tomaszewski	TrustArc (then called TRUSTe)	General Counsel & Point of contact for the World Trustmark Alliance (2006 - 2013)
Alisa Vekeman	DG Justice	Legal Advisor – Data Protection Unit
Wojciech Wiewiórowski	European Data Protection Supervisor	Assistant supervisor

Appendix B

List of database documents

Organization	Main country or region of activity	Name of regulation	Year of adoption or revision
AICPA	United States	Webtrust	1997
AICPA	United States	Webtrust	1999
AICPA	United States	Webtrust	2003
AICPA	United States	Webtrust	2004
AICPA	United States	Webtrust	2006
AICPA	United States	Webtrust	2009
APEC	Asia-Pacific	Privacy Framework	2005
BBB	United States	BBBOnline Privacy Program	1999
BBB	United States	BBBOnline Privacy Program	2000
BBB	United States	BBBOnline Privacy Program	2002
BBB	United States	BBBOnline Privacy Program	2004
BEUC-UNICE	European Union	European Trustmark	2001
ClickSure	United Kingdom	ClickSure Principles	2001
Cloud providers	European Union	Code of Conduct for Cloud Service Providers	2016
DAA	United States	OBA Principles	2009
DMA	United States	Ethical Guidelines	1997
DMA	United States	Ethical Guidelines	2002
DMA	United States	Ethical Guidelines	2004
DMA	United States	Ethical Guidelines	2006
DMA	United States	Ethical Guidelines	2007
DMA	United States	Ethical Guidelines	2011
DMA	United States	Ethical Guidelines	2014
DMA	United States	Ethical Guidelines	2016

Continued on next page

Continued from previous page

Organization	Main country or region of activity	Name of regulation	Year of adoption or revision
EASA	European Union	Best Practice Recommendation on OBA	2011
EASA	European Union	Best Practice Recommendation on OBA	2016
ECCPG	United States	E-Commerce Guidelines	2000
E-Commerce Europe	European Union	Code of Conduct 2015	
E-Commerce Foundation	European Union	SafeShop Trustmark	2017
EDAA	European Union	Self-Certification Criteria for OBA	2012
EMOTA	European Union	European Trustmark	2002
ERA.Europe	European Union	Europe Guidelines	2005
ESOMAR	Global	International code on market and social research	1994
ESOMAR	Global	International code on market and social research	2001
ESOMAR	Global	International code on market and social research	2007
ESOMAR	Global	International code on market and social research	2016
ESRB	United States	Privacy Online Principles and Guidelines	2000
ESRB	United States	Privacy Online Principles and Guidelines	2001
ESRB	United States	Privacy Online Principles and Guidelines	2003
ESRB	United States	Privacy Online Principles and Guidelines	2006
EU-US	Transatlantic area	Safe Harbor	2000
EU-US	Transatlantic area	Privacy Shield	2016
EuroCommerce	European Union	Euro-Label	2000
EuroCommerce	European Union	Euro-Label	2002
European Commission	European Union	Data Directive	1995
European Commission	European Union	ePrivacy Directive	2002
European Commission	European Union	Data Retention Directive	2006

Continued on next page

Continued from previous page

Organization	Main country or region of activity	Name of regulation	Year of adoption or revision
European Commission	European Union	ePrivacy Directive Amendments	2006
European Commission	European Union	General Data Protection Regulation	2016
EuroPrise	European Union	Privacy Seal	2011
EuroPrise	European Union	Privacy Seal	2017
FEDMA	European Union	Code of Conduct for e-commerce	2000
FEDMA	European Union	Code of Practice for the Use of Personal Data in Direct Marketing	2003
FEDMA	European Union	Code of Pratice with Annex on OBA	2010
GBDe	Global	Privacy Guidelines	2000
GBDe	Global	Global Trustmark	2001
IA	United States	Code of Conduct	1997
IA	United States	Code of Conduct	1998
IAB	United States	Code of Conduct	2011
IAB.Europe	European Union	European OBA Framework	2011
ICC	Global	Code on Advertising and Marketing on the Internet	1999
ICC	Global	Code of Direct Marketing	2001
ICC	Global	Consolidated Code on Advertising and Marketing	2006
ICC	Global	Consolidated Code on Advertising and Marketing	2011
ICDPPC	Global	Madrid Resolution	2009
IMRG	United Kingdom	Code of Practice	2000
IMRG	United Kingdom	Code of Practice	2003
IMRG	United Kingdom	Code of Practice	2004
IMRG	United Kingdom	Code of Practice	2005
IMRG	United Kingdom	Code of Practice	2008
IRSG	United States	Industry Principles	1997
Health Application Developers	European Union	mHealth Code of Conduct	2016
NAI	United States	Code of Conduct	2000
NAI	United States	Code of Conduct	2008
NAI	United States	Code of Conduct	2013
NAI	United States	Code of Conduct	2015
NAI	United States	Code of Conduct	2018

Continued on next page

Continued from previous page

Organization	Main country or region of activity	Name of regulation	Year of adoption or revision
OECD	Global	Privacy Guidelines	1980
OECD	Global	Privacy Guidelines	2013
OPA	United States	Guidelines for Online Privacy Policies	1999
PwC	United States	BetterWeb Standards	2000
SafeBuy	United Kingdom	Code of Practice	2003
SafeBuy	United Kingdom	Code of Practice	2004
SafeBuy	United Kingdom	Code of Practice	2006
SafeBuy	United Kingdom	Code of Practice	2007
SafeBuy	United Kingdom	Code of Practice	2011
SquareTrade	United States	SquareTrade Seal	2001
TrustArc (TRUSTe)	United States	Privacy Program	2000
TrustArc (TRUSTe)	United States	Privacy Program	2004
TrustArc (TRUSTe)	United States	Privacy Program	2012
TrustArc (TRUSTe)	United States	Privacy Program	2017
TrustArc (TRUSTe)	United States	Privacy Program	2018
TrustedShops	Germany	Quality Criteria	2001
TrustedShops	Germany	Quality Criteria	2003
TrustedShops	Germany	Quality Criteria	2008
TrustedShops	Germany	Quality Criteria	2009
TrustedShops	Germany	Quality Criteria	2012
TrustedShops	Germany	Quality Criteria	2014
TrustedShops	Germany	Quality Criteria	2015
TUV SUD	Germany	Safer Shopping	2001
TUV SUD	Germany	Safer Shopping	2003
TUV SUD	Germany	Safer Shopping	2004
TUV SUD	Germany	Safer Shopping	2005
TUV SUD	Germany	Safer Shopping	2006
TUV SUD	Germany	Safer Shopping	2007
TUV SUD	Germany	Safer Shopping	2009
TUV SUD	Germany	Safer Shopping	2010
TUV SUD	Germany	Safer Shopping	2014

Continued on next page

Continued from previous page

Organization	**Main country or region of activity**	**Name of regulation**	**Year of adoption or revision**
US Government	United States	Health Insurance Portability and Accountability's Privacy Rule	2000
US Government	United States	Health Insurance Portability and Accountability's Privacy Rule	2013
US Government	United States	Federal Trade Commission Fair Information Practices Principles	1998
US Government	United States	CAN-SPAM Act	2003
US Government	United States	Children's Online Privacy Protection Act	1999
US Government	United States	Children's Online Privacy Protection Act Amended	2002
US Government	United States	Children's Online Privacy Protection Act Amended	2005
US Government	United States	Children's Online Privacy Protection Act Amended	2013
US Government	United States	Fair and Accurate Credit Transactions Act	2003
US Government	United States	Graham-Leach-Bliley Act	1999
Verasafe	United States	Privacy Program Certification Criteria	2014
Verasafe	United States	Privacy Program Certification Criteria	2015
Verasafe	United States	Privacy Program Certification Criteria	2017
Which	United Kingdom	Webtrader	1999
Which	United Kingdom	Webtrader	2000
Which	United Kingdom	Webtrader	2002
WTA	Global	Global Guidelines	2008

Appendix C

Codebook

Methodology

How were the documents collected?

- This database includes publicly available regulations in Europe and the United States dealing with privacy and data protection issues. The concept of regulation was understood in a broad sense and includes laws, directives, guidelines, codes of conduct and private requirements. The mere explanation of the sense of a law or a code was however not considered to be a regulation in itself.
- Documents only dealing with technical matters of operating a website (e.g.: server security or web architecture) were excluded. This database only focuses on data protection rules, not technical standards.
- Both public and private regulations in the transatlantic area were included.
- The laws or regulations of U.S. federal states or EU Member States were not included.
- Similarly, only the regulations adopted by private associations operating at the European level (or in at least more than two Member States) or US federal level were included. Private associations only active in one EU member state or one U.S. federal state are not part of this database.
- Regulations adopted by transnational private associations active in the transatlantic area were included.

- To access and download older versions of private regulations, the digital archive *Wayback Machine* was used. This archive made possible to collect almost all documents put forward by private associations in the transatlantic area since 1995.
- Only regulations that were in force between 1995 and 2017. The choice of 1995 as a starting date reflects the year of adoption of the European Data directive in 1995. Only two regulations adopted before that were included: the OECD privacy guidelines of 1980 and the 1994 code of marketing and social research practice jointly adopted by the ICC and ESOMAR.

What counts as a "rule"?

- Rules are standards of behavior followed, voluntarily or not, by an actor.
- Rules can have a high degree ("must", "shall", "will", etc.) or low degree ("may", "could", "encourage") of commitment.
- Rules can be found in a single sentence or an entire paragraph. Similarly, a rule can be really detailed or really broad.
- Rules potentially found in the preamble, the foreword or the explanatory memorandum of a regulatory document were not considered. The explanatory memorandum could however be used to clarify the meaning of a rule and code it accordingly.
- Lists of definitions and objectives were also not considered as creating rules.
- Rules can be repeated many times in the same regulatory document. Those repetitions do not need to be found in the same parts of the regulation.
- Vague references to another article or another regulation were not considered as incorporating the rules found in them.
- Similarly, it is not assumed that a general reference to another regulation means that an actor adhere to all the rules potentially found in it. It is only coded when it is clearly mentioned that the actor will apply the rules put forward in the regulations.

What counts as "data protection"?

- Data protection broadly refers to measures taken to insure that personal data are safeguarded against any wrongful actions.
- "Personal information" are understood as a synonymous of personal data.
- Rules aiming to protect "data privacy" are also included.

- This database only focuses on data controller's obligations towards data subjects and on data subject's rights vis-a-vis data controllers. Data controllers' obligations towards states or states' obligations towards data subjects were not coded.

- Importantly, this codebook uses a terminology ("data subjects", "data controllers", "data protection", etc.), which is traditionally used in Europe. This however does not reflect any personal preference for the EU model. It is moreover not intended to exclude rules using another terminology, such as the American one ("individuals", "consumers", "privacy", etc.). This codebook aims to compare the extent to which rules on "data protection" or "data privacy" are substantively similar, not how similar their terminology is.

Coding rules

01. Transparency

- Broadly refers to data controllers' obligations to clearly inform and notify data subjects of their data collection practices.
- Include data controllers' obligation to publish a "privacy notice", "privacy policy", "privacy statement" or "policy content".
- Include data controllers' obligation to follow an openness principle and inform data subjects of their online practices.
- The content of the privacy policies or the nature of the information that data controllers must give to data subjects should be coded in their respective nodes.

01.01 Privacy statement

- Include the obligation for data controllers to publish a privacy notice or statement on their website.
- Include any mention that a data controller should broadly inform or describe its privacy practices to data subjects.
- Include the obligation for data controllers to have a privacy notice, which is clear, conspicuous and/or easy-to-read.
- Include the obligation for third parties to provide notice on their own website. However, the obligation for data controllers to inform data subjects that third parties collect their personal data should be coded in node 01.09.
- Exclude the obligation to provide information with the aim to educate consumers (see node 15). Only code here the obligation for data controllers to inform data subjects or their consumers of their own privacy practices.

01.02 Data controller's identity

- Include the obligation for data controllers to inform data subjects of their identity.
- Include any rules stating that data controllers must provide their contact information in their privacy notice or statement.

01.03 Data types and purposes

- Refer to the obligation for data controllers to inform data subjects of the types and purposes (or nature) of data affected by their data collection or processing practices.
- Include rules requesting data controllers to say how they will use personal data.
- Include the obligation for data controllers to indicate that no personal data is collected or that some types of personal data are excluded from their data collection and processing practices.

01.04 Data source

- Include any rules requiring data controllers to inform data subjects of the source of their data.
- Include the obligation for data controllers to inform data subjects when they merge their data with personal data collected from other sources.
- Include rules indicating that data controllers cannot prohibit other controllers or users of personal data to inform data subjects that they are the ones which originally collected their personal information.

01.05 Data retention time

- Include any rules stating that data controllers must inform data subjects of how long their personal data will be kept.
- Also code here the obligation for data controllers to reveal how do they determine the data retention time.

01.06 Third-party transfer

- Include rules providing that data controllers must inform data subjects that their personal data might be shared or disclosed with third parties.
- Include rules requesting data controllers to disclose with whom they share personal data.

01.07 Third-party transfer safeguards

- Include the obligation for data controllers to inform data subjects of which safeguards are implemented by third parties with which their personal data is shared or disclosed.

01.08 Third-party collection

- Include the obligation for data controllers to inform data subjects that third parties may collect personal data on their website.
- Include rules indicating that third parties must post an enhanced notice on the website where they are collecting personal data.

01.09 Automated or passive data collection (Cookie notice)

- Include the obligation for data controllers to inform data subjects that they may be subject to passive or automated data collection techniques (e.g.: cookies).

01.10 Consequences of withholding personal information

- Include any obligations of data controllers to inform data subjects of what consequences are entailed from their decision not to disclose their personal data.

01.11 Policy change

- Include any rules providing that data controllers must notify or inform data subjects of any policy change.
- Also include rules providing that data controllers must obtain consent before applying any policy change, even though it is not clearly written. It is implicitly understood that data subjects will have to be notified to be able to provide consent.

02. Consent

- Refer to any rules pertaining to the obligation for data controllers to obtain the consent of data subjects before collecting and processing their personal data.
- Include both opt-in and opt-out approaches. Opt-in approaches are situations where the data subjects must take affirmative steps to allow data collection or processing practices. As opposed, opt-out approaches are situations where the data subjects must take affirmative steps to prevent data collection or processing practices.

02.01 Original consent

- Refer to the obligation for data controllers to obtain the consent of data subjects, either implicitly (opt-out) or expressly (opt-in), before collecting and processing their personal data.
- Include the obligation for data controllers to provide data subjects with choices with regards to the collection and use of their personal data.
- Include the obligation for data controllers to obtain consent before using personal data for secondary uses (i.e., use unrelated to the original transaction. However, exclude rules requiring to obtain consent before using for purposes other than that for which they were originally collected. See 02.02 and 04.01.
- Also code here any mentions that data controllers should respect the choices or wishes of data subjects.

02.02 Consent renewal

- Include any rules requiring data controllers to renew consent after having changed their privacy policy.
- Include any rules indicating that data controllers must treat personal data according to their original privacy policy to which data subjects have consented until they are able to renew their consent.
- Include any rules stating that data controllers can only use personal data in ways compatible with their original policy except if they obtain the data subject's consent. Also code this norm in 04.01.

02.03 Consent withdrawal

- Refer to the possibility for data subjects to withdraw their consent to the collection or use of their personal data. It can either be for implicit or explicit consent.
- Include the possibility to withdraw consent for data transfer.

02.04 Cookie consent

- Refer to the obligation for data controllers to obtain data subjects' consent or provide a choice to data subjects before storing cookies on their computer. The obligation to obtain consent before storing information on a data subject's computer, even when there is no mention of cookies should also be coded here.

- Include the obligation for data controllers to obtain data subjects' consent before automatically harvesting/collecting all URLs traversed by a particular computer.

02.05 Third-party collection and use consent

- Refer to the obligation for data controllers collecting and using personal data from third-party websites to gain consent or offer choices to data subjects.
- Do not confuse with the obligation to obtain consent before sharing personal data with third parties. Only code here the obligation for a party collecting personal data own the website of another party to still allow data subjects to make choices or give consent. This obligation is often linked with rules on Online Behavioural Advertising (OBA).

02.06 Right to refuse automated decision-making

- Refer to the obligation for data controllers to respect the choice of data subjects not to be subject to decisions solely based on automated data processing.

02.07 Right to object

- Refer to the obligation for data controllers to offer data subjects the possibility to object to the use of their personal data. This rule should not be confused with to obligation to offer choices to the data subject. Most notably, do not code here the obligation to allow data subjects to opt-out at anytime. Only code here, the obligation for data controller's to allow data subjects to object to the use of their personal data when it is not based on his consent (i.e.: legitimate interests or public interests).

03. Collection limitations

- Refer to rules requiring data controllers to minimize data collection to what is necessary for specified and legitimate purposes.
- Exclude mere indication that privacy policies must inform individuals of their data collection practices. Code as a transparency measure.
- Exclude data controllers' obligation to collect personal data that is relevant to fulfill legitimate purposes. See 06.02.

03.01 Purpose limitation

- Include the obligation for data controllers to only collect personal data that is necessary for the specified purposes.
- Include the obligation for data controllers to only collect personal data for legitimate purposes.
- Include the obligation for a data controllers to limit their collection practices to data appropriate to their business (e.g., marketing or sale).
- Include the obligation stating that data controllers should limit their collection practices to data relevant for their specified purposes.

03.02 Fair and lawful

- Include the obligation for data controllers to collect personal data in a fair and lawful way.
- Do not confuse with the obligation to *process* personal data in a fair and lawful way. This rule should be coded in 04.02, not here.

03.03 Third-party source

- Refer to the obligation for data controllers using personal data collected from third parties to verify that the latter collected the data in a legitimate way.
- Include the obligation to do due diligence when collecting personal data from third parties.

04. Use limitations

- Refer to any obligations limiting the use of personal data by data controllers.
- Exclude any limitations based on the special nature of personal data (sensitive data, children data, third-party collected data, etc.)

04.01 Original purposes

- Refer to any rules providing that data controllers should only use personal data as originally notified to data subjects.

- Include any obligations to only use personal data for one specific purpose (e.g.: marketing) or only in ways associated with a data controller's business.
- Include any rules requiring data controllers to not process personal data for new purposes, except with the consent of data subjects. Also code in 02.02.

04.02 Fair and lawful

- Refer to the obligation for data controllers to only use personal data in a fair and lawful way.
- Do not confuse with the obligation to *collect* personal data in a fair and lawful way. This rule should be coded at 03.02.

04.03 Right to restrict

- Refer to the possibility for data subjects to temporarily limit the use of their personal data by data controllers.

05. Disclosure

- Refer to any rules related to the transfer of personal data by data controllers to third parties.
- Include the obligations of data controllers regarding cross-border transfers and the sale of personal data.

05.01 Sharing with independent controller

- Refer to any obligations related with the transfer of personal data from a data controller to an unaffiliated third parties.

05.01.01 Consent

- Code here the obligation to obtain the consent of data subjects before transferring their personal data to third parties.
- Include the obligation to offer a choice to data subjects before transferring their personal data.
- Include the right of data subjects to refuse that data controllers share their personal data with third parties. This is considered to be equal to an opt-out form of consent.

05.01.02 Adequacy of third-party policies

- Refer to the obligation for data controllers to verify the adequacy of third parties before sharing with them personal data.
- Include any rules requiring data controllers to share personal data with third parties which provide substantially similar privacy protections. The obligation to otherwise inform data subjects if their personal data is transferred to third parties without sufficient privacy protections should also be coded here.
- Include the obligation for data controllers to share their privacy policies with third parties with which they are sharing personal data.
- Include the obligation for data controllers to have an agreement providing an equivalent level of protection to their privacy policy with third parties should both be coded here and in 05.01.03.

05.01.03 Contract

- Refer to the obligation for data controllers to have have an agreement or contract with any third parties with which they share personal data.
- Include any mention that a data controllers should "contractually" require that a third party receiving personal data should abide by its policies.
- Include the obligation that the contract specifies that the data controller remains responsible for the use of its collected personal data.

05.01.04 Remedial actions

- Refer to the obligation for data controllers to take remedial actions against third party which receives personal data. It is often based on a contract that the data controller should have established with the third party.

05.02 Sharing with joint controller

- Refer to any rules defining how two or more data controllers which jointly manage personal data should operate.

05.03 Sharing with processor

- Refer to any obligations of data controllers when sharing data with processors or service providers, i.e., third party companies employed to specifically analyze the data for the data controllers.

05.03.01 Use limitations

- Refer to the obligation for data controllers to ensure that processors will only process under the instruction of the data controller.
- Include any rules indicating that a processor should not hire another processor without prior authorization from the data controller. Also code here the obligation that this second processor should respect the same obligations than the first one.

05.03.02 Adequacy of processor policies

- Refer to any obligations of data controllers to ensure that processors respect the same level of protection that they offer.
- Include any rules stating that processors must respect the privacy policy of the data controller and keep personal data confidential.
- Include any mention that processors must maintain a level of security equivalent to the one of the data controller.

05.03.03 Contract

- Refer to the obligation for data controllers to have a contract or an agreement when sharing personal data with a processor or service provider.
- Importantly, if it is indicated that the contract should foresee that the processor or service provider must respect the privacy policy of the data controller or only use personal data under its instruction, also code in 05.03.01 and 05.03.02.
- Include the obligation that the contract specifies that the data controller remains responsible for the use of its collected personal data.

05.04 Third-country transfer

- Include any obligations that data controllers must specifically respect when transferring personal across borders.

05.05 Prohibition to transfer prospect information

- Refer to the obligation for data controllers not to share personal data collected indirectly, i.e., personal data on a data subject collected through another one.

06. Data quality

- Refer to rules aiming to ensure that personal data collected by data controllers is of quality.
- Include the obligation for data controllers to ensure that personal data they collect is accurate, complete and kept up-to-date.
- Include any obligation for data controllers to develop procedures to maintain the accuracy of personal data.
- Any mention that data controllers should allow data subjects to access their personal data to ensure they remain up-to-date should both be coded here and at 07.01.

07. Individual participation

- Refer to the ability of data subjects to control how their personal data is used and shared.

07.01 Acces and review

- Refer to the possibility for data subjects to access and potentially review personal data that a data controller has on them.
- Include the obligation for data controllers to ensure that data subjects are able to determine whether a data controller holds information on them. Similarly, the obligation for data controllers to confirm to data subjects if they hold personal data on them should be coded here.
- The obligation for data controllers to ensure data quality by providing data subjects with an access to their personal data should be coded here and at 06.01.
- Also code here rules providing that data subjects may correct their personal data if no rules specifically indicate that a data subject may access its personal data. It is implicitly assumed that to be able to correct its data, data subjects will be given access to its personal data.

07.02 Correct

- Include any rules providing that data subjects may correct, rectify or change the personal data that a data controller has on them.

07.03 Erasure

- Include any rules providing that data subjects may request the erasure, suppression or blocking of their personal data.
- Include any rules providing that data subjects can request that data controllers remove inaccurate data.

07.04 Notification of third parties

- Include any rules providing that the data controller should inform any data recipients of changes to the personal data of a data subject.

07.05 Access denial

- Code here any rules requesting data controllers to explain to data subjects why a request for access, correct or remove personal data has been refused.

07.06 Right to challenge

- Include any rules allowing data subjects to challenge any decision by data controllers to deny access requests.

07.07 Right to be informed of automated practices

- Include the obligation for data controllers to inform data subjects of the existence and logic behind their automated processing practices.

07.08 Authentication

- Include the obligation for data controllers to verify the identity of a data subject before giving him/her access to personal data.

07.09 Not unduly limit

- Include the obligation for data controllers to not create any unnecessary barriers for data subjects to access, correct and delete their personal data.
- Include any obligation stating that access to personal data should be free or should not cost more than a specific price.

07.10 Data portability

- Include any rules providing that data subjects may request to receive their personal data in portable format. Do not confuse this norm with the possibility to have access to its personal data. Only code here, rules specifically requesting that the personal data may be shared in a portable format (i.e., in a format, which can easily reused by another data controller).

08. Sensitive data

- Refer to any rules which specifically apply to the protection of sensitive data.
- Sensitive data include information. While the definition of sensitive data may differ, it generally includes data on racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health or data concerning a person's sexual orientation.

08.01 Consent

- Include any rules providing that data subjects must give their consent before sensitive data may be collected and/or processed by data controllers.
- Include rules that only apply to one type of sensitive data (e.g., health data or financial data).
- Also code here any indication that sensitive data require a "higher" level of choice than non-sensitive data.

08.02 Third-party transfer

- Include any rules that a data controller must request data subject's consent before sharing personal data with any third parties.
- rules indicating that a data controller should use encryption or any other security measures when sharing sensitive data should not be coded here, but in 08.03.

08.03 Special security measures

- Include any rules indicating that data controllers should adopt security measures specifically designed to protect sensitive data.

- Include rules requesting data controller to use encryption to protect sensitive data, either when storing or sharing them.
- Include rules providing that data controllers should adapt their security measures to the level of sensitivity of personal data.

09. Children data

- Refer to any rules which specifically apply to the protection of children data. The different age used to determine who is a children is not considered.

09.01 Special notification

- Include any rules providing that data controllers must provide a special notice for the collection and/or process of children data.
- Include rules indicating that data controllers should notify children when they leave their website for another one which may not use the same privacy policy.
- Include any rules requiring data controllers to provide any type of information (e.g., data source, potential use, etc.) on their data collection and processing practices relating to children data.
- rules calling for data controllers to notify data subjects of their rights and obligations should be coded here and in the other nodes applicable.
- The obligation to use "awareness tools" when dealing with children on their website should be coded here.
- Parental notifications should also be coded here.

09.02 Special collection limitations

- Include any obligations of data controllers to limit their data collection practices with regards to children.
- Include the obligation for data controllers to remind children of not posting online personal data.
- Include the obligation for data controllers to not condition a children participation in an activity online on the condition of giving his/her personal data.

- Include any rules indicating that children data may not be collected for a specific purpose.

09.03 Parental control

- Include any rules requiring data controllers to encourage parents to get involved an monitor their children's online activities.
- Include any rules pushing data controllers to encourage parents to use the adequate technology and software to protect the privacy of their children online.
- Include any rules indicating that data controllers should inform parents about ways to protect the privacy of their children online.

09.04 Parental consent

- Include the obligation for data controllers to obtain parental consent before collecting, using and/or processing children data.
- rules providing that data controllers should allow parents to refuse further use of their children data.

09.05 Parental access

- Include any rules providing that parents may access the personal data of their children.
- Include any rules allowing parents to request that their children data be corrected or removed.

09.06 Third-party transfer

- Include any rules providing that data controllers must provide specific information to parents when sharing their children data with third parties.
- Include any rules requiring parental consent before any children data may be transferred to third parties.

09.07 Automated collection practices

- Include any rules requiring specific measures when using automated practices (cookies, web beacons, etc.) to collect children data.

09.08 Special security measures

- Include any rules stating that data controllers should adopt security rules specifically designed for children data.

10. Data security

- Refer to any rules requesting data controllers to implement security measures to protect the confidentiality of personal data.

10.01 Commitment to data security

- Refer to any rules specifying that data controllers should develop an environment conducive to data security.
- Include broad statements that data controllers should take reasonable precautions, maintain a written data security policy and adopt control measures.
- Importantly, rules foreseeing that security measures must be proportional to the sensitivity of the personal data being collected or processed should be coded in 08.03.
- Include rules providing that data controllers must use specific techniques like notably encryption, firewall, safe servers or VPN to protect personal data.
- Include rules asking that data controllers take measure to protect themselves against virus or malicious codes. However, do not code here rules providing that data controllers should refrain from introducing virus or malicious codes on the computer of data subjects. This is not considered to be a data protection measure.
- Include rules requesting that personal data may not be accessible to any people. However, rules providing that personal data may only be accessed by a data controllers' employees with a legitimate business reason should be coded in 10.02.
- Include rules stating that data controllers must establish physical, electronic and administrative security measures.
- Include rules indicating that data controllers must adopt security measures of a physical nature (e.g., locks, secured rooms, etc.)

10.02 Anonymization or Pseudonymization

- Include any rules requiring that data controllers anonymize or pseudonymize the personal data that they have collected and processed.

- Exclude rules stating that "de-identified" or "anonymized" data is considered to be non-personal information. Only include rules that indicates that anonymiation or pseudonymization should be used when possible.
- Exclude rules requiring that data controllers adopt encryption or other technical measures to protect personal data.
- Exclude rules that require data controllers to destroy or *anonymize* when the personal data is no longer needed. See node 11 instead.

10.03 Access control

- Include any rules limiting access to personal data to employees who "need to know" based on their job responsibilities.
- Exclude any rules stating that data controllers must prevent unauthorized access by external people or third parties. Similarly, exclude rules stating that only authorized users can access personal data. Instead code 10.01 as broad commitments to data security.

10.04 Record-keeping

- Include any rules providing that data controllers must keep a record of their processing activities or authorized users accessing personal data.
- Include any rules requiring that data controllers should keep a record of to whom they share personal data.

10.05 Review and monitor

- Include any rules requiring data controllers to regularly review and monitor their security measures.
- Exclude the obligation for data controllers to regularly check or demonstrate their compliance with their broad privacy policy. Code instead in 13.02.

10.06 Employee training

- Include rules providing that data controllers must provide training to their employees to ensure that they respect their privacy policy.

10.07 Privacy risk assessment

- Include any rules providing that data controllers must do a privacy risk assessment *before* processing personal data.

- Exclude any mention of annual or regular risk assessment of current security practices. Code in 10.05 as a review mechanism.

10.08 Data protection officer

- Include any rules requiring data controllers to designate an individual as accountable for the implementation of its privacy policy (i.e., data protection officer).
- Any mention that responsibility and accountability must be assigned to an employee should be coded here.
- Include rules indicating that a data controller must establish a contact point for privacy enquiry.
- Include rules requesting data controllers to name a chief privacy officer or engineer.
- Include rules indicating that data controllers should assign responsibility of ensuring the respect of their privacy policy to an individual or group of individuals.

11. Data retention

- Refer to any rules indicating that data controllers must not keep personal data for longer than necessary.

12. Data breach

- Refer to any rules requesting data controllers to take actions to prevent or resolve data breaches.

12.01 Privacy breach management policy

- Include any rules providing that data controllers should adopt a specific policy or procedure to deal with potential data breaches.
- Include the obligation to set up a readiness plan.
- Exclude obligations to notify data subjects or authorities, see 12.02 & 12.03.

12.02 Data protection authorities' notification

- Include any rules requiring data controllers to inform relevant data protection authorities of data breaches.

12.03 Data subjects' notification

- Include any rules requiring data controllers to inform all data subjects affected by a data breach.

13. Accountability

- Refer to any rules aimed at ensuring that data controllers comply with their own rules and remain accountable for their data practices.
- Include all rules related to complaint mechanisms.
- Exclude vague rules indicating that data controllers need to be accountable. Only code rules requiring the existence of specific accountability mechanisms.
- rules indicating that responsibility or accountability should be attributed to an individual or group of individuals should be coded in node 10.08 as they are considered to be equivalent to name data protection officer(s).

13.01 Complaint mechanism

- Include any rules requiring data controllers to establish a complaint mechanism or join a dispute settlement program.
- Include rules requesting data controllers to inform data subjects that they can submit complaints with regards to the use of their personal data.
- Include any rules stating that data controller must establish a mechanism to appeal any decisions taken by the dispute settlement body.
- Include rules related to the possibility to have access to a remedy with the data controllers. But exclude rules indicating that data subjects retain the right to a remedy in front of national courts.
- Exclude rules stating that data controllers must allow data subjects to challenge decisions to refuse them access to their personal data. See instead 07.06.

13.02 Compliance mechanisms

- Include any rules stating clearly that the data controller must be able to demonstrate how it is accountable for his/her data practices. It may includes annual compliance review with its data policies, external audits, etc.

14. Education

- Include any obligation for data controllers to educate or teach data subjects about their data collection and data processing activities.
- Exclude rules requiring data controllers to educate its employees. See 10.05.