Internet Privacy in the European Union and the United States

Three Essays on Privacy, the Internet, Politics, Implementation, Business Power, and Surveillance in the European Union and the United States

Agustín Rossi Silvano

Thesis submitted for assessment with a view to
obtaining the degree of Doctor of Political and Social Sciences
of the European University Institute

Florence, 19 September 2016

European University Institute
Department of Political and Social Sciences

Internet Privacy in the European Union and the United States

Three Essays on Privacy, the Internet, Politics, Implementation, Business Power, and Surveillance in the European Union and the United States

Agustín Rossi Silvano

Thesis submitted for assessment with a view to
obtaining the degree of Doctor of Political and Social Sciences
of the European University Institute

Examining Board

Prof. Sven Steinmo, European University Institute (Supervisor)
Prof. Alexander Trechsel, European University Institute
Prof. Henry Farrell, George Washington University
Prof. Bastiaan Van Apeldoorn, Vrije Universiteit Amsterdam

Researcher declaration to accompany the submission of written work
Department of Political and Social Sciences - Doctoral Programme

I Agustín Rossi Silvano certify that I am the author of the work Internet Privacy in the European Union and the United States:Three Essays on Privacy, the Internet, Politics, Implementation, Business Power, and Surveillance in the European Union and the United States I have presented for examination for the Ph.D. at the European University Institute. I also certify that this is solely my own original work, other than where I have clearly indicated, in this declaration and in the thesis, that it is the work of others.

I warrant that I have obtained all the permissions required for using any material from other copyrighted publications.

I certify that this work complies with the Code of Ethics in Academic Research issued by the European University Institute (IUE 332/2/10 (CA 297).

I declare that this work consists of 62.504 words.

Signature and date:

Agustín Rossi Silvano, 4 March 2016

Table of Contents

Acknowledgements

Writing this dissertation has been an enormous pleasure and privilege. First and foremost, I am forever grateful to my supervisor and mentor, Sven Steinmo, for providing me with the intellectual and emotional support I needed to finish this project. Being accepted to the European University Institute (EUI) to work under the supervision of Sven has been a life changing experience. Thank you, European and Spanish tax payers for making the EUI possible.

I also want to thank Henry Farrell for welcoming me at the George Washington University (GWU), Bastiaan Van Apeldoorn for being willing to read my research since my Master's in Amsterdam, Alex Trechsel for being a wonderful second-reader and Head of Department, and Javier Astudillo for uncountable recommendation letters and constant encouragement. Likewise, thanks to the administration of the EUI and the SPS department for their responsiveness and patience, especially to Martina Selmi. I am also indebted to the Institute for European, Russian, and Eurasian Studies at GWU for giving me a place to work in the United States.

During the research and writing process I have enjoyed the friendship, and intellectual challenge, of more people than I can name –some, however, have been outstanding. Surviving the first years of the PhD would have been impossible without the friendship of Mireia, Andreu, Pedro, Abián, Gama, Benedita, Clodo, Agus, Fede and Quique. In DC, Chad and Alex have made me feel at home. Flying back to Barcelona allowed me keep some healthy perspective and grounding about life outside academia, and for that I owe more than I can ever repay to my unconditional friend and part-time analyst, Juanpa. Gracias!

Muchas veces durante mis años como estudiante e investigador mi mamá Mechi, mi hermana Delfina, y Rubén, creyeron en mí más de lo que yo creí en mi mismo: esto hubiese sido del todo imposible sin el aliento constante de ustedes ante cualquier adversidad. También fue muy importante contar con el cariño a la distancia de la familia en Argentina: especialmente mi papá Agustín, mi hermana Sabina y mi hermano Nacho.

Finally, the last years of writing and re-writing (and re-writing) would have been much worse without the help, support, patience, and love of Molly. Most people (outside academia) would complain about their partner spending weekends and nights struggling to find the right word to express an idea. Instead, she always asked with a smile "how can I help?". And then I knew.

Washington DC, July 17th 2016

Abstract

This dissertation is a collection of three stand-alone papers each making distinct contributions and addressing different, but closely related, empirical puzzles that contribute to the literature on Internet privacy.

The first article starts by exploring some of the tangible consequences of the Snowden revelations and challenges the common-wisdom culturalist theories of Europe's privacy regime. Then, the second article offers a new explanation of the origins of America's privacy framework that also defies conventional culturalist explanations. Finally, the third article closes by offering a novel implementation and policy design analysis of the American and European privacy regimes.

Each article employs slightly different research methods and uses different yet compatible and complementary theoretical frameworks. In general, this dissertation adopts an institutionalist perspective studying how and why certain institutions change, and "why some flourish in some context and/or why some die out in others" (Steinmo, 2003a). The first article focuses on institutional reform, and resistance to institutional reform by corporate actors, following Culpepper's quiet politics framework (2011). The second article, borrowing from Steinmo (2003b) and Blyth (2002, 2011), discusses the interaction between ideas and institutions, following perhaps the clearest institutionalist narrative of all the pieces of this dissertation. The third article, building on Rothstein's general theory on implementation (Rothstein, 1998) discusses the implementation and policy design of the European and American institutions for the protection of privacy

List of Abbreviations and Acronyms

1995 Directive	1995 Data Protection Directive
ALDE	Alliance of Liberals and Democrats of Europe
AmCham	American Chamber of Commerce
BND	*Bundesnachrichtendienst*, German intelligence agency
CAB	Civil Aeronautics Board
CEO	Chief Executive Officer
CIA	Central Intelligence Agency
CNCIS	*Commission nationale de contrôle des interceptions de sécurité*
CNIL	*Commission nationale de l'informatique et des libertés* (French DPA)
COPPA	Child Online Privacy Protection Act
DC	District of Columbia, Washington
EC	European Commission
ECON	Economic and Monetary Affairs Committee (EP)
EDRi	European Digital Rights (NGO)
EIF	European Internet Foundation
EMPL	Employment and Social Affairs Committee (EP)
EP	European Parliament
EPA	Environmental Protection Agency
EPP	European People's Party
EU	European Union
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FISA	Foreign Intelligence Service Act
FISC	Foreign Intelligence Service Court
FoP	Future of Privacy Forum
FRA	European Union Agency for Fundamental Rights
FTC	Federal Trade Commission
G-10	Committee on Surveillance

GCHQ	Government Communications Headquarters
GDPR	General Data Protection Regulation
IAB	Interactive Advertising Bureau
IAPP	International Association of Privacy Professionals
IMCO	Internal Market and Consumer Protection Committee (EP)
IPT	Investigatory Powers Tribunal
ISC	Intelligence and Security Committee
ISP	Internet Service Provider
ITRE	Industry, Research and Energy Committee (EP)
JURI	Legal Affairs Committee (EP)
LIBE	Civil Liberties, Justice, and Home Affairs Committee (EP)
LQDN	La Quadrature du Net, NGO
MEP	Member of the European Parliament
MoU	Memorandum of Understanding
MP	Member of Parliament
NPR	National Partnership for Reinventing Government
NSA	National Security Agency
NSC	National Security Council
NTIA	National Telecommunications and Information Administration
OMB	Office of Management and Budget
OSHA	Occupational Health and Safety Act
Patriot Act	Uniting and Strengthening America by Providing Appropriate Tools to Intercept and Obstruct Terrorism Act
PKGr	Parliamentary Control Panel
PPSC	Privacy Protection Study Commission
PRISM	NSA surveillance program
RIPA	Regulation of Investigatory Powers Act
TEMPORA	NSA surveillance program
UK	United Kingdom
US	United States

List of Figures and Tables

I. Introduction

Human activity generates data. Human activity connected to the Internet generates lots of data. Who gets to collect and process this personal data is one of the most debated and important political issues faced by modern societies. Europeans and Americans have settled these issues quite differently, as a growing body of political and legal literature on privacy and surveillance demonstrates. Given that personal data generated in the Internet has sparked entirely new business models and created new powerful giant corporations such as Google and Facebook (World Economic Forum & Bain & Company, Inc, 2011), and that governments have controversially determined that collecting as much information as possible on their own and foreign nationals is fundamental for national security (Greenwald, 2014) it is not surprising that political science has paid attention to privacy and the Internet.

However, there are three crucial elements of privacy protection in the EU and the US that we know little about. First, we still do not know much about the tangible effects that the 2013 global surveillance revelations made by Snowden had in the politics and the privacy policies of the EU. Europeans were outraged by the Snowden revelations that took place in the middle of the reform process of Europe's privacy framework. Did that outrage have any tangible consequence? Second, the origins of the exceptional American privacy framework remain underexplored. America is the only advanced democracy without a comprehensive privacy framework like the European. We still only have a superficial explanation of why. Third, we still do not know much about the implementation of the American and the European privacy regimes.

The politics of Internet privacy are one of the most important policy concerns of the era of the Internet and the communication society; yet we still do not know some very important things about it. The three articles of this dissertation offer explanations to these three crucial elements of privacy protection in the EU and the US.

In fact, not only we know little about these three largely unexplored crucial elements of Internet privacy, but also what we think we know is often unsuitable. For example, contrary to conventional wisdom Europeans and their representatives are not permanently and automatically alert about their privacy. When in 2012 the European

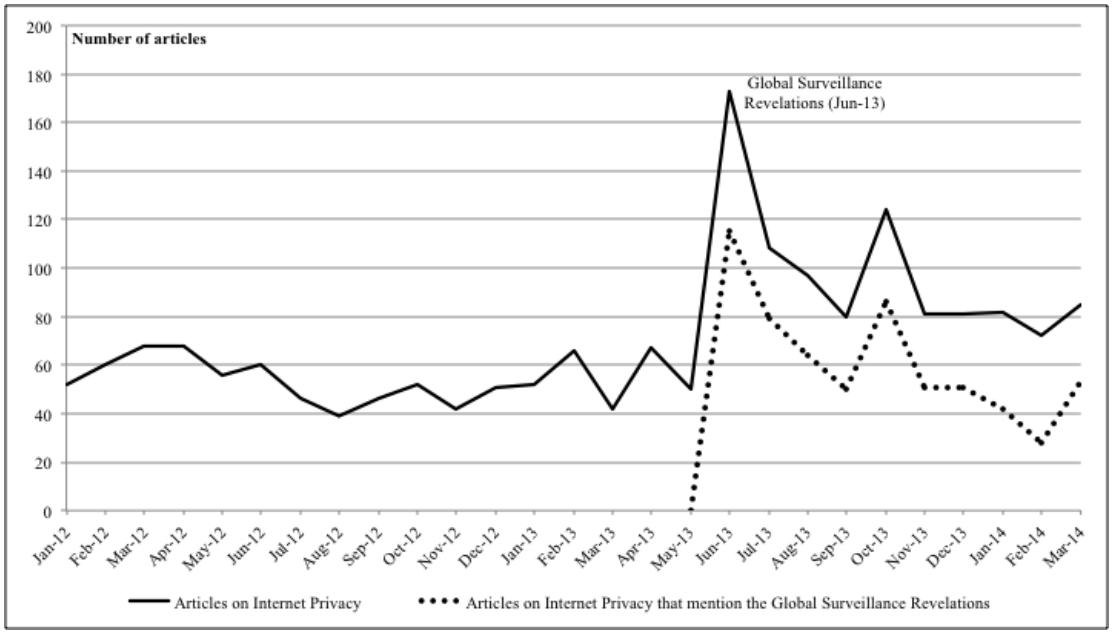
Commission (EC) presented a proposal to reform the EU's privacy framework and adapt it to the Internet it was predicted that the European Parliament (EP) would easily approve that proposal. However, until the global-surveillance revelations made by Snowden in the summer of 2013 it was very likely that in the midst of public indifference, the EP would vote against strengthening European's privacy rights, conceding to business lobbying. The first article of this dissertation argues that it were the Snowden revelations that triggered outrage in Europeans and raised the salience of Internet privacy issues across the EU what turned the parliamentary debate around and allowed privacy advocates to advance their interests against the lobbying of powerful corporations.

The second article argues that political culture alone cannot explain why the US is the only advanced democracy without a comprehensive privacy regime like the European. Instead, I explain how and why the resulting and institutionalized policy paradigms that emerged in response to the crises of 1973 (the collapse of the Bretton Woods system, that resulted in the deregulatory paradigm) and 2001 (the 9/11 terrorists attacks, that created the surveillance state paradigm) biased American politics and institutions against comprehensive privacy reform. Policy paradigms are the ideas that structure the thinking about what can and should be in done in a political system as a whole.

Finally, it is commonly assumed that Europeans, who have created remarkably complex and stringent laws and bureaucracies to protect the privacy of their citizens, enjoy more privacy protection than Americans, because they are constantly worried about their privacy. In comparison we assume that the US, where individualism and anti-statism is rampant, will allow companies to treat personal data as just any other commodity because of underlying trends in American culture. Yet, these assumptions are incomplete. The third article demonstrates that since both the EU and the US legislators have few incentives to regulate intelligence agencies and provide resources for data privacy authorities, the American and European privacy frameworks have fundamental policy design and implementation flaws. We tend to assume that laws and bureaucracies will translate into governance outcomes. However, because of implementation and design flaws, the American and European privacy regimes do not provide the expected governance effects. The third article of this explores the implementation and policy design of the American and European privacy frameworks.

In this dissertation I explore some very important aspects of the American and European privacy frameworks, and make sense of the graph exposed bellow.

Figure 1 Newspaper articles mentioning Internet privacy issues in selected EU countries. Own elaboration



The existing literature

This dissertation contributes to the field of Internet governance in general, and the subfield of Internet privacy in particular. But what is Internet governance? According to the UN Working Group on Internet Governance (WGIG) it is the "norms, rules, decision-making procedures, and programs that shape the evolution and use of the Internet" developed and applied by governments, companies and civil society (WGIG, 2005, p. 4). Perhaps because of the novelty of the term, Mueller and Eeten have identified that the literature on Internet governance has been divided in two categories in a way that makes it difficult to identify the boundaries of the field (2013). On the one hand there is a specific subset of literature that deals with some specific international organizations that are easily identifiable as being part of Internet governance such as that the Internet Governance Forum (IGF) or the Internet Corporation for Assigned Names and Numbers (ICANN). Thus, for example, in *Ruling the root* Mueller explains the history and power-struggles for the control of ICANN (2002), and in *Protocol Politics* DeNardis explores the discussions

about the new Internet Protocol IPV6, deeply related to the governance of the Internet (DeNardis, 2009). On the other hand, there is large group of research on telecommunications policy, cybersecurity, privacy, or surveillance, that does not always self-identify with the Internet governance field despite dealing with issues that directly affect the governance of the Internet. This dissertation falls in the second category, dealing with a fundamental aspect of the steering of the governance of the Internet, the regulation of the collection and processing of personal data in the EU and the US that takes place beyond the easily identifiable institutions that provide the governance of the Internet.

Political science understanding of how the Internet affects policy arenas and issues has come a long way since 2004, when Daniel Drezner called to bring the state back into the analysis of Internet governance, and eventually to the analysis of Internet privacy (2004). A popular and widespread argument about the Internet until the beginning of the 2000s was that the Internet knew no borders and as such escaped the regulatory arm of the state. As late as 1996 *A declaration of Independence of Cyberspace* famously and influentially told governments: "You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear" (Barlow, 1996). Nicholas Negroponte, founder of MIT's Media Lab, wrote in 1996 that "national law has no place in cyberlaw" (Negroponte, 1996, p. 237). And Kevin Kelly, former editor of *Wired*, wrote in 1995 "no one controls the Net. No one is in charge. […] The Internet is, as its users are proud to boast, the largest functioning anarchy in the world" (1995, p. 464). Cairncross argued that because of the Internet the nation state would have to reinvent itself, since "governments' jurisdictions are geographic, but the Internet transcends geography", and even the power to impose taxation will be challenged (Cairncross, 2001, p. 159). Similarly, Spar argued that "International organizations lack the power to police cyberspace; national governments lack the authority; and the slow pace of interstate agreement is no match for the rapid-fire of technological change" (Spar, 1999, p. 47).

During the first decades of the Internet, the conventional wisdom was that the Internet was an independent sphere where governments had no power, and a new horizontal and democratic society made the rules.

Since then, academic literature has successfully established that states can, and in fact do, regulate and impose their laws on the Internet inside their borders: Nazi

paraphernalia is forbidden and filtered by Internet companies in Germany, (Goldsmith & Wu, 2006) websites that offer links to download, watch or listen to copyrighted content without permission by the owners of the rights in a specific country are often persecuted by national authorities in Europe and the United States (Mueller et al., 2012).

Consequently, political science literature has long studied the EU and the US privacy regimes. The predominant focus of political science research on privacy has been on the variation of the privacy regimes across time (i.a. Colin J. Bennett, Haggerty, Lyon, & Steeves, 2014; A. Newman, 2008, 2011c) and jurisdictions (i.a. Colin J. Bennett, 1992; Colin John Bennett, 2008; H. Farrell, 2002a; A. Newman, 2008). As a consequence, we know that the institutional frameworks created by the EU and the US to protect the privacy of their citizen's look very different and are intended to work in different ways. We also know how these two regimes interact and institutionally shape each other. We know little, however, about the implementation and effective governance effects of the EU and US privacy frameworks. In response, article 3 offers an implementation analysis of the American and European privacy frameworks.

If until the 1970s scholars and the OECD noted an increasing convergence in how advanced nations regulated privacy protection (Colin J. Bennett, 1992; Hondius, 1975; OECD, 1975), the 1990s marked a point of divergence. With the approval of the 1995 Directive the EU has become the central actor in the global privacy debate (i.a. Colin J. Bennett & Raab, 2006; A. Newman, 2008; Swire & Litan, 1998), establishing what some have considered the "de facto international privacy standard" (Bach & Newman, 2007, p. 836; see also Schwartz, 2013, p. 1968). In fact, as the *Wall Street Journal* noted in 2003, EU privacy rules "are increasingly shaping the way businesses operate around the globe" (Scheer, 2003).

There are two predominant accounts on the origins of the European privacy framework, one cultural and the other institutionalist. The cultural account briefly states that Europeans learned the importance of defending their privacy as a consequence of the fascist experiences of the 20th century (i.a. Greenleaf, 2014; Kilian, 2008; Lindsay, 2005; Mullerat, 2007; Rotenberg & Jacobs, 2013; Ruyver, Vermeulen, & Beken, 2002). A second variant of the cultural account is offered by Whitman (2004), who argues that

Europeans view privacy as a matter of dignity, and that this is rooted in ancient notions of honor and personality in French and German law.

However, cultural explanations cannot account for variation in privacy approaches in the European Union before the 1995 Directive since they pair origins and intention. For example, the United Kingdom (UK) had privacy laws similar to those of Germany without having experienced a fascist government, while Spain only introduced a privacy framework because of the 1995 Directive. Given the limitations of the culturalist explanations, Newman offers a historical institutional account of Europe's privacy framework (2008). In *Protectors of Privacy* (2008), Newman studies the origins of the 1995 Directive arguing that the Data Protection Agencies (DPAs) established in the 1970s in some European countries, lobbied the European institutions and threatened to block data flows between EU companies and governments to achieve a common European privacy framework. By holding the European integration process hostage, DPAs managed to see their preferences reflected in form of the Directive against intensive lobbying by corporate and state actors (H. Farrell, 2002a; A. Newman, 2008). However, because since the adoption of the 1995 Directive DPAs cannot threaten with blocking intra-EU data flows, we only have culturalist notions to explain why the EP adopted the privacy strengthening GDPR against corporate lobbying. The first article of this dissertation offers a power centric explanation of why the EP adopted a privacy strengthening GDPR.

In comparison with the EU's, the origins of the limited US privacy framework have received less attention, despite the surprising fact that America is the only advanced nation without a comprehensive privacy regime (Greenleaf, 2014). Literature explains this case of "American Exceptionalism" using the Liberal Traditions explanation originally suggested by Alexis De Tocqueville (2004): Since Americans are more individualistic than other nations, resistant to accept state intervention in their society, and reluctant to accept government intervention in the market, comprehensive privacy reform becomes impossible in the US (i.a. Drezner, 2004; Strauss & Rogerson, 2002; Swire & Litan, 1998). Regan, for example, explains that "the formulation of privacy policy in the United States has been profoundly shaped by its liberal traditions emphasizing individual rights and a limited role for government" (Regan, 2008, p. 74). The second article of this dissertation argues that America does not have a comprehensive privacy regime not because of American culture, but because the policy-paradigms that have determine which

policies are possible and desirable since the 1970s have been biased against comprehensive privacy reform.

Presenting Internet privacy puzzles

Therefore, this dissertation intends to solve three puzzles: Why was the EP opposed to strengthening Europe's privacy rights before the Snowden revelations? Why does America not have a comprehensive privacy regime like all other advanced nations? Why did the privacy governance efforts of the EU and the US not provide the expected results? These puzzles are intriguing because the answers we expect notably diverge from reality. We expect Europeans and the EP to be constantly alert about privacy. We assume that America does not have a comprehensive privacy regime because Americans are individualistic and anti-statist. We think that Americans and Europeans effectively enjoy of privacy protection because the governance arrangements created by their states. Part of the reason why the answers to these puzzles diverge from the answers we expect is that we have a rather mechanistic and simplistic way of understanding privacy protection in Europe and America. If privacy frameworks would simply reflect common understandings of past experiences of societies, then we could expect Europeans to treasure the right that is cornerstone to everything once taken from them –freedom of religion, expression, organizing, etc.-, and Americans to be less vigilant since they did not experience fascism. Privacy frameworks, however, are about much more than simple declarations of respect for common history.

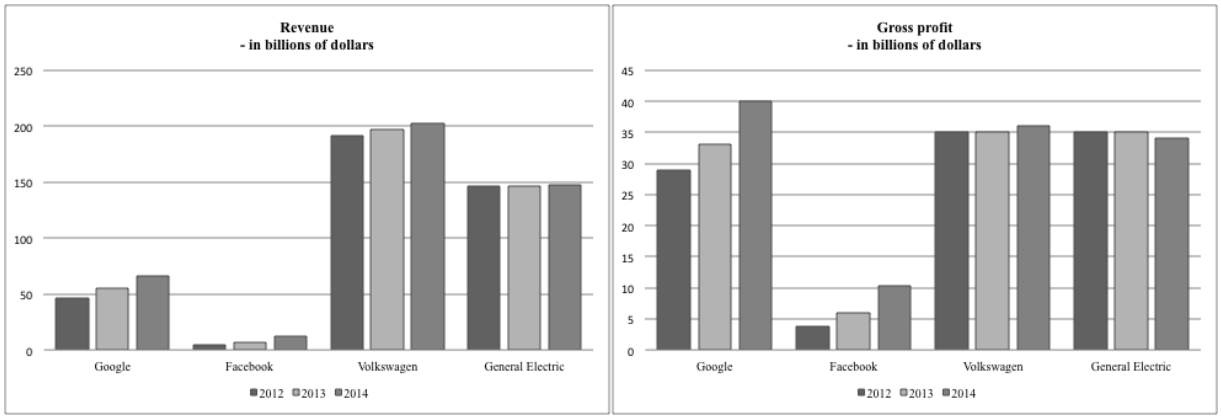
Privacy frameworks aim to strike a balance between the protection of a right, the enabling of markets, and national security. Fundamentally, *all* privacy frameworks try to regulate the collection, processing, and transfer of personal data for trade and government related issues. Indeed, in today's world and economy, privacy frameworks make or break fortunes and also facilitate or difficult massive state-surveillance. It is important to understand that privacy policies serve multiple functions and that therefore they are subject to political and economic tensions. Only by understanding this we can start to answer the questions, why was the EP opposed to strengthening Europe's privacy rights before the Snowden revelations? Why does America not have a comprehensive privacy

regime like all other advanced nations? Why did the privacy governance efforts of the EU and the US not provide the expected results?

The cost of free services

Internet companies are increasingly powerful and rich political actors yet the most important Internet services are free of monetary charge. In the year 2000 the average e-mail inbox could store just 10 megabytes of information (the equivalent to three average size mp3 compressed songs) and the service was usually linked to a particular Internet service provider. Today Google offers virtually unlimited e-mail storage with a friendly user interface without ever asking to see its users' credit card number. Similarly, Facebook enables people to connect, chat, and videochat with old-friends and family without ever subjecting them to the discomfort of having to deal with a check for what they have used. Yet, Internet giants report growing revenue and profits, as Figure 2 shows. How?

Figure 2 Revenue and gross profit of selected Internet and traditional companies. Own elaboration. Source: Google Finance



The personal data by and about people created by human interaction with Internet services generated a new wave of opportunity exploited by Internet companies. The personal data being collected varies in type, quantity, value: its our web searches and sites visited, our social network activity, our tweets, the content of our emails, our location, the photos and videos we share with our close –and not so close- friends, our phone calls. And the list grows constantly. Companies collect and use this personal data to target behavioral and user specific advertisement: the more data they collect, the more accurate and valuable their ads services. The uncomfortable truth is that the business model of the

Internet is based around the collection and processing of personal information for the targeting of behavioral advertisement. At the end of the day Facebook, Google, Twitter, and Yahoo are nothing else but glorified, tech-savvy, advertising companies –that is what sustains their bottom line. Certainly, end users benefit from free of charge personalized consumer experiences such as unlimited email and social networks. Yet, as economists like to say, there is no such thing as a free lunch.

If it was once true that in the Internet no-one knows if you are a dog, as a *The New Yorker* vignette famously quipped (Steiner, 1993), now we have come to the realization that every step of our ever bigger digital footprint is potentially being recorded, stored, analyzed and trade as commodity (World Economic Forum & Bain & Company, Inc, 2011). And this realization does not always come in good terms. For example, Europeans fought for their right to be forgotten, resisting to the idea that once something makes it to the Internet is never going away (ECJ, 2014). And Internet companies tried to resist this change fiercely lobbying Brussels.

Thus, one of the functions of privacy frameworks is to regulate the conditions in which companies are allowed to collect, process and transfer personal information. For politicians, this means that when they face the regulation of privacy they are often touching directly the interests of corporations that sometimes have more money available for influencing politics than traditional corporate giants, as General Electric and Volkswagen. Politicians and regulators must then deal with the companies with clear material incentives to shape the laws and bureaucracies that determine the privacy frameworks and exploit their limitations to maximize their business.

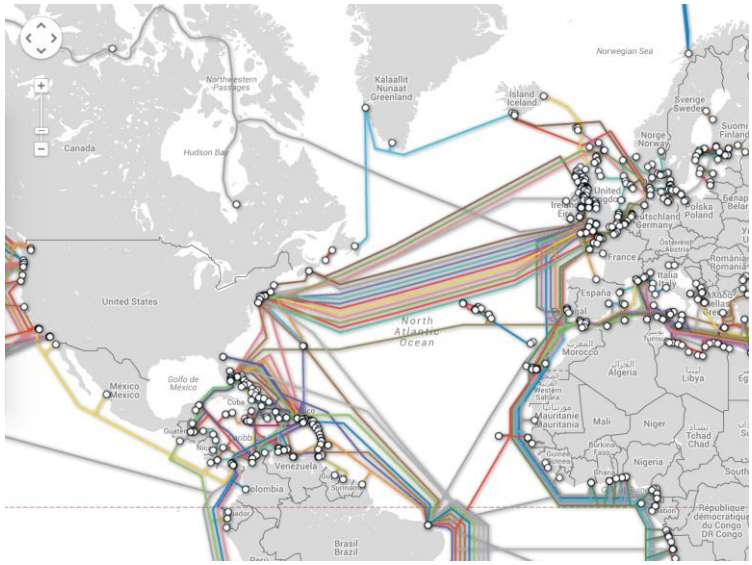
The first article of this dissertation by publications is about the political power of corporations, how they lobbied against strengthening Europe's privacy rules, and how they would have won if Snowden had not disrupted the political debate. Would not have been for the outrage generated by the Snowden revelations, the EP would have opted for watering down European's privacy rights. The second article explains why American companies have not been the target of a comprehensive privacy reform –and perhaps surprises the reader arguing that it was not because American culture. Finally, the third article describes how underfunded regulators struggle to enforce the American and European privacy regimes.

Privacy and state-surveillance

In the second half of the 20th Century, the recently emerged Welfare States embraced another byproduct of World War II, the computer. Governments quickly adopted computers for their day-to-day operations, and eventually decided to create national data banks linking the information dispersed in different individual data banks to enhance efficiency and oversight of public and private services. In 1965 the US Social Science Research Council proposed to create one of the first data banks, to link the data collected by various government agencies to centralize the access to that information, and one year later the Bureau of the Budget followed the lead and established the National Data Center to centralize twenty data banks of other agencies (Flaherty, 1979; Regan, 1995). And in Europe, for example, in 1971 France secretly created the SAFARI project (*Système automatique pour les fichiers administratifs et le repertoire des individus*) with the aim of constructing a directory of individuals with the connection of individual files (Martin, 1995, p. 503).

In general, the public reacted with suspicion to the emergence of the powerful super-informed government. But it was not until the eruption of scandals related to the new surveillance powers of the state that privacy entered the policy-agenda and politicians started to seriously debate the creation safeguards to massive personal data collection and processing. The 1972 Watergate scandal, that obliged President Nixon to resign for being suspected of ordering to spy on the opposition Democratic party with the help of the intelligence agencies (Lewis, 1972), eventually lead to regulation to protect the privacy of Americans and attempt to control the intelligence agencies, principally in the 1974 Privacy Act. In Europe, between 1972 and 1974 the French media reported on the secret existence of the SAFARI project, an attempt to centralize the information of the French perceived as an intrusion of people's privacy heir of the Vichy's regime (Mattelart, 2010, p. 121). The debate generated by SAFARI culminated in the enactment of a privacy law the *Loi Informatique et Libertés*, passed in 1978 as a precursor to the EU's 1995 Directive (Mattelart, 2010, p. 122; A. Newman, 2008, p. 46). Given the interconnectivity of the Internet, the regulation of intelligence agencies is fundamental for the protection of privacy.

Figure 3 Submarine Internet cables. Source: Telegeography.com



As the map presented above shows, the submarine Internet cables that move the Internet information travel across many jurisdictions. The map serves to highlight the interconnectivity of the Internet and the importance of understanding the relevance of some jurisdictions to guarantee the effectiveness of any kind of Internet privacy regulation. In other words, it is a good reminder that given that the most important Internet companies are located in the US, and that the US authorities have not only jurisdiction over these companies but also physical access to the cables that move the Internet's information, how America deals with Americans and Europeans' personal data is as important as any EU regulation for European's privacy. Likewise, the reader should keep in mind that most of the Information that leaves the European continent towards the Atlantic does it through the UK, increasing the relevance of the British intelligence agencies. How to regulate what intelligence agencies can do with personal data is important in any jurisdiction, but how some key jurisdictions regulate their services is crucial for all regulations.

Article 1 explains how the revelations of state-surveillance made by Edward Snowden outraged Europeans and allowed privacy advocates to defeat Internet companies, since the Snowden revelations perceived as accomplices of intelligence agencies by the general public. Article 2 illustrates the effects of Watergate and the obsession for national security product of 9-11 in the American privacy protection regime. Finally, article 3 carefully studies the implications for Europeans and Americans privacy of the lack of

control and oversight of intelligence agencies consequence of legislator's lack of will to regulate them.

This dissertation

The three presented papers of this dissertation are stand-alone, distinct contributions each addressing different, but closely related, empirical puzzles that contribute to the literature on Internet privacy. The first article starts by exploring some of the tangible consequences of the Snowden revelations and challenges the common-wisdom culturalist theories of Europe's privacy regime. Then, the second article offers a new explanation of the origins of America's privacy framework that also defies conventional culturalist explanations. Finally, the third article closes by offering a novel implementation and policy design analysis of the American and European privacy regimes.

Each article employs slightly different research methods and uses different yet compatible and complementary theoretical frameworks. In general, this dissertation adopts an institutionalist perspective studying how and why certain institutions change, and "why some flourish in some context and/or why some die out in others" (Steinmo, 2003a). The first article focuses on institutional reform, and resistance to institutional reform by corporate actors, following Culpepper's quiet politics framework (2011). The second article, borrowing from Steinmo (2003b) and Blyth (2002, 2011), discusses the interaction between ideas and institutions, following perhaps the clearest institutionalist narrative of all the pieces of this dissertation. The third article, building on Rothstein's general theory on implementation (Rothstein, 1998) discusses the implementation and policy design of the European and American institutions for the protection of privacy. In sum, this dissertation analyzes three Internet privacy empirical puzzles from an institutionalist perspective, highlighting the crucial role of institutions structuring policy debates. Institutions, even for the regulation of something that seems as intangible as the Internet, matter. Institutions structure politics because they determine who is able to participate in a particular policy arena, shape actor's strategies, and influence what these actors believe to be possible and desirable (Steinmo, 2003a). But institutions are not the only thing that matters. For this reason, the articles of this dissertation also study the importance of power, political salience, of ideas and of the implementation and design of institutions.

Article 1 (II Chapter): The Snowden effect. How the Global Surveillance Revelations strengthened the Data Protection Regulation in the European Parliament

Article 1 is an analysis about power, power expressed power and quiet power. It details the politics around the GDPR and shows how it was not European's privacy culture what determines the adoption of a privacy-strengthening piece of legislation by the EP. Instead, this article argues that the adoption of a privacy strengthening GDPR is an expression of the outrage that Snowden's revelations evoked in the European public, reflected by the MEPs, which diminished corporate lobbying power. This article is a demonstration of Culpepper's "Quiet Power" thesis (2011), that briefly argues that corporate power grows in low salience debates, but adds to the insights an understanding of what happens when the light is shining. Secondly, this article contributes to understanding the weakness of culturist theories in general. Too often people assume that Europeans are distinctive in their concern about privacy because of underlying cultural variables result of the European fascist experiences of the 20th century. Showing the weakness of culturalist theorizing I argue that privacy-advocates used the change in the salience of the GDPR debate produced by the Snowden revelations to push their preferences forward. This article also shows that the revelations of cooperation between Silicon Valley companies and the NSA transformed the support of the US Government to the preferences of corporations into a liability in the eyes of European policy-makers.

Using a historical narrative that centers in issue salience and building on Culpepper's "Quiet Politics" theory (2011), in this paper I show that the documents revealed by Snowden outraged Europeans, raised the salience of Internet privacy issues including the GDPR, and allowed privacy-advocates to revert the EP's opposition to privacy strengthening rules.

Quantitatively, this article analyses the salience of Internet privacy issues and the incidence of Snowden revelations in the GDPR debate. To measure salience I use two printed-editions of the main newspapers available on *Lexis-Nexis* of the big five European Union countries -Germany, France, the UK, Spain and Italy– that together account for more than 60% of the EU's population. Methodologically, I first search for the news and opinion pieces on Internet privacy or the GPDR from the 1st of January 2012 (when the

GDPR was presented by the Commission), to the end of March of 2014 (when the EP Plenary voted its position). Within those results I look for hose mentioning the global surveillance revelations to add detail to the understanding of their effect in the salience of Internet privacy issues at large. I show how Snowden's global surveillance revelations tripled the salience of Internet privacy issues and allowed pro-privacy advocates to push for privacy-strengthening rules in Committee in November 2013 and in Plenary in March 2014, against the desires of corporations.

This article also offers a discussion of literature on business power and lobbying and details the parliamentary process of the GDPR in the EP by comparing the positions of corporations, the EU privacy regulators, and the amendments and opinions adopted by the parliamentary committees that dealt with the Regulation. It is detailed how the corporate lobbying campaign was run by public affairs experts and experienced politicians and public servants hired by corporations aware that Brussels is an insiders' town when it comes to lobbying.

Article 2 (III Chapter) American Exceptionalism – Why does America not have a comprehensive privacy regime?

Out of 89 nations with some kind of privacy law, the United States and Thailand are the only countries with laws that do not cover the private sector (Greenleaf, 2012). Instead America has what has been often called a patchwork of protections (i.a. Colin J. Bennett, 1992; Flaherty, 1992; A. Newman, 2008; Regan, 1995). As a consequence of the lack of a comprehensive regime, and according to a 2010 green paper of the United States' Department of Commerce on privacy and the Internet economy, Silicon Valley corporations "operate without specific statutory obligations to protect personal data" (2010b).

But why does America not have a comprehensive privacy regime? The most common, obvious, and prevalent explanation is that of the liberal traditions theory: comprehensive privacy legislation is against America's political culture, since Americans are more individualistic than other nations, resistant to accept state intervention in their society, and unwilling to let the government intervene in the private market.

Instead I demonstrate that the prevalent liberal traditions explanation is oversimplified and wrong since it fails to explain that polls show that Americans support an increasing role of the government for the protection of privacy from private sector invasions, and the surveillance state that emerged after the 2001 terrorist attacks.

I use an institutional approach that considers ideas and institutions as interdependent variables to explain that the interpretation of two critical conjunctures in recent American history shaped institutions and policies in a way that took comprehensive privacy reform as a casualty. First, the collapse of the Bretton Woods system, effective in 1973, marked the beginning of a deregulatory wave in American politics that makes the enactment of regulation and regulatory institutions like the ones required by a comprehensive privacy regime less likely. Due to external shocks, by the end of the 90s some American institutions, namely the Federal Trade Commission, had started drifting away from their original purpose and advocating for comprehensive privacy regime within the existing policy paradigm. However, in response to the 9-11 attacks, the American political system values security over civil rights such as privacy, rendering then the enactment of a comprehensive privacy regime impossible once again.

This article argues that reading the evolution of the American privacy framework in a vacuum prohibits understanding the nature of the policy debate. As Steinmo points out, policy makers thinking "is fundamentally framed within the economic/intellectual climate in which they work" (Steinmo, 2003b, p. 227). The predominant cultural explanation of America's privacy regime is appealing and plausible at first glance, yet oversimplifies history and policy debates bringing the reader to wrong or insufficient conclusions. A reading that pays attention to the evolution of the American policy paradigm through ideas, interest, and institutions, on the other side, offers a more nuanced and complex interpretation of history that explains why America does not have a comprehensive privacy regime.

Article 3 (IV Chapter): Willing to govern? Privacy protection in Europe and the United States

The third Article is an article about what happens when politicians govern by enacting laws and building bureaucracies theoretically aimed to solve a problem, but without the will to effectively exercise steering in a certain policy area. It provides an answer to the following question: Why did the privacy governance efforts of the EU and the US not provide the expected results? Regarding data protection literature, this article contributes to filling the gap that exists in the study of the outcomes produced by the different privacy regimes and the study of variation of the protection of individual's privacy across jurisdictions (Colin J. Bennett & Raab, 2006) and to bridging the gap between the literature on surveillance and the literature on privacy - that talk to each other less than would be expected (on this, see Colin J. Bennett, 2011a, 2011b). In more abstract terms this article illustrates how vague legislative statutes and policy guidelines and a lack of legislative oversight generates mission drift in agencies (i.a. Halperin, Clapp, & Kanter, 1974; Lipsky, 1983; Pressman & Wildavsky, 1984).

Building up on implementation literature (i.a. Hogwood & Gunn, 1984; Mazmanian & Sabatier, 1983; Pressman & Wildavsky, 1984) but fundamentally on Rothstein's critique and proposal for a general theory on implementation that enables researchers to explore policy design and execution (1998) I argue that the American and the European privacy regimes did not provide the expected results because policy makers are unwilling to control intelligence agencies or to provide the necessary resources to the implementing data protection authorities. As a consequence, the American and the European privacy governance schemes have been poorly designed and implemented. If policy-makers are unwilling to exercise effective governance in a certain policy area, the resulting governance arrangements will fail to provide the expected results for being poorly designed and executed. While political scientist and privacy expert Colin Bennett has already briefly argued that "privacy protection is flawed" because "laws are often weakened by broad exemptions, especially for law enforcement [and] the regulators have few resources" (Colin J. Bennett, 2011, p. 493), this article offers a more detailed analysis of the origins of the flaws in privacy protection.

Summary and Conclusions

The introduction of this dissertation provides a context for the papers presented. One of the main findings of this dissertation is that culturalist explanations of the origins of the American and the European privacy regimes are insufficient. Regarding studies of privacy in the EU this finding is consistent with the research of Newman and Farrell among others (i.a. H. Farrell, 2002b; A. Newman, 2008). In contrast, regarding studies of privacy in the US the findings of this dissertation constitute a novel argument that it is not culture what explains why America does not have a privacy regime like the one of the rest of the advanced democracies.

A second finding of this dissertation is that the Snowden revelations had a tangible and clear effect in European political debate because they outraged Europeans and enabled privacy advocates defeating organized corporate interests and strengthening the EU's privacy framework. More specifically, the Snowden revelations raised the salience of Internet privacy issues in the EU and weakened the lobbying position of Internet companies against the GDPR since public opinion started perceiving them as accomplices of the American surveillance-state.

A third finding of this dissertation is that American and European legislators unwillingness to address state-surveillance and provide with resources to the data protection implementing agencies has resulted in two privacy frameworks that did not achieve their governance effects. A careful study of the design and the implementation of the American and the European privacy frameworks explain why, as revealed by Snowden, Americans and Europeans have no expectation of privacy.

Following, the three articles are presented. A conclusion closes this dissertation.

II. Article 1: The Snowden effect. How the Global Surveillance Revelations strengthened the Data Protection Regulation in the European Parliament

In the first half of 2013 privacy advocates in Europe were rightfully worried about the state of negotiations for a General Data Protection Regulation (GDPR) in the European Parliament – proposed in 2012 to adapt the European privacy rules contained in the 1995 Data Protection Directive to the Internet era. In the midst of public indifference, the Internet companies heavily and successfully lobbied the Members of the European Parliaments against the proposed GDPR.

The cultural accounts of European privacy leadership cannot explain why the European Parliament was failing to ratify European privacy leadership until June 2013, when Edward Snowden started leaking documents that revealed a massive global surveillance scheme coordinated by the American National Security Agency. Cultural accounts assume that Europeans are, at least since World War II, intrinsically concerned about their privacy.

Instead, I explain that the global surveillance revelations raised the salience of Internet privacy debates in the European Union, which allowed key privacy advocates defeating the interests of Silicon Valley companies in the European Parliament. When the salience of Internet privacy issues went up, the power of corporations went down, and privacy advocates saw their preferences reflected in the GDPR.

Introduction

It is commonly assumed that Europeans care all the time about their privacy, and that the European Parliament (EP) is a relentless privacy advocate (i.a. Beignier, 1992; Greenleaf, 2012; Lindsay, 2005b; Mullerat, 2007). After all, it is only logical that Europeans would treasure their privacy after the traumatic experiences they lived at hands of autocratic and totalitarian regimes during most of the 20th century. Once free from the abuses committed by dictatorships of the left and the right, Europeans pledged not to repeat the past and be vigilant to guarantee that they will never again be stripped of their basic rights by any government. Privacy, the right that enables people to think differently, organize to defend their dignity and ideas, profess their own beliefs, practice their own religion, and choose how to live their lives is so fundamental for Europeans because it is the cornerstone sustaining everything that once was taken from them. As the popular adage goes, one does not know what one has until it is gone. And if one gets it back, one carefully and automatically treasures it. Lindsay perfectly summarizes this reasoning: "The European experience of mid-20th century totalitarianism resulted in a deep suspicion of any attempts by centralised authorities to increase their capacity for surveillance of individuals […] European data protection law is part of the broader European project of building institutions and practices, including the EU itself, which are intended to ensure that the horrors of European totalitarianism are not revisited" (Lindsay, 2005b, pp. 157–158).

Therefore, when at the beginning of 2012 the European Commission (EC) proposed a General Data Protection Regulation (GDPR) as the central piece of legislation of a package of reforms aimed to "strengthen online privacy rights and boost Europe's digital economy" (EU Commission, 2012, p. 1) everyone expected it to pass the legislative process without complications. After all, the GDPR, intended to replace the 1995 Data Protection Directive (hereon the 1995 Directive), aimed to update Europe's privacy rules to meet the needs of the Internet era—an era when personal data has become nothing else but a new asset class, as explained by the World Economic Forum (2011). And in fact, the GDPR that eventually left the European Parliament (EP) in 2014 after many amendments did promise to strengthen European's privacy rights. Unsurprisingly, the privacy-wary EP had ratified privacy leadership in the name of privacy-wary Europeans.

However, unknown to many and hidden in primitist cultural accounts of European privacy leadership, during the process of the GDPR debate and until the summer of 2013, the EP seemed determined to water-down the GDPR below the levels of protection of the 1995 Directive. In the midst of public indifference, Internet companies heavily lobbied the Members of the European Parliament (MEPs) the European Commission (EC), and European national executives against the reform proposal, as they had done previously and unsuccessfully against the 1995 Directive (Regan, 2008; see also A. Newman, 2008). EU Commissioner for Justice and original proponent of the legislation, Vivienne Reding, declared that she "[had] not seen such a heavy lobbying operation" (Warman, 2012)[1], MEPs were using amendments written directly by corporations (Doctorow, 2013) as proved by LobbyPlag.eu, a website that matches corporate lobbyists and legislator's amendments, according to one EU diplomat EU officials "received briefing materials from the US government" (Guarascio, 2012); and Google alone had more people lobbying the European Commission than the Commission had people working on the new laws (Senior Official EC Justice, 2013).

But then, why did the behavior of the EP change in time? Why despite the odds, did Silicon Valley lose and the GDPR passed by the EP in first reading reflected the preferences of privacy advocates? Using a historical narrative that centers in issue salience and building up on Culpepper's "Quiet Politics" theory (2011), in this paper I show that the documents revealed by the former contractor of the US National Security Agency (NSA) Edward Snowden in the summer of 2013 (Glenn Greenwald, 2014; Poitras, 2015) outraged Europeans, raised the salience of Internet privacy issues including the GDPR, and allowed privacy-advocates to revert the EP's opposition to privacy strengthening rules.

This article is then an analysis about power, power expressed and quiet power. It details the politics around the GDPR and shows how it was not the cultural biases of the Europeans that determined the outcomes, but instead the expression of outrage that Snowden's revelations evoked. This story is a demonstration of Culpepper's "Quiet

[1] While the lobbying against the GDPR was certainly strong, it was not the first time that the EP faced strong lobbying. For example, Regan explains how the 1995 Directive was also heavily lobbied (1999), and Wonka details the corporate operations against the Registration Evaluation Authorization of Chemicals (REACH) policy (2008). Nevertheless, even if an hyperbole Reding's statement still reveals that corporations were heavily trying to influence the GDPR.

Power" thesis (2011), that briefly argues that corporate power grows in low salience debates, but adds to the insights an understanding of what happens when the light is shining. Secondly, this article contributes to understanding the weakness of culturist theories in general. Too often people assume that Europeans are distinctive in their concern about privacy (and conversely Americans are also distinctive) because of underlying cultural variables. Showing the weakness of this kind of theorizing I argue that privacy-advocates used the change in the salience of the GDPR debate produced by the Snowden revelations to push their preferences forward. This article also shows that the revelations of cooperation between Silicon Valley companies and the NSA transformed the support of the US Government to the preferences of corporations into a liability in the eyes of European policy-makers.

As expanded below, measured by the number of articles and opinion pieces mentioned in the main newspapers of the five biggest EU countries[2], Snowden's global surveillance revelations tripled the salience of Internet privacy issues in Europe and allowed pro-privacy advocates to push for privacy-strengthening rules in Committee in November 2013 and in Plenary in March 2014, against the desires of corporations. The EP's first reading is fundamental in the EU law-making process since it sets the EP's bargaining position vis-à-vis the Council. The EP can only introduce substantive amendments to law proposals in first reading, since in second reading—when the text comes back from the Council, if the Council did not adopt the EP's first reading—the EP has only three months to deliberate and can only present amendments that serve to restore wholly or partly its first reading position, to reach a compromise with the Council, or to take into account a new facts or legal standings.

To prove my arguments, methodologically I use systemic process tracing in which "the point is to see if the multiple actions and statements of the actors at each stage of the casual process are consistent with image of the world implied by each theory" (P. Hall, 2003, p. 394; see also: i.a. Collier, 2011; Checkel, 2005; P. A. Hall, 2006). Using primary and secondary sources I follow the parliamentary process of the first reading of the GPDR comparing the predictions made by the cultural and institutional theories with the quiet politics framework here proposed, focusing in the declared preferences of key political

[2] Germany, France, the UK, Italy and Spain

actors, corporate representatives, lobbyist and privacy advocates. In sum, I use media and literary citations, interviews, and analyze the effect of the change that the raising salience of privacy issues brought by Snowden had in the debate of the GPDR debate and its final outcome.

Empirically, this piece explores the tangible consequences of the global massive surveillance revelations made by Edward Snowden starting the summer of 2013 (Glenn Greenwald, 2014), arguing that would not have been Snowden leaking documents to the press on the massive public-private surveillance scheme orchestrated by the NSA, the EP would not have chosen to *strengthen* Europe's privacy rules.

This article is structured as follows. First, the literature review discusses the cultural accounts of the European privacy framework and its limitations, the institutionalist explanation of the 1995 Directive, and an overview of the literature on business power, lobbying, and issue salience. Then, part one of the analysis explores the GDPR debate from its announcement until the first documents revealed by Snowden are published, focusing on corporate lobby and the low salience of the debate. Part two explains Snowden's revelations and why and how they affect the GDPR debate, creating a window of opportunity for privacy advocates to reframe the now high-salience GDPR debate and defeat business power. A conclusion closes this piece.

Literature Review

The cultural accounts of Europe's privacy leadership: fascist legacies and European dignity

There are two predominant cultural accounts of European privacy leadership. The first and prevalent variant, known as the "fascist legacies theory" (A. Newman, 2008) highlights that Europeans have learned to defend and protect their privacy due to the totalitarian and fascist experiences of the last century (i.a. Beignier, 1992; Greenleaf, 2014; Lindsay, 2005b; Mullerat, 2007; Rotenberg & Jacobs, 2013; Ruyver et al., 2002). As Kilian points out, the experiences of World War II and long standing intellectual and cultural themes on privacy and the private sphere made Germany one of the first countries in the world to

adopt data privacy codes, and to this day Germans remain concerned about privacy invasions (2008).

However, this first cultural account has important limitations. First, as Newman highlights, the fascist legacies explanation fails to account for variation among the privacy approaches of different EU countries, for example: the UK, that did not experience a totalitarian government during the 20th century, adopted strong privacy institutions well before the enactment of the 1995 Directive and earlier than other nations that did experience fascist governments such as Spain and Italy (2008). Second, this first cultural account fails to explain the diffusion of German-style rules to the rest of the European Union: why did other countries with a different history than Germany adopt German rules? Third, somehow paradoxically, this account logic concludes that having learned to distrust the state, Europeans turn to the government and create powerful governmental agencies and institutions to protect themselves from that very same government. It is also ironic this this culturist explanation runs counter to the classic Tocquevillian argument about American Exceptionalism (Tocqueville, 2004). But, fundamentally, this account fails to explain the current surveillance state in which Europeans live (D. Wright & Kreissl, 2014). After all, if what motivates European leadership in privacy affairs is the fear of repeating surveillance abuses, why do Europeans allow their governments to create again powerful surveillance apparatuses?

Another verisimilar cultural account is the European dignity explanation, given by Whitman (2004). Comparing the American and the European privacy approaches, but only studying France and Germany and making claims for all Continental Europe, Whitman contends that Europeans view privacy as a matter of dignity while Americans see it as a question of liberty. According to Whitman, European ideas of privacy have their origins in late eighteen century notions of dignity and honor in French law, and Kantian notions of personality in Germany that place a greater emphasis in the right to control one's public image (2004). Whitman argues that European's, compared to Americans, are more reluctant to let the market determine one's amount of privacy.

And certainly, Europeans have built strong welfare states that try to counter-balance and regulate the effects of the market (Esping-Andersen, 2013) because they believe that there certain rights that belong to any citizen regardless of her or his social

condition. European welfare states guarantee its citizens generous paid holidays, while in America many workers cannot afford to get sick. Europeans have long had access to universal health-care provided or guaranteed by the government, while in America this is only a partial novelty. Europeans, in sum, believe that regardless power or money people have a fundamental right to privacy.

However, Whitman's argument also fails to explain variation in privacy approaches across the European Union before the 1995 Directive, and under close examination, reveals some limitations in its internal logic. For example, the UK, a non-continental Anglo-Saxon European nation, adopted privacy laws similar to those of Germany, while continentals and Latin-Spain and -Italy did not do so until mandated by Brussels. That limitation aside, Whitman's reading also fails to explain the expansion of German- and French-style privacy rules to the rest of Europe because of the 1995 Directive. In addition, like the other cultural explanation, Whitman fails to account the surveillance state prevalent in Europe –why did Europeans sacrifice their dignity and control of their own image with the creation of massive surveillance apparatuses? Last but not least, Whitman cannot account for why if Europe and the United States have historically and long-standing different approaches to privacy, contemporary researchers found that until the 1970s the privacy approaches across the Atlantic were strikingly similar (Colin J. Bennett, 1992, p. 95; Hondius, 1975).

In sum cultural explanations, as Steinmo has pointed out, have three severe analytical problems. First, cultural explanations fail to account for political change. Second, considering that political cultures consist of a mix of often contradictory or competing ideas, cultural based theories fail to provide a convincing explanation of why the dominant political culture might change in certain times or in certain arenas. Finally, the casual mechanisms of culture as an independent variable remain vague (Steinmo, 1994, p. 107). As a consequence of the limitations of cultural explanations, it is worth exploring other theories that account for the EU leadership in privacy matters. In the following section I present and discuss the Newman's institutionalist account.

The institutional account of the EU privacy leadership

In “Protectors of Privacy” (2008), centrally discussing and explaining the adoption of the 1995 Directive using a historic institutionalist framework, Newman argues that the DPAs established in the 1970s in some European countries, lobbied and “persuaded” the European Commission (EC) and the European Council and “held the European integration process hostage to their demands for greater protection within Europe by threating to block data flows between EU companies and governments” (A. Newman, 2008, p. 143) to achieve the 1995 Directive against intense lobbying by corporate and non-corporate actors (H. Farrell, 2002a; A. Newman, 2008). According to Newman, the DPAs became political actors capable of bolstering European rules and trough institutionalization they managed to make privacy a “taken-for-granted issue in European debates” (A. Newman, 2008, p. 143). And despite new security challenges that push to a rebalancing of national preferences toward privacy (A. Newman, 2008, p. 143), DPAs “continue to participate in and shape European policy” (A. Newman, 2008, p. 143). However as Newman explains, once the 1995 Directive was adopted the DPAs lost their veto power (A. Newman, 2008) and, as one can consequentially conclude according to Newman’s theory, the DPAs no longer had the same leverage within the political process of the GDPR as they had regarding the 1995 Directive. This contributes to explain why before Snowden, the MEPs reflected the preferences of corporations and not of the DPAs.

In later works, Newman has rightly pointed out that institutional innovations born as consequence as the 1995 Directive, such as the establishment of a European Data Protection Supervisor (EDPS) overseeing the compliance of data privacy rules by the European institutions and advocating for DPAs’ interests in Brussels and the consolidation of a network of coordination and work among DPAs in the 29th Article Working Party (WP29), signal that DPAs (including the EDPS) are actors whose presence is now taken for granted in European politics and that have reshaped European politics dynamics (A. Newman, 2010).

Newman has also highlighted how DPAs have used their newly granted powers to limit unilateral action from the European Commission in privacy matters, in alliance with the European Parliament (A. Newman, 2011). Newman illustrates this insight by discussing the case of the 2003 Passenger Name Record (PNR) agreement between the European Union and the United States: after the September 2001 terrorists attacks, the United States started requiring all airlines to share extensive personal information about

their passengers before accepting planes into its territory. The European Commission quickly tried to achieve an agreement with Washington in order to allow European airlines to keep their business running as usual, but since DPAs opposed and leveraged their authority in data privacy issuing public statements and lobbying the EP, the final PNR agreement of December 2003 was a compromise of the possible between the Commission and the DPAs (A. Newman, 2011, p. 492).

In sum, Newman's insightful explanation of the adoption of the 1995 Directive serves us in understanding the importance of institutions in Europe's privacy politics and to not take for granted cultural explanations. As Newman explains once the 1995 Directive was enacted, DPAs institutionalized their power in a way that makes it very unlikely that the general levels of privacy protection in the European Union will go down from the levels established in 1995 without first a watering down reform of the Directive. As Newman predicted, the cost DPAs pay for achieving that mostly certain floor of privacy protection was the tool that allowed them to raise the ceiling (A. Newman, 2008).

Paradoxically, DPAs lost their leverage once they succeeded in achieving the 1995 Directive. While in 1995 DPAs directly influenced and shaped common European rules and achieved the institutionalization of other similar agencies in European countries without them, by agreeing to the creation of a single European market for personal data they gave up their ultimate leverage. As long as the 1995 Directive is in place, DPAs cannot threaten with blocking the functioning of the single market since that would mean questioning the credibility of the framework that not only institutionalized their power, but that created many of them. In other words, DPAs success in forcing the creation of common data protection rules across Europe by threatening to block personal data transfers across EU nations came at the cost of –precisely- losing the capacity to threaten blocking personal data transfers across EU nations once the 1995 Directive established common rules *and* a single market. DPAs achieved institutionalization but lost leverage power vis-à-vis the other political actors of the EU.

Because DPAs lost their veto power with the adoption of the 1995 Directive, they failed to impede the enactment of the 2006 Data Retention Directive (Servent, 2013), that obliged EU member states to collect and store telecommunications for at least six months and that was declared invalid by the European Court of Justice (ECJ) in 2014 (Arthur,

2014). It is also why, despite the opposition and routine complaining of European DPAs, the 2000 Safe Harbor agreement that allows American companies to trade with Europeans personal data was signed and in full vigor (i.a. Falque-Pierrotin, 2014; H. Farrell, 2002a) until it was declared invalid by the ECJ in 2015 (Drozdiak & Schechner, 2015) and, crucially, why until Snowden's revelations the DPAs were being incapable of beating the corporate lobby convincing the EP to water down the GDPR so much so, that just a day before *The Guardian* (Glenn Greenwald & MacAskill, 2013) and *The Washington Post* (Gellman & Poitras, 2013) revealed the NSA's PRISM program to the public, on June 6th 2013, the EU Commissioner for Justice promised that the "absolute redline" for the GDPR was the levels of privacy protection of the 1995 Directive and called to "resist […] all attempts by those who are still trying to weaken data protection standards in Europe" (EC, 2013a).

In sum, the institutional account of the adoption of the 1995 Directive draws light in understanding Europe's privacy framework and the increasing role of the DPAs. In this regard, the institutionalist account correctly identifies that having lost their leverage with the adoption of the 1995 Directive one cannot account with the DPAs leverage capacity vis-à-vis the other European actors to achieve a GDPR that reflects the preferences of privacy advocates. It also proves that that it is necessary to question culturalist explanations beyond the obvious. Thus this explanation calls to consider new theories to explain *why* the GDPR was adopted.

The following section presents the analytical framework of this piece that sustains a theory to explain why the GDPR was adopted.

Analytical framework: business power and issue salience

The theoretical framework that better allows for analyzing and understanding the outcome of the parliamentary process of the GPDR is Culpepper's *Quiet Politics* framework, which briefly states that as "business power goes down as political salience goes up" (2011, p. 77). I argue that when the GPDR debate happened under low political salience, corporations were able to see their preferences reflected by the EP, and when the debate became high salience, it was more possible for privacy activist to beat the corporate lobby and push the EP to strengthen Europe's privacy rules.

According to Culpepper, when people do not care or are not informed about an issue, it is easy for corporations to influence politicians with their expertise and knowledge on a topic. If politicians do not feel that the people care about an issue they will prefer to follow the interested advice of corporations, hoping that by doing so the economy will not be disrupted –and consequently the voters will award them with re-election (P. Culpepper, 2011). Under low salience scenarios, corporations triumph: "Superior knowledge of the terrain and access to key decisionmakers are the most valuable resources in quiet politics, compensating for the small number of votes directly represented by senior managers in any democracy" (P. Culpepper, 2011, p. 4).

If the public salience of an issue goes up, politicians will be more open to looking for additional sources of information than just corporations to satisfy public needs, fearing to lose office if they do not do so (i.a. P. Culpepper, 2011, p. 4; Kollman, 1998, p. 9). Thus, raising the salience of an issue makes corporations less influential (i.a. P. Culpepper, 2011; Smith, 2010; E. T. Walker & Rea, 2014; Werner, 2012). Anyone involved in politics or activism quickly grasps the logic and powerful simplicity of Culpepper's argument. Most of the time, poor, un-influential organized groups that want to defeat the interests of organized business can only win if people start paying attention to their cause and aligning with them. Most politicians want to be re-elected and will not risk voting against a majoritarian public sentiment. Corporate influence is visible thorough lobbying and donations, yet the primary method of civil society coalitions influence is raising public awareness through targeted campaigns funded by limited resources.

Kollman has defined political issue salience as "the relative importance people attach to policy issues", and argued that "more salient policy issues will weigh more heavily on voting decisions that will less policy issues" (1998, p. 9), and therefore the higher the issue salience, the more likely policy makers will make an effort to be informed on them and advance policy or regulatory change (i.a. Baumgartner, Boef, & Boydstun, 2008; Baumgartner & Jones, 2010; T. J. Johnson, 2013; Kollman, 1998). In other words: when the salience of an issue is high, policy makers have more incentive to learn more about an issue because they know their voters care about it, and will not only weigh differently the advice given by corporate representatives, but will be more open to hearing non-corporate groups in order to capture constituents' preferences.

A good and generally accepted proxy for political salience is the presence of an issue in mass media such as newspapers, since more attention political actors pay to such issues and the more concerned members of the public are about specific issues, the more likely the news media are to cover them (Atkinson, Lovett, & Baumgartner, 2014; Boydstun, 2013; Edwards & Wood, 1999). After all, in aggregate, newspapers will only persist in publishing news that their consumers care about reading and being informed enough to continue using their services (P. Culpepper, 2011, pp. 5–9; Gormley, 1986; Wilson, 1974). In general, this insight builds up a broader agenda of research on media salience that proves that the higher the media salience of an issue the more chances the public is going to have an informed opinion about it (i.a. Barabas & Jerit, 2009; Kellstedt, 2003; Zaller, 1992).

Epstein and Segal argue that the coverage offered by national newspapers is a good measure of issue salience since it offers the advantage of being a "reproducible, valid, and transportable measure of assessing whether the particular actors under investigation view an issue as salient or not" (2000, p. abstract). In fact, many studies of policy-making use press coverage as an indicator of salience of an issue (i.a. Baumgartner & Jones, 2010; Collins & Cooper, 2012; Nicholson-Crotty, 2009; Smith, 2010). While research focused in the United States usually relies in only one source for measuring issue salience, mostly *The New York Times*, this preference presents three serious methodological problems. First, even a newspaper with national and international vocation such as *The New York Times* is more likely to cover stories that impact the immediate geographical surroundings of its headquarters (Oppermann & Viehrig, 2011, p. 242). Second, one could object that the editorial boards of newspapers will bias coverage to their political concerns (P. Culpepper, 2011, p. 20; L. Epstein & Segal, 2000). Third, relying on a single source might make the researcher unaware that the chosen proxy does not represent a larger "news agenda" (Atkinson et al., 2014).

A straightforward solution to the limitations mentioned in the previous paragraph is to increase the number of sources analyzed to guarantee more geographical coverage, including newspapers with different editorial houses to the equation (P. Culpepper, 2011) "since it is clear that certain events or topics are so clearly newsworthy that, if we track attention in a range of sources, all will show similar trends" (Atkinson et al., 2014, p. 356). However, measuring salience at the European level adds a layer of complexity to the

issue, since there are no truly European-wide newspapers. Mahoney has tried to solve this problem by using *The Financial Times* as a source for measuring issue salience in Europe, arguing that such measure offers comparability with *The New York Times* for transatlantic comparative studies (2007, 2008). However, while *The Financial Times* is likely the closest thing to a European-wide newspaper, relying on it only would suppose the same limitations that relying only on *The New York Times* supposes (*The Financial Times* is a London based newspapers with a right-of-center editorial board), plus the aggravating fact that *The Financial Times* is a newspaper specialized in economic and financial issues.

To counter these limitations, I instead use two printed-editions of the main newspapers available on *Lexis-Nexis* of each of the big five European Union countries - Germany, France, the UK, Spain and Italy– that together account for more than 60% of the EU's population. Methodologically, I first search for the news and opinion pieces on Internet privacy or the GPDR[3] from the 1st of January 2012 (when the GDPR was presented by the Commission), to the end of March of 2014 (when the EP Plenary voted its position). Within those results, I look for those mentioning the global surveillance revelations[4] to add detail to the understanding of their effect in the salience of Internet privacy issues at large. I controlled for duplicates and false positives. A graph presenting the findings is present in Figure 1, in the analysis part of this article.

But how does an issue become salient? There are two main reasons why an event might make become a public political issue: the intrusion of an issue because of a crisis or external shock (Jones & Baumgartner, 2005, p. 68) or the work of political entrepreneurs trying to mobilize the public opinion by revealing a scandal, putting opponents at the defensive, and associate certain policies with widely shared values (Derthick & Quirk, 2001; Wilson, 1980). The first refers to the raising of the salience of an issue because of a sudden crisis or shock that brings attention to a specific issue. The second refers to the work of an individual or a group of political entrepreneurs trying to bring the attention to a specific issue with mobilization campaigns. In the case of the GDPR debate we will see

[3] The query terms were: In English, *(regulation w/10 "data protection") OR (internet AND privacy) OR (online AND privacy)*; in Spanish, *(regulación w/10 "protección de datos") OR "privacidad en la red" OR (privacidad AND online) OR (privacidad AND internet)*; in French, *(régulation w/10 "données personnelles") OR "confidentialité en ligne" OR (confidentialité AND internet) OR (confidentialité AND online)*; in Italian, *(regolazione w/10 "protezione dei dati") OR "privacy su internet" OR (privacy AND internet) OR (privacy AND online)*; in German, *datenschutzverordnung OR datenschutzreform OR (datenschutz AND internet) OR (datenschutz AND online).*

[4] The query term was the same for all languages: *(Snowden OR NSA OR PRISM OR xkeyscore OR tempora or XKeyscore).* PRISM, xkeyscore and tempora are the names of the most well known NSA programs revaled by Snowden.

the manifestation of both main reasons for an increase in the salience of an issue in Snowden and his actions: the first revelations of Snowden, while he was still in anonymity, produce a shock that bring attention to privacy and surveillance issues in general and the GDPR in particular; second, we see the clear behavior of a political entrepreneur in Snowden –and a close group of collaborators- once he leaves anonymity and starts to carefully publish information and bring attention to privacy and surveillance issues and the GPDR during 2013.

However, before turning to the empirical analysis of this piece, in order to understand and explain the influence of business in relevant policy discussions as the GDPR, one must first revisit the distinction between the concepts of instrumental and structural power of business, and the two dimensions of business power mobilization: strategic or automatic.

The dimensions of business power and how to mobilize them

In the *Communist Manifesto*, originally published in 1848, Marx and Engels declared that "the executive of the modern state is but a committee for administering the common affairs of the whole bourgeois class" (1967, p. 2). In 1913 the privacy advocate and future Judge of the American Supreme Court Louis Brandeis denounced an oligarchy of bankers working towards the consolidation of industries (2009). However, the interest of political science in the study of business did not start consolidating until the aftermaths of World War II and has fluctuated ever since (Hacker & Pierson, 2002; Paster, 2015; Vogel, 1987).

Since the 1960s, political scientists have conceptualized two sources of business power: instrumental (Miliband, 2009; Mills, 1999) and structural power (i.a. Block, 1987; Dahl & Lindblom, 1976; Charles E. Lindblom, 1982; Charles Edward Lindblom, 1977). And while both sources are now read as complementary (i.a. P. D. Culpepper & Reinke, 2014; Fairfield, 2010; Hacker & Pierson, 2002; Vogel, 2003), until the 1970s instrumentalists dominated the debate and from then until the end of the 1980s structuralists built their theory largely neglecting the instrumentalists' insights (Hacker & Pierson, 2002).

During the 1960s and until the mid-1970s, instrumentalists overemphasized the instrumental power of business by arguing that capitalist societies were dominated by a

cohesive and unchallenged "power elite" (e.g. Mills, 1999). Instrumentalists argued that the power of business comes from its "ability to staff governments with business supporters and to exert direct influence on government decision makers through campaign contributions and lobbying efforts" (Hacker & Pierson, 2002, p. 280). Instrumental power, then, comprises the toolbox of instruments that corporations have to influence policy makers: with campaign donations and the hiring of lobbyist as perhaps the most obvious instruments, companies also have privileged access to policymakers by nature of their expertise, and can constitute or participate in organizations that defend their interests (Fairfield, 2010, p. 40).

Unsatisfied with the divisive interpretation of politics and society made by the instrumentalists, a group of reformed pluralists leaded by Lindblom and Dahl started arguing that business are a *structurally* privileged and powerful interest-group, but there is no power elite puppet master behind the scene of politics (Dahl & Lindblom, 1976). In the words of Lindblom, there is "no conspiracy theory of politics, no theory of common social origins uniting government and business officials, no crude allegation of a power elite established by clandestine forces" (1977, p. 175) needed to explain that the nature itself of capitalist democracies makes business structurally powerful, since they are central for its functioning by the fact of creating jobs and wealth (i.a. Block, 1987; Dahl & Lindblom, 1976; Charles Edward Lindblom, 1977).

Structuralists argued that since corporations decide the salaries and working conditions of most citizens and control the aggregate creation of wealth by determining when to invest and when to disinvest, corporate-managers rival elected officials in how their decisions affect people's lives (Block, 1987; Dahl & Lindblom, 1976; Charles Edward Lindblom, 1977). Therefore, the power of companies is structural because the pressure to protect business interests is automatic and apolitical: it results from the aggregate preferences of thousands of corporate managers and not from direct attempts to influence policy makers. Hence, dramatically, Lindblom concludes that "the market might be characterized as a prison", since "it imprisons policy making, and imprisons our attempts to improve our institution […] because it afflicts us with sluggish economic performance and unemployment simply because we begin to debate or undertake reform" (1982, p. 329).

Ironically, this dramatic depiction of the market as prison had a divisive effect in the analysis of business power, similar to of the theorization of a "power elite" governing politics made by the instrumentalists, precisely criticized by the first structuralists. Attempting to amend the first structuralists, Przeworksi and Wallerstein (1988), and Swank (1992), argue that capitalist democracies are compatible with various arrangement between corporations and the state and that the degree of government intervention in the market varies across countries and in time. Crucially, Vogel offers a "dissent from the new conventional wisdom" (1987) of business power constructed by Lindblom and Dahl, arguing that business are not unified and do not share the same set of interests which sign increases the flexibility of public policy (1987, p. 396); that governments are not necessarily afraid of disinvestment and of raising of unemployment, as the government's of Thatcher and Regan demonstrated (1987, p. 395); that corporations do not have concrete preferences in all policy areas (Vogel, 1987, p. 406); and that if a government would listen to every corporate demand the economy would stagnate (1987, p. 396).

Specifically, Vogel (1987) and Hacker and Pierson (2002) argue that the structuralist account as offered by Lindblom and Dahl (1976) fails to explain three crucial issues. First, it fails to explain variation of policy developments across countries and in time, since it cannot explain why when facing the same kind of business power different governments are capable of taking –and take- different policy decisions on similar topics. Second, it fails to explain why companies sometime lose political battles. And third, it fails to account for the confrontation of business with other business (Hacker & Pierson, 2002; Vogel, 2003).

Hacker and Pierson propose amending the structural visions of business power with four logical propositions. First, the structural power of business should be considered as a variable depending on how credible the threat of disinvest is, and not a constant. If policy makers are not afraid that business would actually decide to withdraw from a jurisdiction, then corporate influence is positively not the same as if delocalization is everyday news (Hacker & Pierson, 2002, p. 282).

Second, Hacker and Pierson argue that while the structural power of business is a powerful signaling device for policy makers, it remains just one signal among other pressures policy makers must take into account before deciding a certain policy. In this

sense, they argue that depending how business exercise their instrumental power will have a definitive effect in policy makers' final decision (2002, p. 282). Third, the expectation and understanding of the effects of a policy on profits are as important as the actual effects of a certain policy in determining which is the perceived risk of divestment by business. In other words, if by the state of the economy or the labor market policy makers do not consider a certain policy to be a trigger for divestment, the structural power of business is less relevant. (2002, p. 282).

Fourth, and last, traditional accounts of structural power of business assume that business interest are monolithic, when in reality certain policies might benefit certain industries at the cost of others. For example, copyright-strengthening initiatives might benefit content holders at the expenses of content distributors (2002, p. 282).

In a recent piece, Culpepper and Reinke offer insights that allow us to analyze with more granularity how business exercise their power and the interaction between the structural and instrumental sources of such power. They argue that the prevalent understanding of the sources of business power—that is, if its structural or instrumental—neglect an understanding of the way resources are mobilized, if automatically or strategically (2014). First, Culpepper and Reinke argue that since both the instrumental and the structural faces of business power can be mobilized automatically, it is not how they are mobilized what distinguish them. For example, while having business-friendly legislators is an instrumental tool of business power, it is also an automatic one, such legislator will automatically and logically think about the cost benefit of an initiative to the interest it represents without ever even being asked to do so.

Second, Culpepper and Reinke explain that business can choose to strategically mobilize their structural and instrumental resources to win a political battle—even if the structural power of a certain business is overwhelming, unless such business exercises or threatens to exercise that power, one cannot assume that all its battles will be won. Agency, the willingness and capacity to mobilize structural and instrumental resources can be as important as the resources themselves (P. D. Culpepper & Reinke, 2014). In other words, while the structural power of business is automatically in policy makers' minds, companies can also choose instrumental tools to remind them that divestment is not only a possible outcome, but can be an actual plan. As a consequence, in this paper the structural

and the instrumental sources of business power are read in a complementary matter paying attention to how they are mobilized.

But then, when do companies decide to get involved in a political battle? And how do they do it? Logically, companies are more likely to pursue political activity if they perceive that a piece of legislation or a certain policy might impede or condition how to carry their business (Hillman, Keim, & Schuler, 2004; Shaffer, 1995). And lobbying is a logical step once a company has decided to get involved in a political battle. After all, as lobbying scholars like Walker argue, once companies decide to get involved in a political battle they often seek to mobilize the public in their favor (E. T. Walker, 2012, p. 572). At the same time, since understanding business lobbying is a necessary for understanding what happened with the GDPR, it is worth exploring.

Business Lobbying

While in most people's minds lobbying takes places when a public official receives a person with a suit and a briefcase representing a corporation or a law firm, political science identifies two kinds of lobbying: inside and outside lobbying. Inside lobbying focuses in the private contacts of with policy makers and their teams, the offering of testimonies in hearings and panels, financial contributions to campaigns, the circulation of position papers, and in general all the kinds of influence-aimed activities that typically take place inside governmental offices (Beyers, 2004; E. Walker, 2013). Second to Washington DC, Brussels has the highest concentration of lobbyists in the world (Judge & Earnshaw, 2008, p. 102), with an estimate of at least 30.000 lobbyists, according to the European Corporate Observatory (Traynor, 2014). Like in DC, Brussels lobbyists are aware that Europe's capital is an "insider's town" (Greenwood, 2003, p. 5; Hrebenar & Morgan, 2009, p. 103; Judge & Earnshaw, 2008, p. 102), where to be successful they must know whom to talk with, when, and have access to the key actors.

In contrast with inside lobbying, outside or grassroots lobbying is about the recruitment and mobilization of citizens and other organizations capable of influencing politics, including building coalitions with non-governmental organizations, organizing rallies, and encouraging citizens to contact their representatives (i.a. Bergan, 2009; Beyers, 2004; Kollman, 1998; E. Walker, 2013); this is the point when inside lobbying

meets social movements, civic engagement and public opinion (Mahoney, 2008, p. 147). In Brussels, outside lobbying remains exceptional (Lelieveldt & Princen, 2015, p. 142), at remarkably low levels in comparison to the United States (i.a. Mahoney, 2008; McGrath, 2005; Schendelen & Schendelen, 2010; Thomas, 2004) – in fact, according to research done by Mahoney, only 24% of EU lobbyists use outside lobbying strategies, in comparison with 49% of their US colleagues (Mahoney, 2008, p. 152).

There are several reasons why outside lobbying at the EU level is low. The first responds to how officials are elected: European Commission officials are not elected by the people, and only are only very partially accountable to the EP (i.a. Dijkstra, Fenger, Bekkers, & Edwards, 2013; Lelieveldt & Princen, 2015), and while the EP is elected by popular vote, voters elect mostly following domestic issues not European issues (i.a. Hix, 2013; Hix & Marsh, 2007; Hix, Noury, & Roland, 2006). As a consequence, it is usually not effective for lobbyists to try to orchestrate outside campaigns to convince citizens to pressure to achieve certain objectives. At the same time, many lobbying organizations find difficult to organize and coordinate protests or activities at the European level: not only people have to find an issue worth of their time, but logistically for lobbying organizations is hard to coordinate among many languages, cultures and media sources (Lelieveldt & Princen, 2015, p. 142).

However, when an organization considers outside lobbying, there are two variables they will have to evaluate to be effective. The first variable is the scope or the size of the proposed policy and the potential impact on the public (Baumgartner & Leech, 2001; Mahoney, 2008, p. 150) - an unappealing or highly technical issue will hardly get people's attention. The second variable of interest is how salient an issue is to the public. The highest the salience, the easier to mobilize citizens (Kollman, 1998). Evidently, it is important to keep in mind that each organization will also evaluate the convenience and the material cost of trying to mobilize the public. Thus, for example, if a company considers that public attention regarding a certain piece of legislation will be against her interests, she will not promote the raising of the salience of a that issue to attract the public. At the same time, if an organization does not have the material resources to sustain a more expansive outside lobbying campaign it will have to conform to more traditional ways of influencing policy makers.

Another important variant of outside lobbying used by corporations worth considering is "astroturfing", designed to "'fake' the support of broad coalitions behind a paying client's interest" (E. T. Walker, 2014, p. 19). The term "astroturfing" comes from "AstroTurf," a brand of synthetic carpeting designed to look like natural grass. Hence, fake organizations created and/or sponsored by large corporations to support their preferences are referred as astroturf organizations (J. McNutt & Boland, 2007; J. G. McNutt, 2010). Typically, astroturfing does not take place with people-gathering activities (since the people behind the astroturf organizations do not exist), but with e-mails, blogs, papers, fake profiles in social networks or letters to policy makers. In Washington DC, evidence collected by Walker suggests that the methods of astroturfing, in vigor for decades, have become so invasive that policy makers and their aides are at times opting for ignoring e-mails altogether (E. T. Walker, 2014, p. 87).

Realizing that the influence of fake grassroots organizations was diminishing, the lobbying firms that offer their services to corporations figured a way to have "real" fake organizations (E. T. Walker, 2014). These lobbying firms build, at corporate request and expense, the organizational infrastructure to enable true-citizen activism, while carefully crafting and framing a set of talking points for activists to repeat while suggesting venues for expression of those messages (E. T. Walker, 2014, p. 7). As Walker's "Grassroots for hire" book reveals, in the United States, up to thousands of real citizens participate in a typical campaign organized by one of the specialized lobbying firms, helping lobbyist show to legislators and regulators "that a client's concerns have motivated and organized constituencies mobilized to support them" (2014, p. 7).

Similarly to how AstroTurf fake grass is adopted by 21 NFL teams and but none of Europe's Champions League stadiums (Hidalgo, 2014), astroturfing and the sophisticated grassroots for hire are predominantly American. In Brussels, astroturfing is rare, and there is no evidence of the more elaborated fake grassroots for hire. In fact, only as late as June 2013, the influential *The Financial Times* opened an article, precisely on the reform of Europe's data rules and the consequential import of American lobbying methods to the capital of the Old Continent, entitled "Brussels: astroturfing takes root", discussing how European NGOs unveiled that the European Privacy Association (EPA) presented itself as an independent think-tank spite of being fully financed by Yahoo!, Microsoft and Google (Fontanella-Khan, 2013).

As a consequence "More Machiavelli in Brussels" (Schendelen & Schendelen, 2010), a reference scholarly book also popular among EU lobbyists (Moravcsik, 2014), considers that "professional lobby groups usually believe that silence is safer than sound", since noise widens the playing field and no lobbying group can control its chain-effects (Schendelen & Schendelen, 2010, p. 263).

As we will see in the analysis of this paper, corporations and their representatives used both inside and outside lobbying against the GDPR. And for much of GDPR debate it looked like their strategies to exercise their business power were flawlessly working.

The Analysis

Part I – a Copernican Revolution in European data protection

In February 2012, respected privacy expert and law professor Christopher Kuner defined the Commission's proposal for a GDPR like nothing else but a "Copernican Revolution" in European data protection "seeking to shift its focus away from paper-based, bureaucratic requirements and towards compliance in practice, harmonization of the law, and individual empowerment" (2012, p. 1). And, indeed, the proposed GDPR had important innovations for Europe's privacy. First, as a Regulation the law would be implemented in member states without transpositions, largely eliminating the risks of different levels of privacy protection across the continent as a consequence of different national interpretations to which Directives are subject to (Lelieveldt & Princen, 2015, p. 256). Second, the proposed GDPR mandated companies to obtain an explicit consent from customers for the collection of their personal data and limited the further processing of it. Third, the proposed GDPR created more independent and powerful DPAs capable of imposing fines to corporations of up to 2% of their global income (Kuner, 2012, p. 2013).

Privacy defendants positively received the proposed GDPR. In an opinion that together with the "opinion of the [WP29] should be considered as the contribution of the supervisory authorities to the legislative process in the EP" (EDPS, 2012a, p. 2), the EDPS considered that "the proposed GDPR constitutes a huge step forward for data protection in Europe" (EDPS, 2012a, p. 3). Regarding the proposed new sanctioning powers for DPAs, the chairman of the WP29 stated that "with these measures robust and effective

enforcement by DPAs can finally be realized" and that "that the rules proposed can put an end to the existing fragmentation and, subject to further improvement, strengthen data protection across Europe" (in WP29, 2012a, p. 1). In a broader opinion document, the WP29 as whole, welcomed the proposals "that seek to reinforce the position of data subjects, to enhance the responsibility of controllers and to strengthen the position of supervisory authorities, both nationally and internationally" and, although it called the Council and the EP to introduce some improvements, it sustained a generally positive stance in the crucial elements of the new regulation (WP29, 2014b, p. 4).

Privacy and digital rights NGOs were also happy with the proposed GDPR. European Digital Rights (EDRi, a European wide umbrella NGO of over 30 other civil advocacy organizations) welcomed the GDPR proposal "since Europe needs a comprehensive reform in order to ensure the protection of its citizens' personal data and privacy, while enhancing legal certainty and competitiveness in a single digital market", although it considered it only a first step (EDRi, 2012). Similarly, Privacy International argued that although the GDPR has "a number of weaknesses", "on the whole it goes a long way towards ensuring that data protection law is capable of adequately responding to contemporary and emerging threats to the right to privacy. Importantly it goes some way towards ensuring that all citizens of EU member states will have equal access to these protections" (Privacy International, 2012, p. 2).

Companies, in contrast, were less enthusiastic. Among many others, the American Chamber of Commerce to the EU (AmCham EU) and DigitalEurope, trade organizations based in Brussels that count Apple, Google, and Microsoft among others their members, critically welcomed the GDPR. DigitalEurope believed that there were several "key issues threatening the EU's digital technology industry" since "new administrative burdens" would create "useless paper trails and impose unnecessary costs" that "create significant challenges to […] continued economic growth" (2012, p. 1). Likewise, in an open divestment threat, the AmCham EU called to re-think some provisions of the GDPR in order "to make sure Europe remains a desirable place to do business" (AmCham EU, 2012b, pp. 2–3). More bluntly, Facebook's lobbying papers showed that the company was worried about the potential fines stipulated in the GDPR and believed that considering Europe's "moribund economic environment", "they could be a major blow […] given that

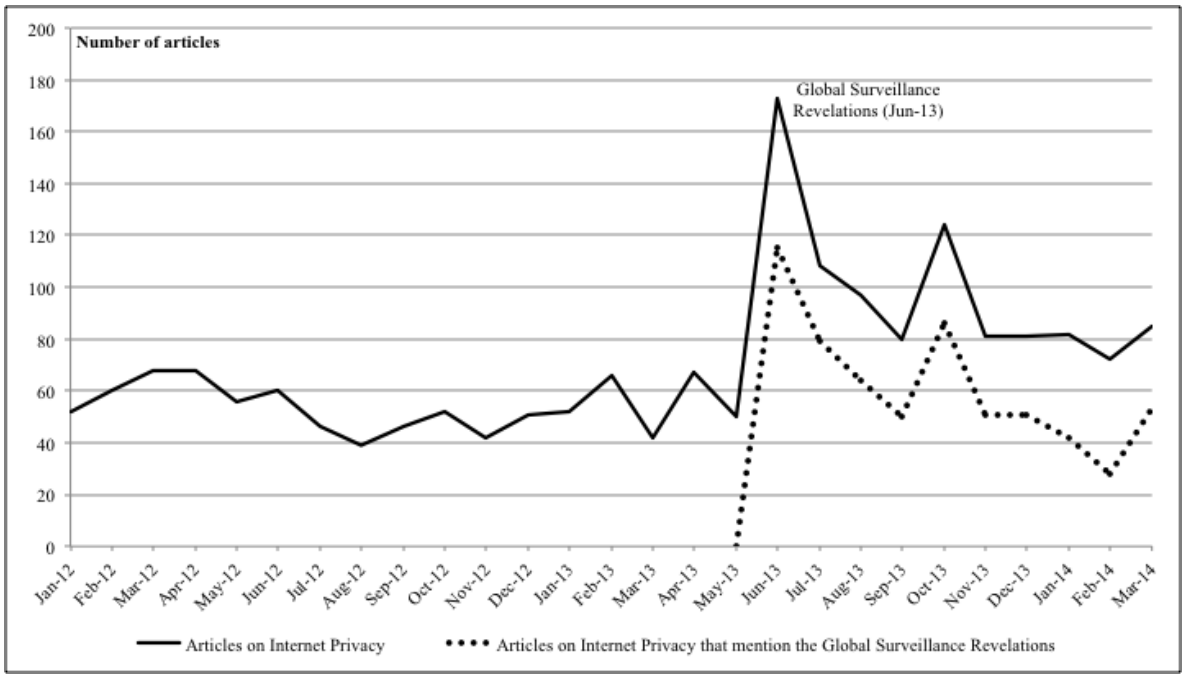
the Internet sector is widely recognized as the major driver of job creation and growth" (Facebook, 2012, p. 10).

Given the obvious fact that the GDPR was on the table and that in 2011 the EP had approved a resolution calling the European Commission to renew and strengthen the 1995 Directive guaranteeing the harmonization of European privacy rules at the highest level of protection (European Parliament, 2011), companies knew that the structural dimension of their power (i.a. Dahl & Lindblom, 1976; Charles E. Lindblom, 1982; Charles Edward Lindblom, 1977) was not proving to be a sufficiently powerful automatic trigger (P. D. Culpepper & Reinke, 2014) to moderate the views of the EP. Thus, companies chose to intentionally mobilize their instrumental power tools to see their preferences reflected in the GDPR.

As the following graph shows, until the revelations of surveillance of June 2013, companies were able to lobby for their preferences in a low salience scenario. The solid line details the number of articles on Internet privacy[5], and the dotted line the amount of those articles that mention the global surveillance revelations. Annex I contains the information disaggregated by country.

[5] The previous section details the construction of this graph.

Figure 4 Salience of Internet privacy issues in the five biggest EU countries



As the chart demonstrates, prior to June 2013 corporate lobbyists were operating in a low salience scenario. According to the quiet politics theory we will expect that in low salience scenarios corporations are going to be able to translate their preferences into policy-making.

The corporate lobbying campaign was run by public affairs experts and experienced politicians and public servants hired by corporations aware that Brussels is an insiders town when it comes to lobbying. For example, and in what illustrates companies' willingness of exercising and effective inside lobbying strategy (Beyers, 2004), one should consider that Facebook's team was composed by Richard Allan[6], who served eight years as Liberal MP in the UK and acted as campaign manager of the former Deputy Minister Clegg, and leaded by Erika Mann[7], who served as a German Socialist MEP for 15 years (1994-2009) and founded while in office the European Internet Foundation (EIF) - a forum that gathers more than 70 MEPs and Internet giants such as Microsoft, Google, Amazon and Facebook with the mission to "support Members of the EP from all political

[6] Richard Allan's LinkedIn https://uk.linkedin.com/in/ricallan
[7] Erika Mann's LinkedIn https://be.linkedin.com/pub/erika-mann/15/ba3/701

groups in their efforts to shape policy and regulation responsive to the growing potential of the internet and new technologies" (EIF, 2014); Microsoft had former Maltese ambassador to the EU (1993-1997) John Vassallo[8] in its public policy team; and Google employed Sarah Hunter[9], a former Senior Policy Advisor (2001-2005) of Tony Blair, as head of UK public policy and Antoine Aubert[10], policy bureaucrat of the European Commission from 2005 to 2008, as head of its Brussels Policy Team.

But not all the corporate lobbying was made in house. Companies hired the services of public affairs consultancies such as Kreab (EU Transparency Register, 2015) - where former Danish liberal MEP (1994-2009) and ALDE's vice-chairwoman Karin Riis-Jørgensen and founder of the astroturfing think-tank European Privacy Association (EPA), serves as senior advisor (Kreab, 2009)-; and law firms such as Hunton & Williams – that had almost half of their attorney staff working on the regulation (Eudes, 2013) – or Field Fisher Waterhouse (Lischka & Stöcker, 2013), whose well-known privacy expert Eduardo Ustaran declared to ZDNET that if Facebook and Google "weren't able to use your data in the way that is profitable or useful for them for advertising purposes, then either the user has to pay for it or stop using the service" (in Heath, 2013).

Aligning with companies, the US ambassador to the EU, William Kennard, told EU diplomats in December 2012 that the GDPR would create "poorly-connected regulatory environments for data exchange [that] will slow down transatlantic and global trade" (Kennard, 2013). Likewise, in an official visit to the EP, a representative of the US Department of Commerce warned MEPs that the GDPR would hurt the economy and cost jobs, and one of his colleagues from the Department of Justice that the Commission's proposal would suppose a threat for security by making fighting crime more difficult (Spiegel, 2012).

But the lobbying arsenal of companies was bigger. In order to push their preferences forward and multiply their voices, companies also used umbrella trade organizations such as the AmCham EU, the Software Alliance, DigitalEurope, the Interactive Adverting Bureau (IAB) Europe, or the Association for Competitive Technologies to publish position papers and organize events; MEP-Industry forums like

[8] John Vasallo's Economist Intelligence Unit Profile http://www.economistinsights.com/speaker/4040
[9] Sarah Hunter's LinkedIn https://www.linkedin.com/pub/sarah-hunter/17/866/712
[10] Antoine Ubert's LinkedIn https://www.linkedin.com/pub/antoine-aubert/2a/a2a/b4

the EIF to convince legislators in private industry-legislators events; and astroturfing think tanks such as the EPA or the Future for Privacy (FoP) to spread their word with scientific jargon. AmCham EU together with sympathizing MEPs organized a series of conferences across the European Union alerting business on the perils of the GDPR. For example, in January 2013 the Swedish conservative MEP Corazza Bildt told a Swedish business audience that her group was "already sharpening our knives when it comes to amendments" (in Landes, 2013). Likewise, DigitalEurope, organized activities such as a "data protection trip to Strasbourg" for industry representatives to have dinner with MEPs like ALDE's Alexander Alvaro to ask for data rules not to "come at the expense of European competitiveness" (DigitalEurope, 2012b), and held a Q&A event with EPP MEP Axel Voss where he expressed his "commitment to a [GDPR] that does not impede companies from doing business while adequately protecting individuals' data in our interconnected world" (DigitalEurope, 2012a).

The EIF, whose governor during 2010 and 2013 was ALDE's MEP Alvaro, organized several events exclusively for MEPs and lobbyists about the reform of Europe's privacy rules to give them "the possibility to hear from leading European technology firms and groups on the impact of the proposed [data protection] regulation" (EIF, 2013). As the EIF's chair, EPP MEP and former Culture Minister of Spain (2000-2004) Pilar del Castillo reflected in the preface of a book written by former British ALDE MEP (2009-2014) Bill Newtown Dunn "the [2009-2014] term of the EP will be remembered, amongst other things, because for the first time the Digital Economy played a leading role [and] in that context the [EIF] played a key role, continuously organizing debates responsive to the political, economic and social challenges of the worldwide digital transformation" (in Dunn, 2015).

Companies also used think tanks for astroturfing. The most famous of those astroturfing think tanks was the EPA, founded and chaired by Karin Riis-Jørgensen before she joined Kreab, that made the news headlines after an NGO denounced that it had failed to properly disclose to EU authorities that Google, Yahoo and Microsoft funded it (J. Baker, 2013). Supporting the position of corporations, EPA fellows had published academic papers in law journals (i.a. Balboni, Cooper, Imperiali, & Macenaite, 2013; Balboni & Macenaite, 2013) and – with the help of Irish MEP Sean Kelly (Balboni, 2013; Lovells, 2013)—held luncheons and breakfasts in the EP with MEPs and corporate

lobbyists (Balboni, 2013; Fontanella-Khan, 2013). However, one should also add to the list of astroturfing think-tanks the FoP, a DC-based think tank fully supported by the IT industry (FoP, 2015), which published papers aligning with the interest of US corporations such as a timely report defending the validity of Safe Harbor agreement from post-NSA surveillance revelations criticism in December 2013 (2013) and a series of papers dealing with the negative impact of the GDPR for US companies, like the "Privacy Papers for Policy Makers" supported by AT&T and Microsoft (2014).

MEPs and authorities felt the pressure from the aggressive lobbying of tech companies. For example, Josef Weidenholzer, Socialist MEP, told *The Financial Times* that "we [MEPs] are bombarded with emails and meeting requests by companies who want to water down the proposal […] I had never experience such lobbying in my life" (in Fontanella-Khan, 2013); similarly, the head of the WP29 considered the lobbying "unprecedented […] and extremely aggressive" (in Fontanella-Khan, 2013). Understandably, pro-privacy NGOs were worried about the impact of lobbying opposing the GDPR. Jeff Chester, from the American Center for Democracy and Technology expressed concern that the American companies' lobby in Europe was a "very intense" attempt to "weaken" European privacy rules (Dembosky, 2013); Likewise, in January 2013, the spokesperson of La Quadrature du Net (LQDN, a French digital rights NGO) Jérémie Zimmermann told *The New York Times* that "The outcome [of the GDPR] is very unclear at this point. The U.S. lobbying on this has been very effective so far. It is impossible to tell what will happen"(O'brien, 2013).

While I trust that the previous paragraphs have convince the reader that corporate lobbying was intense, intentional and serious, I expect skepticism. Was the corporate lobbying successful? How? The next section illustrates how companies had successfully managed to influence the EP.

Evidence of lobbying success in the EP

Capable of accepting, amending or rejecting the GDPR, the EP quickly became the center of the political struggle for Europe's privacy rules. Following the ordinary legislative procedure (previously known as the co-decision procedure), the EP, designated the Committee on Civil Liberties, Justice and Home Affairs (LIBE) as the "lead" Committee

responsible for drafting and approving a report with amendments on the GDPR to be ratified in plenary. After a successful bid by the Green Party, LIBE appointed as rapporteur, or report responsible, Green MEP Jan-Phillip Albrecht, an enthusiastic young digital rights lawyer, who included a well-known privacy expert and researcher as his advisor, fulfilling the traditional requirements for rapporteurs: qualifications, energy, and prestige (Lehmann, 2009, p. 52; Neuhold & Settembri, 2007, p. 159).

LIBE was mandated to consider the non-binding opinions and amendments of five other Committees: Employment and Social Affairs (EMPL); Industry, Research and Energy (ITRE); Internal Market and Consumer Protection (IMCO); Legal Affairs (JURI); and Economic and Monetary Affairs (ECON) –ECON, who however, decided not to give an opinion. Each of these committees also appointed their own rapporteurs for drafting their opinions: EMPL appointed Nadja Hirsch (European Liberal Party, ALDE); ITRE Sean Kelly (European People's Party, EPP) -who would receive the IAB Europe's Award for Leadership and Excellence in Public Policy "for his work on data protection" shortly after ITRE's opinion (Hennigan, 2013); IMCO Lara Comi (EPP); and JURI Marielle Gallo (EPP).

These rapporteurs worked in coordination with the shadow-rapporteurs to LIBE's report, appointed by their groups to closely monitor and control the work of Albrecht, draw the party line functioning as experts on an issue, inform their party peers of the deliberations, develop recommendations of action and write amendments (Neuhold & Settembri, 2007, p. 161). The shadow rapporteurs of EPP and ALDE were Axel Voss, and Alexander Alvaro respectively. Alvaro, who as mentioned before served as chair of the EIF, was later substituted by Sarah Lundford due to a serious car crash (Hudson, 2013). Sophia In't Veld would replace Lundford after the 2014 elections.

The opinions of ITRE, IMCO, JURI and EMPL are important for understanding the political process of the GDPR because they were approved well before LIBE's report (voted in committee in November 2013, after being delayed) and the disruption of the global surveillance revelations in European public debate in June 2013: IMCO approved its opinion on the GDPR in January 2013; ITRE in February; EMPL and JURI in March. In other words, IMCO, ITRE, EMPL, and JURI, gave their opinion when the GDPR was a low salience issue, and LIBE voted its delayed final report under a high salience debate.

The next table presents a timeline of the key events regarding the GDPR here discussed, and voting results where applicable. The EPP and ALDE constituted the core favorable majorities of the opinions.

Year	Month	Event	Result (if applicable: favor, against, abstention)
2012	January	Introduction GDPR	-
2013	January	IMCO's opinion on GDPR	Passed 19-16-1
2013	February	ITRE's opinion on GDPR	Passed 33-24-1
2013	March	EMPL's opinion on GDPR	Passed 35-3-6
2013	March	JURI's opinion on GDPR	Passed 14-6-4
2013	May	Delay of LIBE's report	-
2013	June	First revelations of Edward Snowden	-
2013	November	LIBE's report on GDPR	Passed 48-1-3
2014	March	Plenary Adoption LIBE's report on GDPR	Passed 621-10-22

Table 1 – Timeline: key events and, if applicable, voting results of GDPR in committee and plenary

Using the lobbying papers of corporations I evaluate if their preferences are reflected or not in the committees' opinions. The sources of those documents are the webpages of corporations and corporate organizations themselves (i.a. AmCham EU, 2012a, 2012b; AmCham Romania, 2012; FoP, 2013; Microsoft, 2012), and the more than 2,000 pages leaked by parliamentary assistants to NGOs[11]. It should be noted that the purpose of this exercise is to find which of the amendments proposed in the committees' opinions *respond* to corporate demands, and not to identify copied and pasted amendments - more a signal of laziness of the legislator than of overall lobbying success. For ease of reading and to facilitate the validation of the information provided, in what remains of this section I do not cite the four-committee opinions (EP, 2013a, 2013b, 2013c, 2013d) and instead mention them and the corresponding amendment.

An analysis of the lobbying papers reveal that companies were especially worried about seven key specific aspects of the GDPR: the requirement of explicit consent of the collection and processing of personal data; the definition of the legitimate interest of companies to collect, process and share with third parties personal information; the request for the notification of personal data breaches; the fines and sanctions system; the introduction of the concepts of pseudonymous and anonymous personal data; the new

11 Available at: https://wiki.laquadrature.net/Lobbies_on_dataprotection and http://lobbyplag.eu/docs

consumer's rights (to be forgotten, to erasure, and to data portability); and the mechanism for selection of each companies governing DPA, or one-stop-shop mechanism.

These seven aspects are also the core of the legislation: broad definitions of consent, legitimate interest, or pseudonymous and anonymous data would enable companies to use, massively collect, and process, freely and legally personal data with little-or-no control for citizens; low fines or sanctions of flexible application would relax the burden of non-compliance of the new rules; the not-recognition of new consumer rights will enable companies to continue business as usual; and a one-stop-mechanism that allows companies to be regulated by a friendly DPA would ease their operations across the Continent by enabling regulatory venue shopping. Table 2, at the end of this section, offers an overview of the corporate preferences on these seven issues and how the different committee opinions dealt with them.

In order to test the institutional theory, the preferences of the DPAs and the pro-privacy NGOs on these key issues are also presented. The cultural theories would predict MEPs to strengthen Europeans privacy rights. The quiet politics theory would predict that the preferences of MEPs would change depending on the salience of privacy issues.

- ***Consent***

The requirement of explicit "consent" from consumers to collect their personal data (art.4 of the GDPR) was especially worrisome for corporations. Google believed that "a default expectation of explicit consent [...] creates uncertainty and significant burdens for organizations" (Google, 2012, p. 3), Facebook felt that explicit consent would result in "inundating users with tick boxes and warning and may result in an overly disrupted or disjointed internet experience" (Facebook, 2012b), Microsoft believed that since "there is currently a wide range of mechanisms that effectively enable users to control and consent to collection and use of their personal information" explicit consent requests would "frustrate many users" (Microsoft, 2012, p. 6), Amazon expressed that such requirement would be "overly formalistic and rigid" (Amazon, 2013, p. 12), and eBay felt that is "too strict and creates an unnecessary obstacle to online and mobile business models" (eBay, 2012, p. 1). While the general direction of corporate preferences is towards a watering down of the requirement of explicit consent, eBay, Amazon and Facebook proposed

amendments that call to eliminate the requirement of explicit consent from the GDPR altogether (Amazon, 2013, p. 3; eBay, 2012, p. 1; Facebook, 2013, p. 23).

The EDPS welcomed the proposed clarification of consent on the GDPR (2012b, p. 19), and the WP29 was "of the opinion that the inclusion of the word 'explicit' is an important clarification in the text, which is necessary to truly enable data subjects to exercise their rights, especially on the Internet where there is now too much improper use of consent. It would be highly undesirable should this important clarification be deleted from the text" (WP29, 2012b, p. 7).

IMCO and ITRE were friendly to corporate demands. The 63rd amendment in IMCO's opinion called for the requirement of consent to be "*as* explicit *as possible according to context*", effectively diluting the requirement of explicit consent because of the addition of the qualifier "as possible according to context". The 82nd amendment in ITRE's opinion directly replaced the requirement of explicit for "unambiguous" consent. While JURI's preamble by the rapporteur justifies that "in spite of the hesitation of some parties, the rapporteur would like to retain […] the principle of explicit consent", amendment 5 of JURI's opinion adds that consent could be expressed "by using the appropriate settings of a browser or other application", a stipulation with the exact same language of the ePrivacy Directive, criticized by the WP29 for fearing it could lead to "erosion of the definition of consent and […] subsequent lack of transparency" (WP29, 2009). EMPL's opinion only covered the workspace related implications and aspects of the GDPR, and thus did not deal with consent.

- ***Legitimate interest***

The second aspect that worried corporations was the stringency of the condition for the "legitimate interest" (art. 6 of the GDPR) of processing personal information. In practical terms, the original wording of the GDPR left very little maneuver room for companies to process personal information without getting first the explicit consent of their customers – and as explained in the previous paragraph, companies had several objections to explicit consent. Hence, Google–worried about a clause that could impede the company from gathering the data collected trough their different services, such as YouTube and gMail and analyzing them as a whole—argued that "maintaining the viability of the 'legitimate interests' rule is important because it leaves room for organizations to process information

outside explicit consent through enhanced transparency and user control" (Google, 2012, p. 3). Calling for avoiding "legal uncertainty", eBay also called for extending the understanding of legitimate interest to *third parties* other than the entity collecting the personal information (2012, p. 5). Eurocommerce (the association representing companies selling products or services online, like Ikea, Lidl or Carrefour) and Accis (the association of consumer credit information suppliers, like Equifax or Experian), asked for amendments similar to eBay's since they considered that the GDPR would prevent them from processing data obtained by other organizations, and therefore rending activities such as credit reporting unfeasible since they would have to obtain direct explicit consent from the customer whose financial situation is being audited (Accis, 2012, p. 18; Eurocommerce, 2012a, p. 4, 2012b, p. 3) .

The WP29 considered that an expansion of the of condition of legitimate interest like the one asked for companies might "dilute the level of protection for EU citizens in comparison to Directive 95/46/EC in force" (2015a, p. 1), and the EDPS that "requirements for all data processing to be limited [, and we] recommend avoiding any conflation and thereby weakening of these principles" (2015, p. 5).

Listening to corporate demands, the amendments 70, 100, and 47 of the IMCO, ITRE and JURI's opinion respectively allowed third parties following a legitimate interest to process personal information collected by other organizations. EMPL did not take an opinion about legitimate interest.

- ***Notification of data breaches***

A third contentious aspect of the GDPR was the notifications of personal data breaches (art 4, 31 & 32), since to force businesses to take a more pro-active approach to data security, the GDPR introduced a strict data breach-reporting obligations. The Commission's proposal mandated the notification in 24hs to DPAs of *all* data breaches, and notification to customers if the breach was "likely to adversely affect the protection of […] privacy of the subject" (art 32). BusinessEurope complained that "mandatory notification requirements for all breaches, even minor ones, would impose significant compliance burden […] on controllers [and] supervisory authorities" and pointed to a cyber-security paradox: "only companies with good security will be able to identify breaches. [Companies] with poor security will fail to identify and notify any breaches

[and] will appear secure for the end-users" (2012, p. 14). Articulating that line of thought, Microsoft proposed that companies "should be required to notify data subjects and/or regulators of a breach only when there is significant risk of serious harm to the data subject" not in 24-hours but "without undue delay" (Microsoft, 2012, p. 6).

The EDPS recommended "a more realistic time limit than 24 hours […] (for example no later than 72 hours)" (EDPS, 2012b, p. 32), while the WP29 proposed a two step approach, "whereby notification of the breach [..] must in principle take place within 24 hours [but] in case all information cannot be provided within the 24 hour limit, the controller will have the opportunity to complete the notification in a second phase" (WP29, 2014b, pp. 16–17).

IMCO's opinion amendments 162 and 169 clarified that only breaches that "would have a *significantly adverse* impact on the […] privacy" of citizens should be notified "without delay" –eliminating the requirement of notification within 24 hours-, and that breaches should not be notified to customers "if the data breach does not have significant risks of harm to citizens". Like IMCO, ITRE's opinion amendments 245 and 255 eliminated the requirement of notification within 24 hours to the supervisory authority, and restricted the requirement of notification to data subject to special categories: professional secrecy, relating to criminal offences, or related to bank or credit card accounts. JURI's opinion amendment 11 also eliminated the 24-hour requirement and mandated that authorities only be informed about breaches with "considerable effect" on the data subject –a term relatively ambiguous. In sum, the opinions of IMCO, ITRE, and JURI emptied the notification requirement of content, rendering it vague and flexible –like demanded by companies.

- ***Fines and sanctions***

The fourth, and perhaps most obviously disputed, aspect of the GDPR were the stipulated fines and punitive sanctions (art 79): Companies were worried that the original wording of the GDPR stipulated that DPAs "*shall*" impose fines of up to different percentages of the worldwide turnover of corporations (from 0,5% to 2%) if specific violations were triggered. Microsoft criticized the "one-size-fits-all" of the GDPR since it "could be read to apply the same sanctions to deliberate, flagrant violations of the rules as it does to violations that are merely accidental" and called to a reform so "that DPAs be given the

authority to impose sanctions only where truly warranted" (2012, p. 9). In that direction, the AmCham EU proposed modifying the wording of Article 79 so to substitute "shall" for "may", leaving the reading of the relevant article as following: "the supervisory authority *may* impose a fine" (2012a, p. 49). More radically, BusinessEurope considered the sanctioning mechanisms of the GDPR as following a competition law approach "inappropriate and unacceptable in the context of data protection legislation" (2012, p. 16).

The WP29 was "of the opinion that DPAs should have a margin of discretion in deciding when to impose a fine" (2014b, p. 24), as was the EDPS (2012b) . At the same time, the EDPS and the WP29 preferred to have clear sanctioning thresholds (2012b; 2014b).

IMCO's opinion amendments 208, 209 & 210, ITRE's opinion amendments 370 to 397, and JURI's opinion amendments 178 & 208 eliminated all the originally quantified provisions of fines established in article 79 of the GDPR. ITRE's opinion, however, added a provision allowing DPAs to give written warnings without imposing sanctions and proposes that the "supervisory authority *may* impose [companies] a fine of up to [1 million euro] or [1% of its annual worldwide turnover]". JURI copied ITRE's approach only increasing the ceiling to 2% of a company's annual worldwide turnover while avoiding establishing mandatory sanctioning triggers and remedies. EMPL did not take an opinion in this issue.

- ***Pseudonymous data***

The fifth aspect of the GDPR that business considered important was the introduction of an exception to the use of anonymous and pseudonymous data (data that in theory cannot be traced back to a physical person without other information) with reduced requirements of collection and processing than identifiable data. The Commissions proposal did not contemplate definitions of anonymous or pseudonymous data, and therefore did not create exceptions for the usage of that kind of information. AmCham EU asked to add to article 4th of the GDPR definitions of pseudonyms and anonymous data and to create exceptions in treatment of that data in comparison with identifiable personal information (AmCham EU, 2012b), and Yahoo! to create exceptions in the conditions of the treatment of such information (2012). More specifically, the FoP argued "pseudonymization should excuse

controllers from certain obligations […] such as obtaining explicit data subject consent" (2013, p. 3).

The WP29 called for an explicit inclusion of the concepts of pseudonymous and anonymous data in the GDPR, (WP29, 2014b, p. 11) but considered that it should not be another category of personal data subject to a lighter regime for processing (WP29, 2015b, p. 2). Instead, the WP29 argued that it should simply be a technique for security and risk mitigation (WP29, 2014b).

IMCO, ITRE and JURI's opinion amendments 61 & 75; 77, 79 & 101; and 35 & 36 respectively introduced the concepts of pseudonymous and anonymous data as requested by corporations. Going further, IMCO and ITRE stipulated exceptions in the requirements of legitimate and lawful processing for pseudonymous data. JURI did not do that.

- ***New rights to consumers***

The sixth disputed aspect of the GDPR was the acknowledgment of new rights for consumers, like the "right to be forgotten and to erasure", that would oblige companies to remove from all the personal information considered no longer needed for its original purpose or if the customer withdraws the consent for the use of that information (art. 15, 16 & 17), and the "right to data portability", that would oblige companies to provide its customers with their personal in a "widely-used format" (art. 18). Regarding the "right to be forgotten", BusinessEurope argued that "this new right will have negative consequences for the transaction models of online services and for the functioning of banks, credit registers and other institutions" (2012, p. 8); AmCham EU called the "right to be forgotten and erasure" to be transformed in simply a "right to have […] personal data erased" unless when "identifying all relevant personal data in question proves impossible or involves a disproportionate effort and when […] such right is overridden by the interests or fundamental rights and freedoms of other rights" (2012a, p. 19). Regarding the "right to data portability", BusinessEurope argued that "the proposal does not really reflect the technical reality [and] does not belong to a data protection legislation piece" (2012, p. 9), and Microsoft that it did not "reflect how the internet is technically structured today, what consumers want and need, or how technology is likely to evolve tomorrow" (2012, p. 2).

The EDPS and the WP29 welcomed the introduction of the right to data portability, the right to be forgotten and the right to erasure (EDPS, 2012b, p. 23; WP29, 2014b, p. 6), although the EPDS "consider that the extent to which the right to be forgotten may be enforceable in practice remains unclear" (2012b, p. 23).

While JURI's preamble considered that "the 'right to be forgotten' should also be strengthened", ITRE's opinion amendment 156 and IMCO's opinion amendment 118, eliminated all reference to the right to be forgotten, leaving only a right to erasure of personal information. ITRE's amendment 162 also clarified that in case of the exercise of the right to erasure, a company should not be made liable or responsible of the implementation of such right by third parties that might have acquired the subject's personal data.

Regarding the right to data portability, IMCO's opinion amendment 25 stipulated that such right should not apply to personal data "used only internally" by the company –a vague term that might render ineffective the exercise of the right. ITRE's amendment 172 was written to establish limits to data portability "in relation to the legitimate interest of business" and stipulated that its exercise shall not adversely affect "trade secrets or intellectual property rights". JURI's opinion called for "deleting Article 18 introducing the right to data portability [since it] brings no added value to citizens concerning right of access". JURI proposed replacing Article 18 with a provision obliging companies to share an "electronic copy of non-commercial data underdoing processing in an interoperable and structured format which allows for further use" at request (amendment 78). As a consequence JURI's amendment 78, presents serious limitations to an effective right to data portability. For example, according to the wording proposed by JURI, a PDF file could be considered as an interoperable and structured format that allows for further use since a PDF complies with all those characteristics. However a PDF file does not necessarily allow the customer to change from one social network, like Facebook, to another –as originally stipulated by the Commission's proposal.

- ***One-stop-shop***

The seventh and last aspect of the GDPR that worried corporations was the introduction of a "one-stop-shop" for regulation (art. 51), stipulating that if a business operates in more than one Member State, the DPA of that Member State will have a 'lead authority'

effectively regulating the business' actions across the Union and determined by the location of the main processing activities. For example, Facebook welcomed this provision because "since 2010, Facebook Ireland Ltd has provided Facebook users in Europe with their service […] subject to oversight by the [Irish] Data Protection Commissioner" (2012b, p. 2). However, companies preferred some wording clarification to guarantee that the one-stop shop approach would apply to their operations in the European Union based on the Member State in which the organization's headquarters were based rather than where the processing of the information takes place –Facebook, for example, has its European headquarters in Ireland where it controls the purpose of data processing, and while it processes the information outside Europe would still would prefer to be only regulated by the Irish authorities for its European operations (2012b, p. 2). Microsoft, proposed an amendment to clarify that the one-stop-shop approach would apply to all the organizations depending on where their headquarters are, not where processing takes place (2012, p. 2).

The WP29 welcomed the provision on a one-stop-shop, although it considered that "it should in any event be clear that the competence of a lead DPA is non-exclusive. The competence of the lead DPA is subject to the obligations to cooperate, provide and accept mutual assistance" (2014b, p. 18).

Listening to corporate demands, JURI's opinion amendment 41 clarifies that the competent DPA has "exclusive competence to supervise the activities" of companies, and amendment 139 further explained that "the criterion for designating a competent authority should be the place of the main establishment". ITRE's opinion supported JURI's, and so did IMCO's, arguing "operations covering more than one country can easily be monitored by the main establishment, and should be the responsibility of a single authority" (amendment 35). At this point it is useful to note that until the summer of 2013 corporations were not worried about the standing of the Safe Harbor Agreement due to the fact that the GDPR stipulated that the Safe Harbor would continue to be a lawful mechanism for transfer to personal data from the EU to the US (article 40).

In sum, the previous paragraphs demonstrate that legislators were reflecting many companies' preferences, demonstrated by the opinions of IMCO, ITRE and JURI: the requirements of consent and legitimate interest were broadened, the mandate for

notification of data breaches was eased, pseudonymous data was introduced along with exceptions to its treatment, the right to be forgotten was replaced by a right to erasure and the right to data portability was either eased or deleted, and the arrangement for a one-stop-shop for regulation allows corporations to operate across the Union being subject to only one DPA, effectively authorizing regulatory venue shopping.

Hence considering the success of lobbying efforts, it comes as no surprise that as late as the 29th of May 2013, shortly before from the eruption of Snowden into the public eye, LIBE's GDPR rapporteur Albrecht told the *EUobserver*: "We promised the people that we will help give a proper legislation that will better enforce their rights, better protect their interest … and in the end, the only thing that we are doing - and this is not excluded – is to water down existing law" (Nielsen, 2013). Albrecht was rightfully worried for three reasons. First, as shown, companies were succeeding with their lobbying. Second, by May 2013 LIBE had received more than 3.000 amendments to the GDPR and had decided to delay voting until at least July (Nielsen, 2013). And third, a leaked note of the Irish Presidency of the European Council to the Council revealed "several member states have voiced their disagreement with the level of prescriptiveness of a number of the proposed obligations in the draft regulation" (European Council, 2013, p. 2).

The Irish leaked noted was in consonance with a previous report of the Cypriot Presidency that "Member States have voiced their disagreement with the level of prescriptiveness of a number of the proposed obligations in the draft Regulation" (European Council, 2012, p. 6). According to information collected in different points in time with sources in the EC, the EP, and the privacy advocates, Germany was one of the countries more fiercely opposing the GDPR in alliance with Sweden and the UK inside the European Council (i.a. Josefsson, 2013; Senior Advisor, 2016; Senior EU NGO Official, 2013; Senior Official EC Justice, 2013; Van Der Valk, 2016). The Council's opposition and effort to delay the GDPR was denounced by an anonymous source to *Der Spiegel* in December 2013, which specifically mentioned that Germany was pushing the breaks on the process (Hecking, 2013). After Snowden, however, Merkel would turn Germany's opposition around and denounce British inaction: "The UK wanted to delay the DPR because they feel that it may harm the interests of business […] Germany had

reservations on not moving too quickly to ensure that it can reconcile the existing rights of its citizens," she explained (Fleming, 2013).

Worried by all of this, Albrecht told *Le Monde* on the 2nd of June 2013 that "80% of those amendment proposals are arriving from abroad, from companies, primarily from Silicon Valley giants […], so many and active that it seems as if the same message comes from everywhere. That creates an overall atmosphere, that affects the general spirit"[12] and had turned the EPP MEPs against the GDPR (Eudes, 2013).

Yet, as we will see in the following section, the unexpected irruption of Snowden into the scene transformed the GDPR debate in Europe in general, and turned it around in the EP in particular.

[12] Translated by the author. Original in French: *"Plus de 80 % des propositions d'amendements arrivant de l'extérieur proviennent des entreprises, et principalement des géants de la Silicon Valley. […] Ils sont si nombreux et si actifs que le même message semble arriver de partout à la fois. Cela crée une ambiance diffuse, qui influe sur l'état d'esprit général.*" (Eudes, 2013).

Table 2 Overview of issues, corporate demands and committee's opinions

	Corporate preferences	WP29 / EDPS preferences	IMCO opinion	ITRE opinion	JURI opinion	EMPL opinon
Consent	Eliminate *explicit* consent requirement	Maintain explicit consent	Consent should be "*as explicit as possible"*	Consent should be *unambiguos*	Consent should be explicit but could be expressed *"using the appropiate settings of a browser"*	N/A
Legitimate Interest	Extend legitimate interest of personal data processing to *third parties*	Don't extend the legitimate interest	The legimatimate interest of personal data is extended to third parties	The legimatimate interest of personal data is extended to third parties	The legimatimate interest of personal data is extended to third parties	N/A
Data breaches	Notification should be mandatory only if there is significant risk or harm to a person. Eliminate 24hs notification requirement	EDPS prefered notification in 72hs. The WP29 proposed that companies can complement information past 24hs	Notification only if breach has a *significantly adverse impact on privacy.* No 24hs notification requirement	Notification only if data breached responds to *special categories*. No 24hs notification requirement.	Notifiacation only if breach has *considerable effects* on data subject.	N/A
Sanctions and Fines	Eliminate mandatory fines and sanctions for infringement	Want to eliminate mandatory sanctions, preffering degree of discretionality. They do want clear thresholds	No quantified sanctions. DPAs have discretionality to apply sanctions.	DPAs *may* impose sanctions. Provided maximum sanctions diminished.	DPAs *may* impose sanctions. Provided maximum sanctions diminished.	N/A
Pseudonymous and anonymous data	Create categories of pseudonymous and anonymous data with less obligations for companies than easily identifiable personal data	Include concepts, but without excemptions. Only as security and risk mitigation techniques	Creates categories and excemptions	Creates categories and excemptions	Creates categories	N/A
New rights to consumers	No right to be forgotten, only right to erasure. No data portability rights	Welcome all rights. EDPS wondered about if right to be forgotten is enforceable	No right to be forgotten, only to erasure. Right to data portability severely restricted.	No right to be forgotten, only to erasure.Creates categories and excemptions	Considers right to be forgotten should be strenghtened. Prefers deletion of right to data portability.	N/A
One-stop-shop	DPA of Member State where a company's headquarters are located should be the solely responsible authority over all EU operations of such company.	DPA of Member State where company is should be lead authority with *non-exclusive rights in cooperation* with other DPAs.	DPA of Member State where a company's headquarters are located should be the solely responsible authority over all EU operations of such company.	DPA of Member State where a company's headquarters are located should be the solely responsible authority over all EU operations of such company.	DPA of Member State where a company's headquarters are located should be the solely responsible authority over all EU operations of such company.	N/A

Part 2 – An unexpected twist

As we have seen, until June 2013 corporate lobbyists operated in a low salience scenario that enabled them to influence legislation. In the wake of the success of corporate lobbying, privacy defendants and activists were playing defense: a group of 100 European academics signed an open letter started by six worried German professors in February 2013 (Günter et al., 2013)[13] "to reply to some arguments that aim to weaken data

13 The list of signing academics is available at http://www.dataprotectioneu.eu/#signed

protection in Europe" since "huge lobby groups are trying to massively influence the regulatory bodies"; in June 2013 EDPS' chair, Peter Hustinx, told *The New York Times* that "the benefits for industry should not and do not need to be at the expense of our fundamental rights to privacy and data protection" (in Kanter & Sengupta, 2013); and LQDN was rhetorically asking if Europeans "will let protection of [their] data go down the drain" (2013c) after "US corporations win against privacy" (2013a) in IMCO and seeing "citizens' privacy jeopardized in EU Parliament [ITRE, IMCO and EMPL] committees again" (2013b).

The privacy-advocates had two important reasons to be worried about the possible outcome of LIBE's report. First, as we saw in the previous section, the corporate lobbying offensive had demonstrated to be effective in making legislators translate their preferences into amendments to the GDPR. Second, the rapporteurs of ITRE, IMCO, JURI and EMPL had presented joint amendments with the ALDE's and EPP's shadow-rapporteurs in LIBE in the same direction expressed in the opinions of the opinion-giving committees[14].

Not only were there pro-corporate amendments on the table, but also those amendments posed the real and tangible possibility of becoming the official position of the Parliament. The EP had a corporate friendly majority: shadow-rapporteurs Voss and Alvaro represented their parties' line regarding the GPDR, and EPP and ALDE had almost 50% of the votes, adding to the 7% of the Group composed by the British Tories. Therefore in the summer of 2013, even a *very* conservative best-case scenario prediction for privacy advocates of the Parliament's opinion on the GDPR would have been that the Parliament was *not* going to strengthen Europe's privacy framework and ratify European leadership in that field. After all, as Commissioner Reding put it just one day before the PRISM program was revealed to the public, the 6th of June 2013: "The absolute red line below which I am not prepared to go is the current level of protection as laid down in the 1995 Directive" (European Commission, 2013a). Yet, the next day everything would change.

[14] For example Axel Voss and Sean Kelly (EPP) presented join amendments watering down the requirements for explicit consent (am. 765); calling for the introduction of pseudonymous data (am. 730); expanding the legitimate interest to third parties (am. 878); eliminating the requirement of notification of data breaches in 24hs (am. 1957); watering down the right to data portability (am. 1492).
Alvaro and Ludford (ALDE) presented similar amendments (for example amendments 726, 762, 729, 898, 1959, 2885, 2896, 1506).

On the 7th of June of 2013, *The Washington Post* and *The Guardian* jointly published Top Secret documents leaked by a then unknown NSA whistleblower –revealed two days later to be Edward Snowden (Glenn Greenwald, MacAskill, & Poitras, 2013)- demonstrating how the NSA and the GCHQ were capable of "Collecting [data] directly from the servers of these U.S. Service Providers: Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, Apple." (B. Gellman & Poitras, 2013).

Luckily for privacy advocates the revelations of PRISM were not only an external shock that momentarily raised the profile of the Internet privacy debates in Europe, as seen in Figure 1, but were just the first of a series of revelations made by an activist, Edward Snowden. The timing and the pacing of the revelations were made strategically since Snowden identified himself as a privacy activist: "I want to spark a worldwide debate about privacy, Internet freedom, and the dangers of state surveillance" Snowden told journalist Greenwald in an email exchange (in Glenn Greenwald, 2014, p. 18).

Thus, for example on the 17th of June *The Guardian* revealed that GCHQ intercepted foreign politician's communications at the 2009 London G20 summit (MacAskill, Davies, Hopkins, Borger, & Ball, 2013); on the 21th of June *The Guardian* exposed that GCHQ and the NSA are taping on Internet fiber-optic cables to access world's communications (MacAskill, Borger, et al., 2013a); on the 30th of June *Der Spiegel* reported that the NSA is monitoring "half a billion telephone calls, emails and text messages in" Germany every month (Poitras, Rosenbach, & Stark, 2013); the 8th of July *Dear Spiegel* published an interview with Snowden in which he explains that German secret services are collaborating with the NSA (Der Spiegel, 2013); in August it became public that the NSA routinely spies on 75% of US Internet traffic (Gorman & Valentino-DeVries, 2013); in September revealed that some Internet companies cooperate with the NSA to circumvent encryption on their services (Ball, Borger, & Greenwald, 2013); and in October German chancellor Merkel announced that her cellphone was being spied by the NSA following an investigation triggered by Snowden's documents (Traynor, Olterman, & Lewis, 2013)[15].

[15] Wikipedia offers an exhaustive account of the Global Surveillance Disclosures: https://en.wikipedia.org/w/index.php?title=Global_surveillance_disclosures_(2013%E2%80%93present)&redirect=no

Due to these revelations, the previously aggressive and successful corporate lobby was forced to take the defensive and to distance itself from the US Government who had been supporting their lobbying efforts in Brussels. Mark Zuckerberg, CEO and founder of Facebook, said in an interview with *The Atlantic* that the Obama Administration's "response to the NSA issues that have blown up are a big deal for [Facebook's] global platform. Some of the government's statements have been profoundly unhelpful" (*The Atlantic, 2013).* Zuckerberg referred to a particular statement by Obama on *The Tonight Show*, where the President said "there is no spying on Americans. We don't have a domestic spying program" (Graham, 2013). "Oh, we only spy on non-Americans.' Gee, thanks! We're trying to provide an international service and not get crushed in those places either" (*The Atlantic*, 2013) was Zuckerberg's ironic remark to Obama's statement.

Internet companies tried to downplay their relationship with the US Government by publicly expressing outrage regarding the surveillance revelations. In December 2013 Google, Facebook, Microsoft and others launched the platform Reform Government Surveillance[16] and published "An open letter to Washington" arguing "[w]e understand that governments have a duty to protect their citizens. But this summer's revelations highlighted the urgent need to reform government surveillance practices worldwide" (O'Brien, 2013). However, companies never managed to explain why they did not denounce surveillance requests by the US Government or asked for a reform of the American surveillance apparatus before Snowden. As further secret documents revealed by *The Guardian* and *The Washington Post*, and statements of reactions of corporate lawyers to the newspaper's news confirmed, Internet companies were asking for and being reimbursed by the US Government for their efforts in complying with the NSA surveillance programs since at least 2011 (Fung, 2013; MacAskill, 2013).

These revelations severely hurt companies lobbying power since the general public began to perceive them as collaborators and enablers of state surveillance, as it is visible in various articles and opinion columns published in the EU after Snowden. For example, in June 2013 the well-known British historian Timothy Garton Ash published and op-ed titled "If Big Brother came back, he'd be a public-private partnership" in *The Guardian* (2013a), syndicated by *El País* with the less subtle translated title "The Big

[16] www.reformgovernmentsurveillance.com

Brother with the help of Google" (2013b)[17], in which he argued that "Edward Snowden's revelations about massive data-mining by American and British spying agencies show that most of the sources they are digging into are privately owned […].This commercial accumulation of intimate personal information is worrying in itself. The reassurance we are offered from Facebook, Google and others – 'trust us' – is not good enough. After all, it now turns out they've been sharing some of it with the spooks" (Garton Ash, 2013a). Similarly, *Le Monde* published a piece titled "The advertising terrorism"[18] explaining how the Internet companies have become allies of the "State within the State" by virtue of their data collection for advertising purposes (Enzensberger, 2013). Lastly, in the summer of 2013, the worldwide-read American magazine *The New Yorker* explained in an article named "Big Brother and Silicon Valley" that "the [NSA's] data-mining story has fundamentally changed the public's picture of Silicon Valley and its relation to the state […]. It turns out, the biggest companies in the computer business—Microsoft, Yahoo, Google, Facebook, and Apple, among others—have been giving vast amounts of user data to the government's chief surveillance agency, in some cases for years" (Packer, 2013).

The privacy defendants such as Commissioner Reding, rapporteur Albrecht and the DPAs used the opportunity created by the surveillance scandals to strengthen the GDPR by weakening the position of Internet companies, who now had to explain why they had been cooperating with the NSA behind the backs of their customers. On the 19th of July 2013, after an informal meeting with the Justice Ministers of the EU Council, Reding synthesized privacy defendants new leverage in light of the changed public discourse: "All EU institutions agree that we have to join forces in order to have a strong European data protection law for our continent […] PRISM has been a wake-up call. The data protection reform is Europe's answer" (in EC, 2013b).

Rapporteur Albrecht also quickly reacted to "leaks [that] hit the public in the middle of ongoing negotiations and debates in the EP on the GDPR" and reflected that "weakening data protection in Europe will only serve those who operate under weak or non-existing data protection rules in the United States or elsewhere", and thus called for introducing amendments to the GDPR to address the "NSA/PRISM/Cloud surveillance issues" (Albrecht, 2013). Similarly, the EDPS issued a statement noting that it was

[17] In Spanish, *El Gran Hermano con la ayuda de Google*
[18] In French *Le terrorisme publicitaire*

"following the NSA story closely and is concerned about the possible serious implications for the privacy and other fundamental rights of EU citizens" (EDPS, 2013a).

The companies were affected by the change in the framing of the GDPR debate. In an opinion piece published in *EurActiv* on June 2013, the director general of DigitalEurope complained that Justice Commissioner "Reding is confusing matters further by linking PRISM-gate to her attempts to push through her data protection regulation" and that her supporters "misleadingly claim that the critics are just US tech firms trying to dumb down European privacy laws for their own bottom line advantages" (Higgins, 2013). He, on the other hand, believed the revelations of surveillance highlighted "that the single biggest threat to citizens' privacy is surveillance by governments" (Higgins, 2013). However, companies' legitimacy was severely hurt by the revelations and their previously cozy relationship with the US Government in lobbying against the GDPR.

Unfortunately for companies, the surveillance revelations fundamentally changed the substance of the GDPR debate. If before the revelations the GDPR debate was solely about Internet privacy, now it had become about the protection of Europeans' Internet privacy from unwanted and abusive American surveillance. This is visible in the rhetoric of the conservative Groups. Thus, LIBE's shadow rapporteur Axel Voss (EPP), together with MEPs Gallo, Kelly and Comi called for the introduction of an anti-NSA surveillance clause in the GDPR "to restore the trust of EU citizens as we continue to negotiate the new Data Protection laws" (EPP Group EP, 2013).

Thomas Van Der Valk, parliamentary assistant of MEP Sophie in 't Veld (ALDE, who would become shadow rapporteur on the GDPR after the 2014 EP elections) explained several reasons for the change of ALDE's positioning and the EPP regarding the GDPR. Regarding the EPP, German Chancellor Merkel's outraged reaction to the news that her cellphone had been spied on by the NSA could have been understood as a push for the protection of privacy in general, and against mass surveillance in particular (Peel & Fontanella-Khan, 2013; Traynor, 2013). Regarding ALDE, while the party has had always had both a liberal pro-privacy wing and a pro-business anti-stringent data protection side, the 2014 EP elections saw a shift to the pro-privacy side within the party, including in the leadership of MEP in 't Velt on these issues (2016).

As expected by the quiet politics framework, under this new high salience scenario many of the privacy-advocates' preferences were highly emphasized when, in March 2014, the EP adopted LIBE's report on the GDPR by 621 votes in favor, 22 abstentions and only 11 votes against (in Committee, the report had received 48 votes in favor, 3 abstentions, and only 1 against in November 2013). It is worth noting that in the debate following the approval of the GDPR, MEP In 't Velt (ALDE) said that "this Parliament has to give a clear political signal that contrary to the national governments who are dragging their feet we stand up for the rights of citizens who have massively shown their interest in this legislation" (EP, 2014, minute 48:10), acknowledging the importance of the increasing salience of the GDPR debate. Likewise, it is telling that MEPs Ludford (ALDE), Comi (EPP) and Kelly (EPP), and Voss (EPP) previously opposed to several aspects of the GDPR limited their speeches to congratulate the Rapporteur Albrecht and make rather minor points, such as the importance to ensure a fair play ground to SMEs (EP, 2014)

Against the desires of corporations, the EP voted to maintain the requirement of explicit consent; the effective sanctions threshold was increased up to 5% of a company's worldwide turnover and DPAs could mandate companies to follow compliance and accountability programs; the one-stop-shop regulatory mechanism is maintained but the DPA of the Member State where the company operates must now consult with other authorities; data breaches must be reported not in 24hs but in 72hs; the right to data portability is maintained and strengthened; and, finally, the right to be forgotten is merged with the right to erasure but the provisions remain unchanged. It should be noted that in May 2014 the ECJ recognized the right to be forgotten as existing in the 1995 Directive, in the ruling of a case brought by the Spanish DPA against Google. This ruling, influenced by the Snowden revelations and the general sentiment in Europe, increases the power of DPAs now capable of asking Internet companies to remove content at the request of citizens (ECJ, 2014b). Furthermore, LIBE's report also establishes two innovations as a consequence of the surveillance revelations: international agreements for transfers of personal data such as Safe Harbor should be revised after 5 years, and companies are not allowed to transfer data to third countries authorities unless that happens under European law or an agreement based in European law (the anti-surveillance clause). Companies'

only notable achievement in the proposed regulation is the recognition of the concepts of pseudonymous and anonymous data with different requirements than identifiable data.

Unsurprisingly, the DPAs were happy. After LIBE's committee vote –correctly taking the parliamentary approval of the report for granted-, Peter Hustinx, the chief of the EDPS said that "the result is a positive step for further progress to be made" (in EDPS, 2013b, p. 1); likewise, the WP29 considered LIBE's committee vote "a major step forward in the process towards a comprehensive framework on data protection in the EU" (WP29, 2013, p. 1).

Days after all the Groups had achieved a consensus on the amendments that would be easily incorporated to LIBE's report in committee and in plenary, rapporteur Albrecht told *Time Magazine* what the effect of Snowden had been in the parliamentary process. "After Snowden" said Albrecht, "we agreed that data protection in Europe is part of our self-determination and dignity" but, he conceded he did not expect LIBE to agree in only two hours the privacy strengthening amendments he proposed to what was previously considered an already stringent proposal: "This was a surprise for everybody" (in Shuster, 2013).

Against all expectations and in a situation where not even the most optimistic analyst expected the EP passing a privacy *strengthening* GDPR, Snowden documents raised the issue of surveillance and privacy in the EU, and helped the privacy advocates to pass an even more stringent than original GDPR by providing them a logical framework of contestation. Ultimately, Snowden's revelations allowed the coalition of pro digital rights civil society to defeat corporate and US interests in the EP. This is a fundamental victory for privacy defendants: While the GDPR had yet to be negotiated and agreed between the EP and the Council, in obscure meetings called trilogues, the pro-privacy stance of the Parliament guarantees that many of their preferences will be reflected.

Conclusion

This article made several contributions. Empirically, it showed how corporations influenced the EP during the GPDR parliamentary process and also how the Global Surveillance Revelations made by Snowden tangibly affected the Internet privacy debate in Europe. Theoretically, by carefully analyzing the political process of the GDPR, this article shows the weaknesses of culturalist readings of Europe's privacy leadership. Much

like Newman demonstrated in *Protectors of Privacy* regarding the adoption of the 1995 Directive (2008), when one carefully analyses the political events, privacy reform in the form of the GDPR cannot be attributed solely to a unique blend of European values. In absence of Snowden, the GDPR would not exist as predicted by cultural theories which are limited precisely because they fail to account for political events like the political outrage generated by the NSA whistleblower.

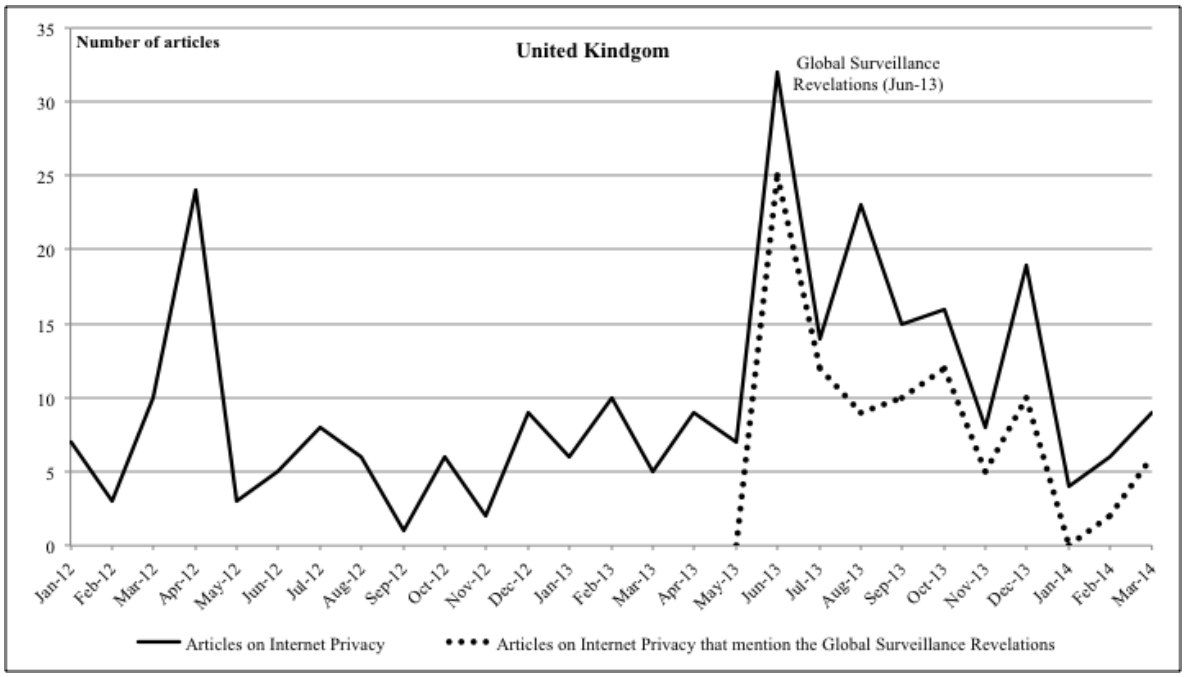
It should be noted then, that this article does not suggest that Europeans do not care about their privacy or only care when privacy is in the news. The fact that Europeans were outraged to the Snowden revelations and that many policy makers changed their position regarding the GDPR when they realized that their constituencies deeply cared about the issue reveals that under some scenarios European's privacy culture has political effects. But by failing to account for political processes and variation in time of the position of political actors, cultural theories tend to fall into a static confirmation bias built upon the narrative fallacy of only accounting for positive outcomes. It is clear then that the Snowden revelations had an effect in the GDPR process in the EP because at least a part of the European public was susceptible to deeply caring about this issue. And we can identify this fact, as well as the fact that in absence of the Snowden revelations policy makers were not automatically defending people's privacy, because of Historic Institutionalism and incorporating power and institutions to societal analyses.

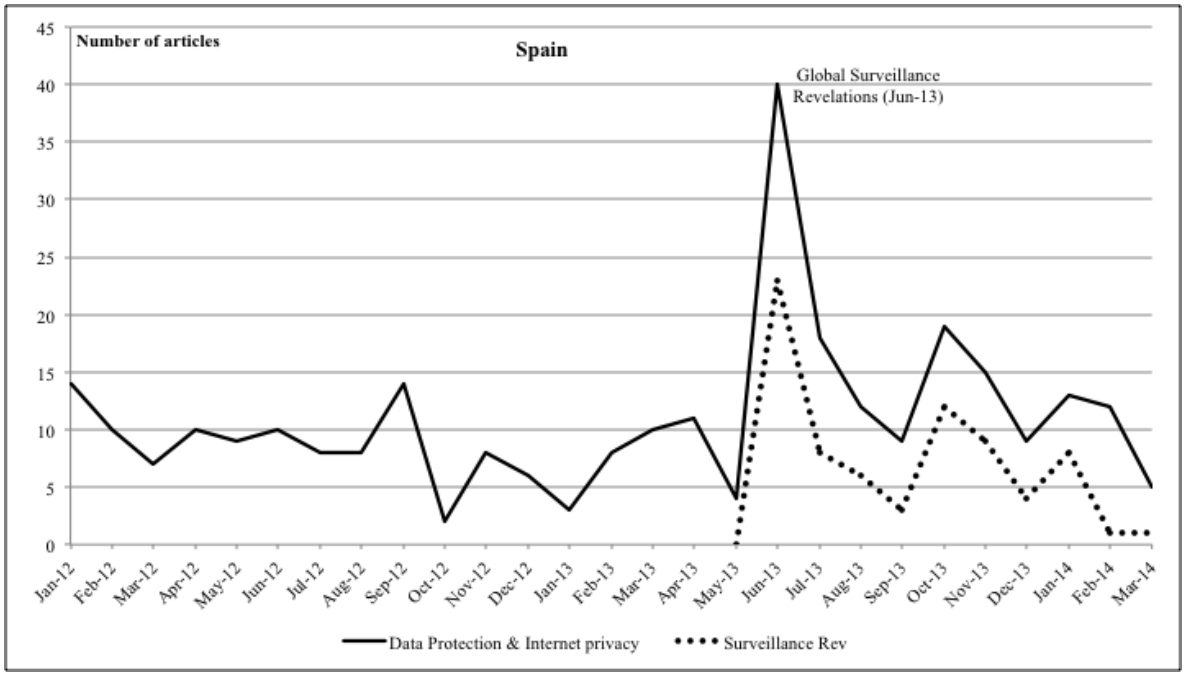
Regarding corporate power, we have seen how Silicon Valley companies used lobbying strategies defined as aggressive and unprecedented by key EU political actors that proved to be very successful in low salience scenarios: the opinions of opinion-giving committees on the GDPR reflected corporate preferences. Yet, the previous pages have also shown that the structural power of these companies did not trigger an automatic response by policy makers, and instead corporations had to turn to an intentional mobilization of their power and a heavy strategy of inside lobbying, which lost much of its effectiveness when the issue salience became high. Likewise—and although this aspect should be explored further—the case of GDPR seems to indicate that astroturfing has been successfully introduced to Brussels by American corporations. The case of the GPDR indicates that in Brussels there no evidence of the "grassroots for hire" phenomena described by Walker (2014).

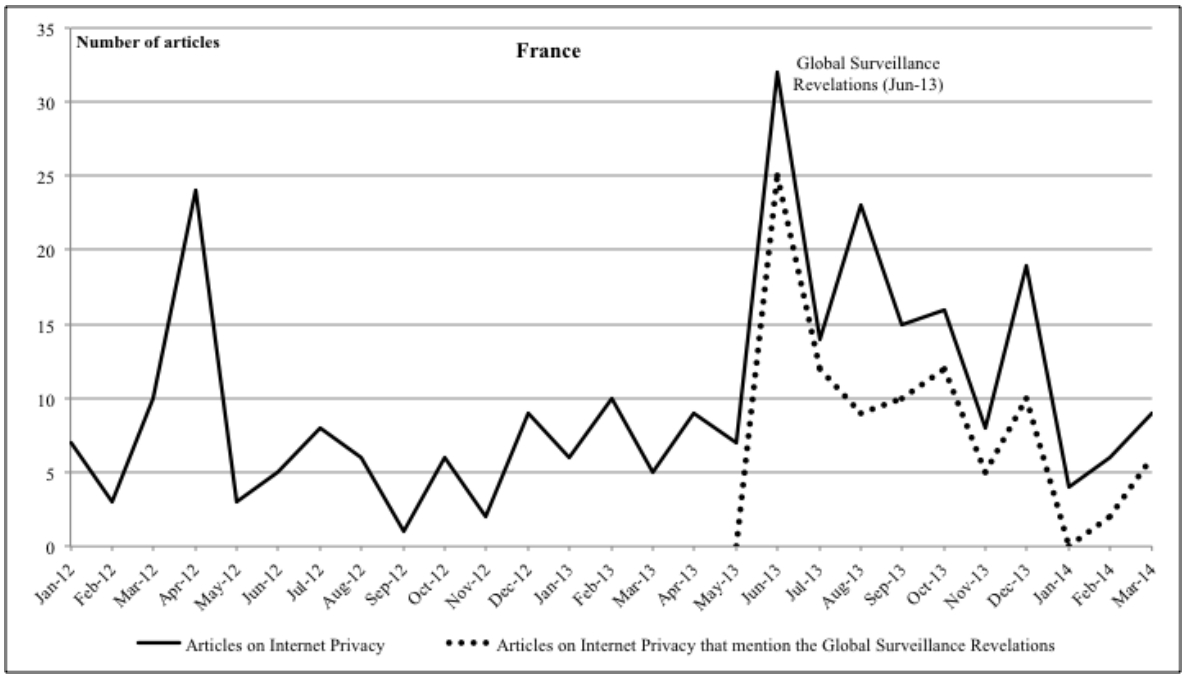
While the theoretical contribution of this piece to the field of corporate power is modest, as a demonstration of yet another case of corporations more likely to win policy debates under low salience scenarios, there is a clear contribution to the field of European privacy leadership. Concretely, this piece has shown that DPA's need high salience scenarios to maintain a meaningful grip in European policy making and to contribute to strengthening European privacy rules –in 1995 DPAs created a high floor for the level of data protection in the EU but lost the tool to raise the ceiling, since they could not threaten to block the European personal data single market. The GDPR case showed how DPAs needed two advocates to impose their preferences: Snowden to raise the salience of Internet privacy debates across the EU, and Albrecht to lead and direct a privacy strengthening approach in the EP.

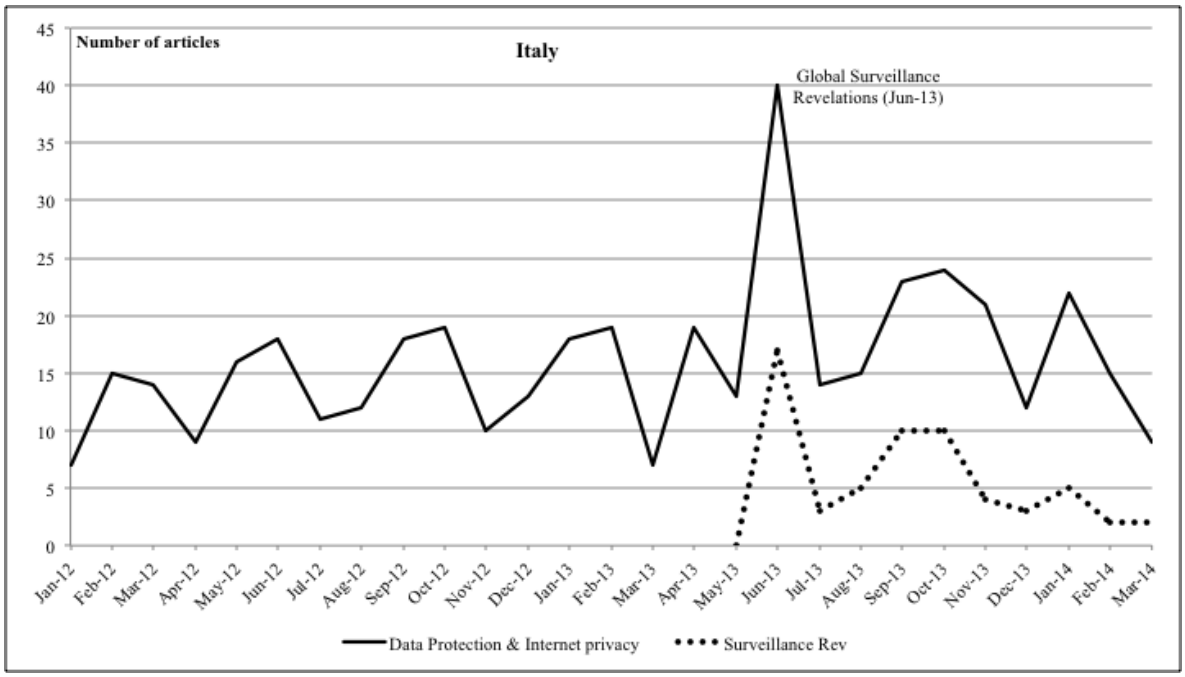
Lastly, by analyzing the evolution of the salience of Internet privacy issues in European media and its impact on the GPDR this article has contributed to measure one of the tangible consequences of the Global Surveillance Revelations started by Edward Snowden in the summer of 2013. As it was shown, the GDPR approved by the EP in first reading would very probably not be privacy strengthening in absence of the role of Snowden as a pro-privacy and anti-surveillance activist. Further research should explore the tangible impact of the Global Surveillance Revelations in other areas of policy making worldwide, and analyze the evolution of the GPDR debate and its future implementation.

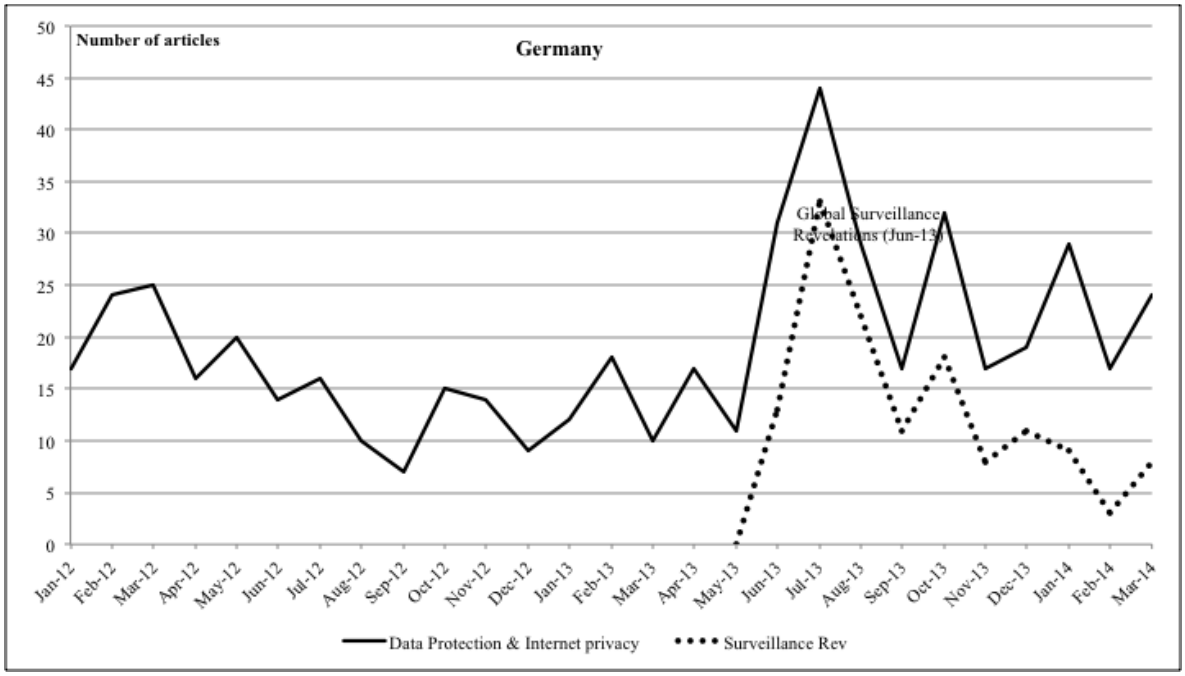
Annex I


Number of articles
United Kindgom
Global Surveillance Revelations (Jun-13)
35
30
25
20
15
10
5
0
Jan-12
Feb-12
Mar-12
Apr-12
May-12
Jun-12
Jul-12
Aug-12
Sep-12
Oct-12
Nov-12
Dec-12
Jan-13
Feb-13
Mar-13
Apr-13
May-13
Jun-13
Jul-13
Aug-13
Sep-13
Oct-13
Nov-13
Dec-13
Jan-14
Feb-14
Mar-14
Articles on Internet Privacy
Articles on Internet Privacy that mention the Global Surveillance Revelations


Number of articles
Spain
Global Surveillance Revelations (Jun-13)
45
40
35
30
25
20
15
10
5
0
Jan-12
Feb-12
Mar-12
Apr-12
May-12
Jun-12
Jul-12
Aug-12
Sep-12
Oct-12
Nov-12
Dec-12
Jan-13
Feb-13
Mar-13
Apr-13
May-13
Jun-13
Jul-13
Aug-13
Sep-13
Oct-13
Nov-13
Dec-13
Jan-14
Feb-14
Mar-14
Data Protection & Internet privacy
Surveillance Rev


Number of articles
France
Global Surveillance Revelations (Jun-13)
35
30
25
20
15
10
5
0
Jan-12
Feb-12
Mar-12
Apr-12
May-12
Jun-12
Jul-12
Aug-12
Sep-12
Oct-12
Nov-12
Dec-12
Jan-13
Feb-13
Mar-13
Apr-13
May-13
Jun-13
Jul-13
Aug-13
Sep-13
Oct-13
Nov-13
Dec-13
Jan-14
Feb-14
Mar-14
Articles on Internet Privacy
Articles on Internet Privacy that mention the Global Surveillance Revelations


Number of articles
Italy
Global Surveillance Revelations (Jun-13)
45
40
35
30
25
20
15
10
5
0
Jan-12
Feb-12
Mar-12
Apr-12
May-12
Jun-12
Jul-12
Aug-12
Sep-12
Oct-12
Nov-12
Dec-12
Jan-13
Feb-13
Mar-13
Apr-13
May-13
Jun-13
Jul-13
Aug-13
Sep-13
Oct-13
Nov-13
Dec-13
Jan-14
Feb-14
Mar-14
Data Protection & Internet privacy
Surveillance Rev


Number of articles
Germany
Global Surveillance Revelations (Jun-13)
50
45
40
35
30
25
20
15
10
5
0
Jan-12
Feb-12
Mar-12
Apr-12
May-12
Jun-12
Jul-12
Aug-12
Sep-12
Oct-12
Nov-12
Dec-12
Jan-13
Feb-13
Mar-13
Apr-13
May-13
Jun-13
Jul-13
Aug-13
Sep-13
Oct-13
Nov-13
Dec-13
Jan-14
Feb-14
Mar-14
Data Protection & Internet privacy
Surveillance Rev

III. Article 2: Why does America not have a comprehensive privacy regime?

Why does America not have a comprehensive privacy regime? The most common, obvious, and prevalent explanation of why America does not have a comprehensive privacy regime is that of the liberal traditions theory: comprehensive privacy legislation is against America's political culture, since Americans are more individualistic than other nations, resistant to accept state intervention in their society, and unwilling to let the government intervene in the private market.

In this article I demonstrate that the prevalent liberal traditions explanation is over-simplified and wrong since it fails to explain that polls show that Americans support the increasing role of government in the protection of privacy from private sector invasions, and the surveillance state that emerged after the 2001 terrorist attacks.

Instead, I use an institutional approach that considers ideas and institutions as interdependent variables to explain that the interpretation of two critical conjunctures in recent American history shaped institutions and policies in a way that took comprehensive privacy reform as a casualty. First, the collapse of the Bretton Woods system, effective in 1973, marked the beginning of a deregulatory wave in American politics that makes the enactment of regulation and regulatory institutions like the ones required by a comprehensive privacy regime less likely. Due to external shocks, by the end of the 90s some American institutions, namely the Federal Trade Commission, had started drifting away from their original purpose and advocating for comprehensive privacy regime within the existing policy paradigm. Second, in response to the 9/11 attacks, the American political system values security over civil rights such as privacy, rendering then the enactment of a comprehensive privacy regime impossible once again.

Introduction

In 1999 the CEO of Sun Microsystems, Scott McNealy, controversially said: "You have zero privacy anyway. Get over it" (Sprenger, 1999). Today, under the light of the many revelations triggered by whistleblower Edward Snowden's leaked documents (Glenn Greenwald, 2014), McNealy´s statement seems not only indisputable but also indubitably well informed. Modern data collection and processing is so formidable that Google knows before you do where you want to go for holidays, the super-store Target can figure out when a young woman is pregnant by analyzing her shopping habits (Duhigg, 2012), and intelligence agencies of both the United States and the European Union, such as the American National Security Agency (NSA), the British Government Communications Headquarters (GCHQ), the German Federal Intelligence Agency (Bundesnachrichtendienst), or the Danish Security and Intelligence Service (Politiets Efterretningstjeneste**)**, are potentially tracking every move of any given citizen by collecting and processing each step of our ever bigger digital footprints (Gallagher, 2014; Glenn Greenwald, 2014). In fact, due to the many revelations of massive state surveillance, for the first time in almost a decade a majority of Americans are more concerned about their civil liberties than about terrorism (Pew Research Center, 2013).

By now, perhaps the reader has learned that America does not have a comprehensive privacy regime and instead has what has been often called a patchwork of protections (i.a. Colin J. Bennett, 1992; Flaherty, 1992; A. Newman, 2008; Regan, 1995). Yet, the reader probably will be surprised to know that not only is the United States the only advanced nation without a comprehensive privacy regime, but also that out of 89 nations with some kind of privacy law, the United States and Thailand are the only countries with laws that do not cover the private sector (Greenleaf, 2012). As a consequence of the lack of a comprehensive regime, and according to a 2010 green paper of the United States' Department of Commerce on privacy and the Internet economy, Silicon Valley corporations "operate without specific statutory obligations to protect personal data"(2010b).

But why does America not have a comprehensive privacy regime? The most common, obvious, and prevalent explanation of this case of "American Exceptionalism" is

the Liberal Traditions explanation originally suggested by Alexis De Tocqueville (2004). According to that explanation, comprehensive privacy legislation is against America's political culture, since Americans are more individualistic than other nations, resistant to accept state intervention in their society, and unwilling to let the government intervene in the private market (i.a. Drezner, 2004; Strauss & Rogerson, 2002; Swire & Litan, 1998; Whitman, 2004). Thus, Regan, for example, argues that "the formulation of privacy policy in the United States has been profoundly shaped by its liberal traditions emphasizing individual rights and a limited role for government" (Regan, 2008, p. 74).

While I do not argue that American 'Liberal Traditions' do not affect political outcomes, I argue that to rely solely on this line of analysis is over-simplified and in the end, wrong. Most obviously, because it fails to explain the surveillance state enforced after the terrorist attacks of 2001; the sustained support for government protection of privacy as evidenced in various opinion polls; that in the 1960s American policy makers worked on privacy issues because they were alerted by the proposed creation of a National Data Center with a centralized computerized inventory accessible by a number of Federal agencies (Colin J. Bennett, 1992; Hanus & Relyea, 1975; Regan, 2008); and why it fails to explain that by the 1970s "[a]lmost every [privacy] issue that arose in Europe was also an issue in the United States, but at an earlier time and on a more dramatic scale" (Hondius, 1975, p. 6).

Instead, drawing upon the work of Blyth (2002, 2011) and Steinmo (2003), I offer an institutionalist account that considers ideas and institutions as interdependent variables to explain the American privacy framework. I explain how and why the resulting and institutionalized policy paradigms that emerged in response to the crises of 1973 (the collapse of the Bretton Woods system, that resulted in the deregulatory paradigm) and 2001 (the 9/11 terrorists attacks, that created the surveillance state paradigm) biased American politics and institutions against comprehensive privacy reform. I interpret privacy policies in their wider historic and institutional context to explain why privacy reform has failed in the United States. The argument, in short, is that concrete policies cannot be understood outside of the overarching policy paradigm in which they function. For policy paradigm we understand the ideas that structure the thinking about what is possible and desirable in a policy domain, for overarching policy paradigms we understand the ideas that structure the thinking about what can and should be in done in a

political system as a whole. Privacy policies, like all policies, were constructed in overarching policy paradigms that, within a certain institutional framework, determined what was possible and desirable for policy makers, and that were biased against comprehensive privacy reforms.

In sum, the theory I propose for explaining the lack of a comprehensive privacy regime in the United States is that a quasi-necessary condition for the materialization of concrete policy proposals is that they are perceived as possible and desirable within the dominant policy paradigm in which they operate. The further away a policy proposal is perceived from the limits of a dominant policy paradigm, the less likely its success will be since it will have few supporters. Hence, a policy proposal that goes against a dominant policy paradigm will have a very low chance of being able to overcome political processes without first having to reform the dominant policy paradigm itself. Therefore, in order to determine why a certain policy proposal failed one should first identify the overarching policy paradigm in which it operates and how the proposal aligns or not to it.

But couldn't the liberal traditions be a grand-overarching policy paradigm of American politics? While it would be possible to operationalize some of the liberal traditions values, such as antistatism and individualism, as part of a policy paradigm –for example through a policy paradigm that perceives state intervention in the market as undesirable or impossible—that would have three important limitations. First, empirically American politics and policies have moved away from what a liberal traditions policy paradigm would predict for many moments of its history. For example, America has a big social security system and a surveillance state. Second, and in consequence, policy innovations outside of a liberal traditions policy paradigm would remain unexplainable. Third, the liberal traditions argument claims to be able to explain America since its conception and as such it cannot be divided in periods, since that would eliminate its fundamental claims.

Since the 1960's frustration grew on both the American left and the right over regulatory capture by businesses. Precipitated by the collapse of the Bretton Woods System, the Watergate scandal in 1972, and the resignation of Nixon, American policy trends began a *de*regulatory wave, making comprehensive regulation and the creation of independent federal agencies even *less* likely than before—as historic institutionalism has

shown, fragmented American political institutions intrinsically make the enactment of comprehensive reform more difficult than in other developed nations (i.a. Steinmo, 1996; Steinmo & Watts, 1995; Weir, 1992). As a consequence, the 1974 Privacy Act, signed into law by President Gerald Ford, does not create a comprehensive American regime as originally designed and proposed by the main sponsor of the Act, Senator Ervin. By the 1980s, America experiences an acceleration and further institutionalization of the general deregulatory wave from the left and the right. Because of the Clinton Administration's belief that the Internet should be left untouched, comprehensive privacy regulation remained off the table in the 1990s, which continued into post-2001 America because of a major national concern over national security.

This article is structured as follows. First, there is an overview of the liberal traditions accounts for the American privacy framework. Second, I discuss the liberal traditions explanation and the historical institutionalism framework. Following, a liberal traditions reading of the 1974 Privacy Act process is presented and discussed in detail. As with all public debates, the privacy debate in America did not take place in a vacuum. Therefore, I then challenge the liberal traditions explanation by introducing the importance of considering the privacy debate within the two predominant policy paradigms of American politics since the 1970s: first, from 1973 to 2001 the deregulatory paradigm, and then the national security paradigm, from 2001 to today. A conclusion closes this piece.

Liberal traditions accounts of the American privacy regime

The liberal traditions theory that fundamentally refers to political liberalism has been directly used to explain why the United States does not have a comprehensive privacy regime. In fact, the liberal traditions theory dominates the accounts for the American privacy framework.

In "The Global Governance of the Internet: Bringing the State Back In", Drezner argues that since the "U.S. attitude toward privacy rights is based on freedom from state intervention, […] there was no push in the United States for comprehensive regulation of data privacy" (2004, p. 486). Similarly, Regan reasons that "the formulation of privacy policy in the United States has been profoundly shaped by its liberal traditions

emphasizing individual rights and a limited role for government" (2008, p. 74), and "[t]his has meant first that the emphasis has been on achieving the goals of protecting the privacy of individuals rather than curtailing the surveillance activities of organizations or of the state"(2008, p. 75).

However, like Bennett, Regan adds that privacy debates in the United States are triggered by public attention but limited by the influence of corporations and other actors opposing privacy (Colin J. Bennett, 1992; Regan, 2008). Oddly, neither Regan or Bennett explain why in a nation where people care about their privacy, legislators present legislation, and there are frequent outbursts of public attention to privacy invasions, comprehensive privacy protections are never enacted, or why corporations have always been successful in advancing their interests.

Swire and Litan consider that to American sensibilities a comprehensive privacy regime "might easily seem an unnecessary regulatory intrusion in how an organization should manage its own information" (1998, p. 178). Likewise Strauss and Rogerson argue that "historically, Americans have been more concerned with government violations of privacy than with private sector intrusions" (2002, p. 175). In the same tone, Pearce and Platten state that Americans "are cautious about supporting federal data protection legislation, unless they are convinced that the risks involved are indisputable and there is genuine evidence of market failure" (1998, p. 2036).

Comparing America to Europe, Fromholz considers that America will never adapt a comprehensive regime like the European since "[t]he relatively narrow scope of U.S. privacy law, based as it is on the Constitution and cultural mores, seems unlikely to change in the near future" (Fromholz, 2000, p. 471). Likewise, in "The Two Western Cultures of Privacy: Dignity versus Liberty", Whitman argues that since America did not experience fascist state intrusion like Europe, and giving their anti-statist culture, Americans have a completely different approach to privacy that focus on the intrusions from the state (2004). However, as Newman demonstrates, comparisons with Europe fail to explain why state intervention is the explanatory variable in the different approaches regarding privacy protection in the private sector between the European Union and the United States. America, after all, did experience the perils of state intrusion with McCarthyism and Watergate and has legal safeguards against governmental privacy

violations (2008, p. 52). It is also unclear under the liberal traditions historical narrative why Europeans would enact public privacy protections against private actors creating powerful public agencies if they are afraid of the government. The static cultural narrative fails any in-depth analysis and tends to oversimplify reality.

In sum, like Steinmo and Watts would say, the American political culture is exceptional and unique but "just as Swedish, Japanese, or French political cultures are unique" (1995, p. 333). Understanding culture is certainly necessary to understand a certain policy outcome. But, I demonstrate, it is not that American political culture is anti-privacy, but that the prevalent overarching policy paradigms of American politics from the 1970s on have been biased against comprehensive privacy reform.

Policy paradigms

Assuming that Americans do not want comprehensive privacy laws and that they prefer the government away from their business, is comforting for the theory of America as an exceptionally liberal land (Lipset, 1971, 1979, 1997; Tocqueville, 2004). In fact, under a superficial analysis, the liberal traditions theory explains the American privacy regime very well: in essence, privacy protection in America tries to limit government intrusions in personal life first and foremost, and deals with private invasions of privacy as an afterthought.

The liberal traditions explanation for the lack of a comprehensive privacy regime in the United States is both plausible and logical: America is a nation founded by immigrants escaping oppressive governments. As it is often, many of those immigrants were the most entrepreneurial and individualistic members of their original societies. Thus, the nation they built is more individualistic, anti-statist, and anti-interventionist than any other nation (i.a. Hartz, 1991; Lipset, 1971, 1997). In fact, as King put it: "the State plays a more limited role in America than elsewhere because Americans, more than other people, want it to play a limited role" (1973, p. 418)

Following Tocqueville (2004), perhaps the first liberal traditions theorist, Lipset has argued, in a series of books running back to his early works (1971, 1979), that America's unique culture of democratic egalitarianism and individualist achievement,

makes it clearly identifiable as an outlier on a comparative international scale of values and has permanently affected the United States history (1996). However, Lipset, as the other liberal traditions theorists, fail to explain why the United States has adopted some institutions that are similar to those of advanced nations like a comprehensive healthcare system, a large social security system, or a surveillance state, institutions that were once considered to be essentially un-American. Lipset has recognized that "major changes have occurred which have modified the original American Creed, with its suspicion of the state and its emphasis on individual rights. These include the introduction of a planning-welfare state emphasis in the 1930s, accompanied initially by greater class-consciousness and trade union growth, and the focus on ethnic, racial, and gender group rights which emerged in the 1960s" (Lipset, 1996, p. 289). Yet, despite Lipset's acknowledgement of changes in American political culture, the liberal traditions explanation fails to explain why changes take place, and why change takes a certain shape and not another.

As Steinmo has pointed out, using a static cultural explanation like the liberal traditions poses three severe analytical issues. First, the liberal traditions explanation fails to explain or account for political change. Second, political cultures consist of a mix of often contradictory or competing ideas, hence liberal traditions theory fails to provide a convincing explanation of why the dominant political culture might change in certain times or in certain arenas. Finally, proponents of the liberal traditions approach usually are quite vague about the casual mechanisms of culture as an independent variable (Steinmo, 1994, p. 107).

Instead, I propose using an institutionalist approach that treats ideas and institutions as interdependent variables, since neither ideas nor institutions alone are sufficient to understand the trajectory of American privacy policy from 1974 to today (Lieberman, 2002). Following Blyth (2011), I explain that ideas are fundamental to explain institutional change since they function as blueprints during periods of uncertainty, as weapons to restructure existing institutional arrangements, and as cognitive locks that reinforce existing institutions during the "itineration of a policy game" (Steinmo, 2003, p. 207). To that, I add the importance of considering that history is non-linear and that it evolves in unpredictable ways according to how agents react to changes in their environment, institutional and ideological. In other words, by analyzing the evolution of ideas *and* institutions from an agent-centered perspective, this analysis breaks

free from the narrative fallacy trap of the liberal traditions account.

Considering ideas as blueprints explains why after a period of crisis of an established institutional equilibrium, a new equilibrium emerges in the specific form that it does. Ideas reduce uncertainty in situations which agents cannot anticipate the outcome of a decision and make institutional change possible. This is not rendering agents interests irrelevant, but highlighting that in conditions of uncertainty agents might not know where their best interests are and, hence, which institutions would best serve those interests (Blyth, 2002, p. 4).

Once used as blueprints for *new* institutional arrangements, ideas can also be weapons to restructure existing institutional arrangements by defining the solutions to the identified problems of the new policy itineration (Blyth, 2011).

Much like traditionally defined institutional path dependence (P. Pierson, 2000), ideas can act as *intellectual* cognitive locks that define and frame the limits of policy making in a period of time. Therefore, policy continuity in periods of environmental change can be a product of institutional arrangements or a product of an ideational cognitive lock that impedes agents from not only entertaining but even considering alternative policies (Blyth, 2011).

This article traces the development of the American policy paradigms in the last decades using a historical narrative primarily illustrated by the relevant manifested political preferences of American Presidents since the 1970s until today. Policy paradigms are understood as the "framework of ideas and standards that specifies not only the goals of policy and the kind of instruments that can be used to attain them, but also the very nature of the problems […] meant to be addressing" (Peter A. Hall, 1993, p. 279). To Hall's definition I add that when thinking of policy paradigms one should be permanently aware of the interdependent relationship between ideas and institutions: first, ideas become dominant paradigms not simply because of being compelling on its own terms, but because in a certain period of time they become persuasive expression among actors whose institutional position gives them both the motive and the opportunity to translate it into policy (Lieberman, 2002). Second, existing institutional arrangements and the historical learning from its consequences condition which ideas emerge, which ideas can even be considered (Weir, 1992) and even which ideas survive as predominant through

time (Berman, 2013).

I chose to concentrate my narrative in the manifested political preferences of Presidents for their capacity to set a political agenda, their powerful institutional role**,** and also for how they synthesize a general political trend of the nation –people usually vote what they want to hear. I use media and literary citations, interviews, and analyze the change, or lack thereof, that each policy paradigm brought regarding privacy policy in America. It is important to keep in mind that the President is part of a general environment in which certain ideas are more dominant than others. However, by paying attention to the presidency, usually a reflection of policy paradigms, we can understand precisely how policy paradigms evolve.

In the following sections I first present a liberal traditions reading of the 1974 Privacy Act debate, the centerpiece of legislation of the American privacy framework. I then present the deregulatory policy paradigm that dominated American politics during the 1974 Privacy Act debate, which, as I explain, critically conditioned the resulting legislation and the American privacy framework. Finally I trace the evolution of the American policy paradigm and explain why it was constantly biased against comprehensive privacy reform, spite sustained public concern. Thus, the fact that America privacy regime is a patchwork of protections is better understood as the result of the tension between demands for privacy by the public in policy paradigms that reject comprehensive privacy reform.

The 1974 Privacy Act explained under the Liberal traditions argument and its limitations

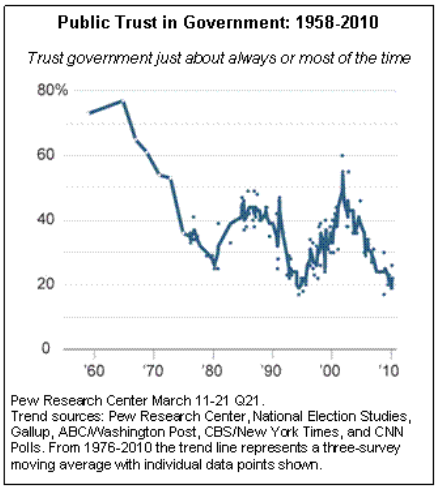
It is certainly easy to build the elements for a liberal traditions narrative that explains the lack a comprehensive privacy regime in the United States. After all, at first glance it is true that Americans have very clear rules for being protected from the State, and in contrast, American privacy protection regarding the private sector is sector specific and not generalized (i.a. A. Newman, 2008; Regan, 2008)**.** While privacy rights in America are not granted by the Constitution, their origins can be traced to the Fourth Amendment and the right against unlawful searches and seizures. This right, which makes Americans masters in their own homes and forbids the state from invading it, has then matured into a

far-reaching right against state intrusion into people's lives (Whitman, 2004, p. 1212).

Under the liberal traditions argument, and taking as a fundamental premise that Americans privacy actions are triggered by fear of government invasions, it is not surprising that the first specific, and now central, law that regulates privacy protection in America, the 1974 Privacy Act, is a result of the Watergate scandal. In response to the exposure of the Nixon administration's abuse of state power to spy on the President's political opposition, the US Congress enacted a law limiting what Federal Agencies can do with personal information. As data collected by the Pew Research Center shows, public trust in the Government had been declining since 1965, but it collapsed even more rapidly in 1972, the year when the Watergate scandal initiated (Petrison & Wang, 1995, p. 23). Since then, with the exception of 2001, never has a majority of Americans trusted the Federal Government (Pew Research Center, 2010, p. 13).

The 1974 Privacy Act establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals maintained in systems of records by federal agencies. The Privacy Act has four basic provisions. First, government agencies are required to show an individual any records kept on him or her. Second, agencies are required to follow "fair information practices" to gather and handle personal data. Third, agencies are banned from the unrestricted sharing of someone's data with other people or agencies. Fourth, citizens can sue the government for violating any of the three provisions.

Figure 5 Public Trust in Government 1958 - 2010



Thus, under the predominant liberal traditions narrative, the Privacy Act reflects the cultural consensus of the Watergate scandal days (Rule & Greenleaf, 2010, p. 5) and came to validate the liberal traditions theory: Americans consider that one should be careful of what personal information the government might have. Under this understanding of history, the liberal traditions explanation can be certainly accurate: Americans do not have a comprehensive privacy regime because, as the 1974 Privacy Act shows, Americans only care about government surveillance. As Newman has pointed out, superficial evidence, that I prove wrong in the following pages, shows that even a central consumer rights advocate such as Ralph Nader did not campaign for comprehensive privacy legislation because of not considering it important (A. Newman, 2008). In consequence, all the subsequent privacy legislation has been in response to particular events.

Yet, the liberal traditions reading of events fails to explain the surveillance state that emerged after the 2001 terrorist attacks. Nor does it recognize that the Senate Bill that would become the 1974 Privacy Act, S3418, proposed creating a Federal Privacy Board, mandating the application of all the provisions of the Act to not only the public sector but the private sector as well, and would have have created an American privacy system similar to those prevalent in the rest of the world.

The liberal traditions argument also fails to incorporate the fact that public opinion has for many years been in favor state intervention to protect privacy. A 1977 survey by Louis Harris and Associates shows that 75% of Americans considered that it was important for the government to enact legislation similar to the 1974 Privacy Act that would "lay down rules for the way *business and other private organizations* should deal with information they have collected about their customers, employees and other individuals" (Louis Harris and Associates, 1997); between 1974 and 1980 more 70% of Americans supported an increasing government role in the protection of privacy (Katz & Tassone, 1990); and a 2013 survey showed that 65% of Americans think that current laws are not good enough in protecting people's privacy online (Rainie, Kiesler, Kang, & Madden, 2013). It is also important to keep in mind that various polls show that the American people have been highly concerned about their privacy throughout time (i.a. Harris Interactive, 1999; Louis Harris and Associates, 1992, 1998; Penn Schoen Berland, 2014; Roberts, 2005).

Thus, to understand why America does not have a comprehensive privacy regime, it is important to keep in mind that the 1974 Privacy Act is the truncated version of a Congressional process started in the 1960s to regulate public and private data collection and usage happening during a specific period of time. In America, like in other developed nations, there has always been concern about private data collection and usage, even if that concern has never materialized in a comprehensive legislation. And in the United States, the comprehensive legislation has never materialized, I argue, because of two fundamental and complementary policy paradigm shifts that took place in America since the 1970s.

The first paradigm I discuss is the deregulatory paradigm born at the beginning of the 1970s that explains why a comprehensive privacy reform was unlikely to be approved with the passage of the Privacy Act in 1974. The crisis of the post-World War II world order gave room and enabled the emergence of a deregulatory policy paradigm, in which policy-makers started interpretation that new regulatory institutions and burdens were not desirable and instead preferred to deregulate the economy. As a consequence, during the prevalence of the deregulatory policy paradigm, policy proposals that are perceived to be a regulatory burden have a small base of support by policy makers and start confronting anti-regulatory institutions. As it is expected by the policy paradigm argument, a comprehensive privacy reform could not pass during this period. The power of this policy paradigm is clearly illustrated when considering that before its consolidation, the American political institutions passed comprehensive reform and created several regulatory institutions, like the Environmental Protection Agency (EPA) and the Occupational Safety and Health Administration (OSHA), and in contrast since its consolidation that kind of reform has been almost impossible.

The second policy paradigm that occupies the following pages emerged as a result of the 9/11 terrorist attacks, and made it very unlikely to pass policies perceived as threatening or limiting national security or national security defense capabilities. 9/11 made a comprehensive reform of the American national security apparatus possible and created a policy paradigm that rejects all policy proposals that are perceived to threaten or limit the American defense capabilities. Again, the policy paradigm argument predicts and explains why comprehensive privacy reform did not happen in this period.

At this point it should be noted that the liberal traditions argument could explain why there is no comprehensive privacy reform during 1974 to 2001 (period of the deregulatory policy paradigm). However, the liberal traditions argument fails to explain the expansion of regulatory institutions in the post-World War II policy paradigm, and the creation of a surveillance state after 2001. As predicted, the liberal traditions argument fails to explain political change (Steinmo, 1994, p. 107).

First Paradigm: Privacy in the deregulatory shift

By the end of the 1960s, the world order established in the aftermath of World War II began to break down both domestically and internationally. The gold standard, used as a metallic base of international money, was abandoned and, from 1970 onward, exchange rates were allowed to float. The International Monetary Fund had to bail out Great Britain in 1975, and unemployment and inflation were surging everywhere, placing the world in a much-feared phase of 'stagflation' that lasted for much of the 1970s (Harvey, 2005). The Bretton Woods system of monetary management, which had established the rules for commercial and financial relations among the most developed nations since 1954, was exhausted and no longer working (i.a. Harvey, 2005; Hughes, 2005; Varoufakis, 2011).

One strategy for responding to the collapse of the Bretton Woods system was tightening regulation and state intervention in the economy with corporatist alliances between state, labor, and capital. This was what countries such as the Scandinavians for example did as a first response to the systemic crisis of the Bretton Woods model (Harvey, 2005). In the United States, the first reaction by the political system in the early 1970s was legislating regulatory reform, signed into law by Richard Nixon. Thus, it is in the early 1970s when key pieces of legislation and regulatory institutions are created, such as the Occupational Health and Safety Act, which creates the OSHA, and the EPA (Eisner, 2000, p. 153). This response however was not enough to save the system that was falling apart. With rising energy prices, queues at petrol stations, and factories suspending production due to lack of raw materials or electricity, "new setting emerged in which all prior deals were off" (Varoufakis, 2011, p. 104), and ideas that had been growing in the previous decades found their moment. As a consequence, the era of regulation as the answer for the

days' social and economic problems ended alongside Nixon's Presidency (Eisner, 2013; Harvey, 2005; Prasad, 2006; Varoufakis, 2011).

The uncertainty created by the collapse of the Bretton Woods system at the beginning of the 1970s was a perfect moment for the emergence of an alternative to the economic and social model dominant since the Second World War, a model heavy (even in America) with state intervention in the economy. At this point, it is important to consider that possibility of change, does not necessarily equal change: had an alternative to the existing model not existed, or had the American political institutions not allowed for the adoption of such alternative, it is plausible that the existing model would have remained even if discredited and weakened. For example, neoliberalism still dominates our current understandings of politics and the economy even after the Great Depression, in absence of conceivable alternatives (Berman, 2013, p. 12).

But, by the end of the 1960s a possible alternative to re-launch the economy was devised, and consisted in going to the other way, and having *less* state intervention in the economy and *less* regulation of the market. That movement, from regulation to *de*regulation, has been usually attributed to the political right, especially in contemporary public debate. What is interesting about the deregulatory movement, however, is that *de*regulation was not grand-plan of the rich and powerful coming from the right, but that the *de*regulatory movement starts as an institutional blue-print from both the left *and* the right (Prasad, 2006).

In the post-war period, economists and social scientists across the political spectrum started arguing that economic regulatory agencies were almost inevitably captured by the business they were supposed to regulate: daily contact, revolving doors and mutual interests created a system in which regulation functioned to benefit industries instead of consumers (Prasad, 2006, p. 66). That intellectual discussion contributed to building a new policy paradigm in American politics in favor of deregulation. For example, Friedrich von Hayek's Mont Perelin Society, which included notables as Ludvig von Mises, Milton Friedman, and even, for a time, Karl Popper (Harvey, 2005, p. 20) argued in its funding statement of 1947 for the need of "the redefinition of the functions of the state so as to distinguish more clearly between the totalitarian and the liberal order"(Mirowski & Plehwe, 2009, p. 25). And it is in 1962 when Friedman, who would

become one of the popes of neoliberalism, publishes for the first time his seminal *Capitalism and Freedom* (2009). There, Friedman argues that "regulatory agencies often tend themselves to fall under the control of the producers and so prices may not be any lower with regulation than without regulation" (Friedman, 2009, pp. 128–129).

From the other side of the aisle, in 1961 Gabriel Kolko, a historian from the New Left generation, publishes *The Triumph of Conservatism* – a critical reassessment of the progressive era in which he argues that major American businesses not only did not oppose many of the regulatory acts from 1900 through 1916, what is known as the Progressive Era, but actively sought and supported many reforms and regulations (Kolko, 2008). Also from the left, Grant McConnell argues, in *Private Power in American Democracy* (published in 1966), that much legislation designed to provide regulation based on the progressive view of the public interest is in fact administered with the interests of only a very few being served (McConnell, 1966). In sum, before the material collapse of the Bretton Woods system there were intellectual elements feeding and building up arguments to the left and the right about the need to stop regulatory capture (i.a. Carpenter & Moss, 2013; Friedman, 2009; Kim & Law, 2009; Kolko, 2008; McConnell, 1966).

Thus, when deregulation consolidates as the policy paradigm of the American political stage, it does not do so as the *free-market* neoliberal platform that we think about today. When deregulation consolidates as the policy paradigm of American politics in the 1970s, it does so as a movement seeking to prevent government from giving an unfair advantage to business over consumers (Prasad, 2006, p. 66). That logic explains the support of the progressive side and the consumer movement to deregulation: the left believed that it was in the best interest of the people to stop government from enacting regulation and creating regulatory agencies, which they believe protected corporations. Senator Ted Kennedy, President Jimmy Carter, activist Ralph Nader, and regulation expert Alfred Kahn, all self-described liberal democrats or progressive activists, where active supporters of deregulation (i.a. Eisner, 2000, 2013; Lynn, 2000; McCraw, 2009; Prasad, 2006). It should be noted that while neo-liberalism has embraced deregulation as part of its agenda, deregulation transcended ideological barriers for a brief period of time and this is why it is important to consider them as two distinct phenomena.

Alfred Kahn, Carter's head of the Civil Aeronautics Board (CAB) from 1977 to 1978 argued in a discussion with a member of the Airline Pilots Association that "I'm anti-excessive government interference […] particularly against government being used to protect powerful business interest […] lower prices introduced by more competition mean *more* jobs, not fewer" (in McCraw, 1994, p. 288). Similarly, in October of 1975, none other than the Chairman of the Federal Trade Commission, Lewis Engman, said "Most regulated industries have become protectorates, living in a cozy world of cost-plus, safely protected from the ugly specters of competition, efficiency and innovation" (UPI, 1975).

Far from being isolated in his demands in the progressive side, Kahn and Engman's arguments resonated with advocacy groups such as the ACLU and Common Cause, that one can hardly accuse of being neo-liberal (Wolfe & NewMyer, 1985, p. 59). In fact, none-other than Ralph Nader, father of the consumer protection movement in America, founder of Public Citizen, and four-time Presidential candidate, was among the first advocates of the abolition of the CAB, perfectly illustrating the *de*regulatory position of the pro-consumers movement. In a written statement to the Oversight of Civil Aeronautics Board Practices and Procedures in 1975 Nader wrote:

> *"In my view, the time has come to face up the fact that this aberrational experiment in controlling airlines through governmental regulation is a demonstrated failure. In short, the Civil Aeronautics Board should now be abolished […] Throughout the land,* ***people are repulsed by arrogant and unresponsive bureaucracies no useful for public purpose and they are looking to this Congress to get on with the national housecleaning job that is needed****. Can you think of a better place to start than with the Civil Aeronautics Board?"* (US Senate, 1975b).

Nader was not short of ideas of what agencies to eliminate, and in a roundtable with then California Governor Ronald Reagan organized by the *New York Times* in 1975 Nader was asked by an audience member to name which government agencies and governmental regulations he would eliminate. His answer: "The Maritime Administration, a good deal of the Department of Commerce, a good deal of the Department of Interior, a good deal of the Department of Defense. Portions of the [General Services Administration], I mean we can go on forever" (in Prasad, 2006, p. 75).

Reagan was likely as astonished by the words of Nader as the reader is, and with his usual charisma replied: "Now Mr. Nader responded to the challenge by naming some of the agencies and I thought for a minute there he and I had become blood brothers" (in Prasad, 2006, p. 76). Thus, it is not a surprise that none other but the President of the

National Chamber of Commerce itself, President of State Farm Insurance Company Edward Rust declared in 1973 "Business should be grateful for Ralph Nader. He is single-mindedly committed to making the free-enterprise system work as it's supposed to –to making marketplace realities of the very virtues that businessmen ascribe to the system" (in Pertschuk, 1982, p. 15).

Nader's positioning regarding regulation is particularly important for understanding the outcome of the 1974 Privacy Act debate since he was the leader of the pro-consumerist movement in America in the time (Glickman, 2009, p. 299). Nader, as I show in the next section, was worried about privacy and aware of the privacy debates happening in the 1970s and abstained from advocating for a comprehensive privacy reform because of his stance regarding regulation in America and not because of indifference towards the privacy debate. The perceived failure of the regulatory institutions in a period of uncertainty made Nader subject to the prevalent ideational blueprint, not having yet constructed the ideational alternative that better defined his interests (Blyth, 2011). In fact, 10 years later Nader would say: "Deregulation is a code word meaning no more law and order for corporations" (Sinclair, 1985). But in the mid-1970s, advocating for new regulatory institutions in front of evidence of their failure was unlikely (Weir, 1992)

President Ford, who took office after Nixon's resignation because of Watergate and who signed the 1974 Privacy Act into law, was the first President to interpret the regulatory shift and use the new deregulatory ideas as weapons to reform the preexisting institutions (Blyth, 2011). In a speech before a Conference of the National Federation of Independent Business in June 1975, Ford outlined his position regarding regulation, framing the issue within an obsession with inflation:

> *"Although most of today's regulations affecting business are well-intentioned, their effect, whether designed to protect the environment or the consumer, often does more harm than good. They can stifle the growth of our standard of living and contribute to inflation […] Over a period of some 90 years, we have erected a massive Federal regulatory structure encrusted with contradictions, excesses, and rules that have outlived any conceivable value."* (Ford, 1975, pp. 334–335).

President Ford's biggest contribution to the deregulatory movement was Executive Order 11821 from November 1974 that institutionalized deregulation by requiring all major legislative proposals, regulations, and rules emanating from the executive branch to

include a statement certifying that the inflationary impact of such proposals had been studied. That executive order extended to all regulatory agencies, including the EPA, the FTC, the Federal Communications Commission (FCC), and OSHA. In sum, Ford was effectively using newly developed ideas to cast previous institutional solutions as problems that only could be diagnosed and cured by new deregulatory ideas and institutions (Blyth, 2011). With his initiatives, Ford was creating a new institutional path, which made enacting new regulatory institutions difficult by casting a shadow of doubt on their efficiency even before they existed, and making the enactment of comprehensive reform even more of a challenge.

But even after establishing that there were conceivable alternative ideas to the collapsing post-World War II system, it remains unanswered why the deregulatory ideas materialized as the successful alternatives. The deregulatory ideas could materialize due to two fundamental characteristics of American political institutions. First, since in the United States political parties are diffuse organizations incapable of taking a predictable role as policy innovators (Steinmo & Watts, 1995; Weir, 1992), individual Presidents often have "considerable leeway" in defining issues and policy agendas (Weir, 1992, p. 197). That leeway is perfectly illustrated by Ford, the first and only President and Vice-President without being ever elected to office by the Electoral College[19] that managed to define the issues and agenda of American politics despite his otherwise relatively weak and precarious political situation.

Second, American Presidents are capable of soliciting ideas from different levels of bureaucracy without following strict hierarchies (Weir, 1992, p. 197) and can easily incorporate agents and ideas from the "parapolitical" sphere, including think tanks, research institutions, or the business world (Horne, 2001). Thus, for example, Ford nominated Alan Greenspan as his Chief Economic advisor bringing him, and his pro-markets ideas, from his consulting firm in New York to design America's economic policies (Cannon, 2013, p. 178). In sum, the flexibility of American institutions allow the President to bring ideas and people from outside the bureaucracy and the political mainstream to create new policies, if perceived as necessary.

To sum up, since the present text is not a treaty on regulation, but one on the lack

[19] In 1973 Nixon nominated and the Congress appointed Ford to be vice-president after the resignation of Spiro Agnew, Nixon's original companion in the electoral ticket.

of a comprehensive privacy framework in America, I trust the presented evidence should suffice to convince the reader that the policy paradigm of America during the 1970s, especially during the second part of the decade, was one of *de*regulation. And it is precisely in this highly deregulatory and anti-regulatory environment, in May 1974 to be precise, that Senate Bill S3418, what would become the Privacy Act, is introduced to Congress.

Reassessing the 1974 Privacy Act

The Senate's bipartisan Privacy Bill, S3418, originally would have enacted a comprehensive privacy regime, similar to those that the great majority of the world has today. S3418 mandated the creation of a new regulatory agency, the Federal Privacy Board, overseeing the compliance by both public *and* private institutions to the code of fair information practices of the 1974 Privacy Act, while also establishing the right for individuals to see, amend, and be informed of the files containing their personal information –increasing, then, the regulatory burden on business.

S3418's lead sponsor was Senator Samuel Ervin (D-N.C.), a conservative Southern Democrat, worried that "the more the Government or any institutions knows about us, the more power it has about us" and that "stripped of our privacy, we lose our rights and privileges. The Bill of Rights then becomes just so many words" (US Senate, 1974a, p. 352). S3418's sponsors were seeing clearly the problems that private data collection could crate if uncurbed. Thus one of the co-sponsors of the Bill, Senator Percy (R-Ill), manifested that American society had "reached a time when we must assert control over runaway technology, and protect the individuals 'freedom of privacy' from haphazard abuse. We must shape our tools, lest they shape us" (US Senate, 1974a, p. 356).

Corporations argued against being regulated by a comprehensive Privacy Act, declaring that that there was no concrete evidence of corporate abuse of personal information, that the regulation they were facing was already burdensome, and that they could eventually enact voluntarily personal information practices (Hanus & Relyea, 1975). They even argued that the First Amendment protected corporations' free flow of information between them and their clients (Regan, 2008, p. 56).

Fortunately for the private corporations, their arguments resonated loud and clear in President Ford's ears and were incorporated in the House version of the Privacy Act, which did not regulate the private sector and did not foresee a privacy-regulating agency (Colin J. Bennett, 1992; R. M. Gellman, 1993; Regan, 2008). The general opposition of business to being regulated is reflected in the legislative report to accompanying S3418, from September 26, 1974: "Numerous representatives of private organizations and of business and industry opposed the total coverage of the bill, citing the lack of hearing record, the existing requirements of the Fair Credit Reporting Act, and prohibitive costs of implementing S3418 in the private section without passing on the costs in consumer services. Most indicated support for or lack of opposition to, a commission study of privacy invasions by the private sector" (US Senate, 1974b, p. 20). It is worth revisiting the wording of the legislative report in context: "passing on the costs in consumer services" is easily understood as generating inflation, and "prohibitive costs of implementing" as regulatory burden. In 1974 and 1975 the American political system was decisively trying to fight inflation *and* regulatory burden. Hardly any law that would be inflationary and burdensome would pass. The question, thus, should not be why S3418 did not pass, but *how* could have it *not* failed. The ideas and institutions dominating American policy debate were the kind of reform that a comprehensive privacy framework required.

Fifteen out of the twenty industry lobbies that provided statements to the Senate hearing on the Bill were against the legislation covering the private sector, and none of them directly supported the adoption of it. Thus, the legislative report accompanying S3418 concluded that "statements by private industry representatives have persuaded the Committee that a substantial measure of industry cooperation can be anticipated", and that while "the original version of S3418 would have created a Federal policy board with regulatory powers to investigate and issue cease and desist orders for violations of the Act", there was not "sufficient evidence to support a case for vesting broad regulatory powers in a board charged with administrating the Act" (US Senate, 1974b).

But then, who was in favor of comprehensive legislation, apart from the Senators that sponsored S3418? According to the 1974 Privacy Act hearings, the only advocacy organization that was defending a comprehensive law was the ACLU. In fact, seemingly aware of the isolated position, ACLU's Privacy Project Director Douglas Lea reflects: "There are organizations we thought would have lined up with us –Common Cause and

Ralph Nader-, but they are wary of the issue. They want more disclosure (by government and business), and they seem to think there would be a conflict [between privacy and transparency]"(CQ, 1974) . Elsewhere, that piece of evidence has been presented as proof that Ralph Nader was somewhat indifferent to privacy issues (A. Newman, 2008).

However, Nader's attitude regarding privacy was not ambivalent, nor did Nader lack a profound understanding of the complexities of the privacy debate[20]. By 1970, two years before Watergate and four years before Senator Ervin introduced S3418 to Congress, Nader gave a speech to the Association of Computer Machinery in which he manifested that "people are being alienated by the way national data banks, owned by credit companies, banks, insurance companies, employment bureaus and others are being used and shared," and that the massive accumulation of secret personal data on millions of people was a "perilous threat to civil liberties." In fact, Nader said: "The problem of doing something constructive in this area is that there aren't enough people who care. The stakes are very high in terms of ignoring the whole question" (Fosburgh, 1970). No, Nader was not ambivalent regarding privacy. As we have seen in the previous section, during the period from 1974-1975, Nader was decisively against regulation and the creation of new regulatory agencies. This is what explains Nader's lack of support for comprehensive legislation, and not his disregard for privacy protection.

In that context it becomes easier to understand that for the advocates of a comprehensive privacy reform, even if a compromise, the Privacy Act signed by Gerald Ford was "an important first step" (in Regan, 2008, p. 75). Not because privacy was not a public issue that had the attention of activists or the people, or because corporate opposition was spectacular, but because 1974 was perhaps the pivotal year regarding regulation in the United States. The policy paradigm of American politics in 1974 was changing in fundamental ways: While it would forever remain in the terrain of the speculative, it is arguable that has S3418 been introduced to Congress five or ten years before it was, the story of America's privacy would be different today. But during 1974, proposing that Gerald Ford and the American people that America's cure would come from more regulation was certainly an anathema. Clearly, ultimately it was the Congress that decided not to enact a more stringent Privacy Bill and try to defy the Presidential

[20] As I also confirmed in an interview with a former staffer of Ralph Nader working with him during the early 1970s.

veto. However, what has been explained here is that Congress was also not convinced about the idea of passing Senator's Ervin proposal.

At the same time one must not lose sight that United States political institutions are structurally biased against comprehensive reform (Steinmo & Watts, 1995, p. 330), making it almost impossible. First, no other advanced democracy has so many veto points: a powerful President without formal legislative initiative cohabits with two equally powerful chambers elected in very different ways, and an independent Supreme Court (Persily, 2015, p. 212). This creates a "wealth of opportunities" for mobilizing an opposition (Weir, 1992, p. 193).

Second, a decentralized federal system, and successive reforms to the functioning of Congress since the Progressive Era, have turned politicians into independent political entrepreneurs, undermining the power of political parties (Steinmo & Watts, 1995, p. 330). As a consequence of the bias of American political institutions against comprehensive reform, political actors tend to put together ad hoc coalitions around specific issues. Thus, policies that depend on reforming existing institutions or building new ones are less attractive than those that use existing institutions, bypass existing institutions altogether, or rely on private initiative (Weir, 1992, p. 193).

Yet, in order to avoid determinisms, it is important to consider that the fact that American institutions make comprehensive reform extraordinarily difficult does not mean that comprehensive reform is impossible: the Social Security Act of 1935, EPA and OSHA Acts of 1970, and Dodd-Frank in 2010 are all examples of comprehensive reform passing through the American political institutions. In sum, institutions alone cannot explain a policy outcome –just like ideas alone cannot do it either. To understand why Bill S3418 failed one needs to think about the interaction between the predominant ideas of the changing policy paradigm *and* the institutions regulating the political processes.

Nevertheless, the fact remains that the first step for America's privacy protection had many conditions, that settled the boundaries (Weir, 1992) of privacy policy innovation in the United States –the perception of what was possible and desire to formulate privacy policies (Weir, 1992). First and foremost, the legislation would not apply to the private sector. Second, there would not be any Federal agency in charge of privacy protection. Instead the 1975 Privacy Act created a temporary Privacy Protection *Study* Commission

(PPSC) -that worked from 1975 to 1977- and held some responsibility for developing guidelines and regulations and for providing continuing assistance to and oversight of agency implementation of the Act to the executive Office of Management and Budget (OMB).

The first of the PPSC's 177 recommendations regarding future measures was for the President and the Congress to establish a federal entity such as a Federal Privacy Board or other independent unit. In support of its recommendation for a Federal Privacy Board, the PPSC wrote about the importance of one for the public and the private sector: "in all areas of the public sector the Commission has studied, the need for a mechanism to interpret both law and policy is clear […] There must also be a way of bringing private-sector recommendations for voluntary action to the attention of all the relevant organizations" (United States & Privacy Protection Study Commission, 1977, p. 3). The work of the PPSC came to validate the original demand by the Senate of the need of a Federal Privacy Board. Regarding privacy, it seemed like the way to go was obvious: create a Federal Privacy Board, or some kind of privacy agency that would advance the interest of privacy advocates, or at least keep the debate alive. Yet, that would have to wait almost 20 years more.

The 1980s deregulatory mantra

The 1980s saw a promising start regarding privacy issues. On April 2, 1979, President Carter had announced "sweeping proposals to protect the privacy of individuals" (Carter, 1980, p. 581) which included five pieces of legislation to protect the privacy of medical records, to extend fair information protections to consumer credit, banking, and insurance records, to protect the privacy of records used for research purposes, and to revise the Privacy Act of 1974 (in R. M. Gellman, 1993, p. 228). These "sweeping proposals" however did not constitute a comprehensive privacy reform. Furthermore, Carter rejected the PPSC recommendation of creating a Federal Privacy Board, since he did not think business should carry that burden, and instead assigned the National Telecommunications and Information Administration of the Department of Commerce (NTIA) as the lead

agency on the study of privacy matters and the OMB as responsible for implementing some administrative issues of the Privacy Act.

Although Carter's privacy proposals seemed promising, Carter continued the deregulatory wave started by Ford in creating the Regulatory Analysis and Review Group, and issuing Executive Order 12044 on the "Unnecessary Burdens on the Economy". He also deregulated the CAB, air transportation, railroads, freight trucking, financial services and natural gas (B. I. Kaufman, 2009, pp. 244–248). Carter, after all, signed the Airline Deregulation Act in 1978, that eliminated powers from the CAB, and the Depositary Institutions Deregulation And Monetary Control Act. In short, Carter was cognitively and institutionally locked into thinking and acting within the institutions of the deregulatory paradigm shift, and that explains why he was acting similarly to more conservative leaders. Carter, however, did not consider it necessary to dismantle the few privacy regulatory institutions in the government that were left untouched, that role belonged to President Reagan.

President Ronald Reagan, elected with the mandate of deregulating business and reducing government, reduced the staff members concentrating on privacy matters at the NTIA from 15 to 1 and only enacted one privacy related act, the Video Privacy Protection Act, that protects the disclosure of video rental records (Petrison & Wang, 1995, p. 24). Reagan's attitude regarding privacy protection was to the incredulity of the OECD Director of Privacy Guidelines Project, who declared in in 1984 Congressional hearings: "Shortly after Mr. Reagan took office, the privacy staff at NTIA was dismantled. No one associated with that effort is currently working on privacy-related issues, and most of the staff has left the Government" (United States., 1984, p. 125).

The day after Reagan's inauguration, in which he noted that "government is not the solution to our problem; government is the problem" (Dallek, 1984, p. 63), Reagan established a Presidential Task Force on Regulatory Relief, chaired by Vice-President George Bush, in charge of reviewing all existing regulatory statutes and rules in order to determine which needed to be revised or abolished. All regulatory agencies were mandated to prepare regulatory impact analyses and an office of Information and Regulatory Affairs was created within the White House (Vogel, 2003, p. 247). Reagan also took power away from important agencies such as the EPA and OSHA. In fact,

during Reagan's mandate the budget of the EPA was cut in half and its Office of Enforcement was closed (Prasad, 2006, p. 76). Reagan neither advocated nor authorized new regulatory agencies or a regulatory program during his Presidency, although it de-emphasized regulatory reform in his second mandate to avoid public backlash (i.a. Prasad, 2006; Vogel, 2003; Weidenbaum, 1997)

President Bush transformed the Task Force on Regulatory Relief into the Council on Competitiveness, established in March 1989. The Council was chaired by the Vice-President and interfered in various regulatory affairs. For example, it stopped an EPA proposal that would have required municipalities to divert 25 percent of their solid waste destined for incineration to recycling programs. However, the Bush administration also supported a number of new regulatory statutes including the Americans with Disabilities Act, the Clean Air Act Amendments of 1990, and the Civil Rights Act of 1991, before establishing a moratorium on the issuance of new regulation (Weidenbaum, 1997, p. 21). Bush, continuing Reagan's legacy, also avoided enacting comprehensive privacy legislation, with only signing into law the Telemarketing and the Telephone Consumer Protection Act, in response to people's annoyance with telephonic spam.

So the 80s ended, with even less institutions in charge of studying and advocating for privacy. The overarching policy paradigm of the time was to keep regulation minimal and the government out of business back. In this context is that the Internet would become popularized. Welcome to the 90s.

The 1990s - Inventing the Internet

"Technology is almost magical" said Bill Clinton on his first inaugural Presidential Address, on a sunny and pleasant morning in Washington DC (2009, p. 605). And he was seriously committed to allowing technology to unleash its magic: according to data from the World Bank, when Clinton entered the Oval Office less than 1% of Americans were Internet users. By the time he left the White House that number grew to 50% (World Bank, 2015).

During the 1992 presidential campaign, Bill Clinton and Al Gore pledged to make deployment of a "national information network" a priority of their Administration. The impetus for this commitment apparently came from Gore, who, as a Member of the House of Representatives, proposed a "nationwide network of fiber optic 'data highways'" in 1979 (*Federal Information Policies*, 1990, p. vii). Together, they campaigned on a promise to create a network that would "link every home, business, lab, classroom and library by the year 2015." (Cate, 1998, p. 2) As anyone living in the United States in 2016 could attest, this goal has by far been achieved. Clinton, consequently, had arrived to office endorsed by thirty high-tech leaders from Silicon Valley corporations (Clinton, 2005, p. 429), whom enthusiastically supported him. In words of John Sculley, CEO of Apple Computers, "Clinton asked us to develop a technology policy for him, and that was refreshing, because he not only embraced a lot of the ideas we put forth but we believe he really plans to implement them." (Sims, 1992)

But which kind of technology policy would the Clinton Administration apply? It is unrealistic to assume that political leaders have the whole universe of policy alternatives at hand in a certain moment of time: the prevalent ideas, history, and institutions condition not only what is perceived as possible but also even what ideas can be entertained. Thus, the Clinton Administration policy options were shaped, bounded, and conditioned by the substantive historical experience and institutions created in the previous decades (Steinmo, 2003, p. 208; Weir, 1992).

The Clinton administration was not only techno-optimistic, but also represented a new breed of Democrats, those that shared much of ideas of the late 70s and 80s regarding regulation. The third-way progressive Administrations that Clinton in the United States and Blair in the United Kingdom embodied believed philosophically that Governments had become overloaded (Scanlon, 2001), which proves the prevalence of the deregulatory shift of the 1970s. During March 1993, when announcing the Initiative To Streamline Government and launching the National Partnership for Reinventing Government (NPR) chaired by Vice-President Gore, Clinton announced that the goal of his Administration was to "make the entire Federal Government both less expensive and more efficient" (Clinton, 1993, p. 350) Gore's first NPR report, from September 1993 and published online—a novelty in the era—asked "Can regulations be eliminated? The answer is yes", while logically proposing "eliminating regulatory overkill" (Gore, 1993). The Clinton

Administration was essentially walking the ideological and institutional path created since the deregulatory turn of the 70s.

Therefore, considering the techno-enthusiasm of the Clinton Administration and its preference for little or no regulation, it is logical that the approach Clinton chose for the development of the Internet was one of minimal Government intervention. In 1997, the Clinton Administration declared that "[f]or electronic commerce to flourish, the private sector must lead. Therefore, the Federal Government should encourage industry self-regulation wherever appropriate" (Clinton, 1998, p. 899). The combination of techno-optimism, and a disbelief that governmental intervention in the economy is what explains the 'hands-off' approach that the Clinton Administration applied to all aspects that affect Internet regulation (Abbate, 2000; Langenderfer & Cook, 2004).

But the Clinton Administration was not the only political actor excited about the Internet. During the 1990s the policy and intellectual paradigm was that the Government should not, and even *could not* interfere with the Internet. The influential *Declaration of Independence of Cyberspace*, written by John Perry Barlow, one of the founders of the Electronic Frontier Foundation (the culturally relevant world-first digital rights NGO) read "Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather. […] You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear." (Barlow, 1996). Barlow's perspective was far from radical or isolated. Nicholas Negroponte, founder of MIT's Media Lab, wrote in *Being Digital* (1966) that "national law has no place in cyberlaw" (Negroponte, 1996, p. 237). And Kevin Kelly, formed editor of *Wired*, wrote in 1995 "No one controls the Net. No one is in charge. […] The Internet is, as its users are proud to boast, the largest functioning anarchy in the world" (1995, p. 464). Academically, Cairncross argued that because of the Internet the nation state would have to reinvent itself, since "governments' jurisdictions are geographic, but the Internet transcends geography", and even the power to impose taxation will be challenged (Cairncross, 2001, p. 159). Similarly, Spar argued that "International organizations lack the power to police cyberspace; national governments lack the authority; and the slow pace of interstate agreement is no match for the rapid-fire of technological change" (Spar, 1999, p. 47).

In fact, up to the late 1990s and early 2000s it was novel to argue that the governments *could* and actually *did* interfere with the Internet: the regulatory approach to the Internet created by the Clinton administration had ossified into such worldview (Hattam, 1992). Wu and Goldsmith's argument in *Who Controls the Internet?*, published in 2006, was that national governments, through coercion and control over local intermediaries, still exert regulatory control in the realm of the Internet, questioning the then popular notion that the Internet was erasing national bonders and rendering nation-states obsolete (Goldsmith & Wu, 2006). Only in 2004, Daniel Drezner published *The Global Governance of the Internet: Bringing the State Back in* in which he argues that "States, particularly the great powers, remain the primary actors for handling the social and political externalities created by globalization and the Internet" (Drezner, 2004, p. 478). In short, during the 1990s, there were two lines of public opinion regarding regulation and the Internet: the one that argued that the Internet should be regulated as little as possible, in fear of harming it; and the other that thought that the Internet could not even be regulated to start with. What the Clinton Administration believed, as the predominant public opinion of the early 1990s, was in a minimal intervention approach to the Internet.

In July 1997, the Clinton Administration published its position regarding regulation of the Internet and privacy issues that might arise from its popularization in the Framework for Global Electronic Commerce (*A Framework for Global Electronic Commerce*, 1997). The paper reflects widespread consultation with industry, consumers groups, and the Internet community. It established a set of principles to guide policy development, outlined the Clinton Administration's positions on a number of key issues related to electronic commerce, and provides a road map for international negotiations, where appropriate. It also identifies which government agencies will take the lead in implementing this work.

The framework also highlights five principles for the development of Internet: (1) the Private Sector should lead, and the Internet should develop as a market-driven arena not a regulated industry; (2) Governments should avoid undue restrictions on electronic commerce; (3) Where governmental involvement is needed, its aim should be to support and enforce a predictable, minimalist, consistent and simple legal environment for

commerce; (4) Governments should recognize the unique qualities of the Internet; (5) Electronic Commerce over the Internet should be facilitated on a global basis.

The above stated evidence does not mean that the Clinton Administration did not care about Internet privacy, or thought that the United States' government could not regulate the Internet. On the contrary, the Clinton Administration was considering the issue and actively took a conscious decision to not regulate the Internet, not even regarding privacy issues: "The Administration considers [personal] data protection critically important", read the Framework for Global Electronic Commerce. "We believe that private efforts of industry working in cooperation with consumer groups are preferable to government regulation, but if effective privacy protection cannot be provided in this way, we will reevaluate this policy" (*A Framework for Global Electronic Commerce*, 1997, p. 20).

At the same time, it cannot be overlooked that the person behind the Clinton administration approach to the Internet was Ira Magaziner (Broder, 1997), the same person behind the President's failed health care reform (Steinmo & Watts, 1995). Interviewed by the New York Times in 1997, Magaziner was questioned about the different regulatory approaches chosen for the Internet and health care reform, and his answer was somehow obvious: "[h]ealth care is a very different industry than telecommunications" (in Broder, 1997).

But, Magaziner had indubitably learned some lessons after the failure of the health care form: "The process was flawed and we ended up with a bill that was more regulatory than we wanted […] I blame myself. I could have put my foot down" (in Broder, 1997). Magaziner had experienced what Weir proved: American political institutions make positive reform difficult (1992). Yet, that does not fully explain the regulatory approach itself: the previously described Clinton administration ideas towards the Internet and technology, in friction with American institutions and recent political history, offer a much more comprehensive reading (Lieberman, 2002).

As his predecessors, Clinton avoided proposing a comprehensive privacy reform, and no one considered that comprehensive privacy reform was necessary, primarily to avoid the possibility of hurting the Internet. Clinton did, however, sign some pieces of sector-specific privacy legislation into law. For example, the Child Online Privacy

Protection Act (COPPA) protects the privacy of children under the age of 13 by requesting parental consent for the collection or use of any personal information of the users, and is a result of public outrage of marketers collecting personal information of children (Warmund, 2000).

The Clinton administration, in sum, considered that Government intervention could only harm the Internet, and therefore had no intention to enact legislation, including privacy legislation, that might do just that. Likewise, Clinton's reelection to a second term came to validate Clinton's stance regarding regulation and the Internet.

However, the desire of the Clinton Administration for minimal or no Internet regulation did not consider the European Union's decision to forbid companies operating in jurisdictions that not adhere to its own standards to handle or control European data. Because of the European Union, American companies began to face regulation, and met a new regulator: the FTC.

The European Union Steps-In

Virtually unregulated at home, American business have been subject to regulation from their own desire to trade with the European Union—American companies wishing to trade with Europeans' personal information are obliged to participate in the Safe Harbor Agreement on transfers of personal data between the European Union and the United States. The Safe Harbor Agreement is a compromise between the European Union and the United States that allows American companies to collect Europeans' personal information despite the United States being a jurisdiction that could hardly be considered to adequately meet European's privacy rights as required under Europe's 1995 Data Protection Directive (H. Farrell, 2002).

The 1995 Data Protection Directive mandated the European Commission certify that third jurisdictions complied equivalent levels of protection to trade with European's personal information before allowing international personal data flows. All jurisdictions, except the United States, that desire to trade in the European personal information market have opted to copy the European Data Protection Directive into their legal systems (A.

Newman, 2008). But why did the United States not copy the European model, like all other nations did?

An obvious and necessary part of any answer is that the United States did not have to, since the structural political and economic power of the United States gave it leverage vis-à-vis the European Commission (EC) that other nations simply do not have. Yet, acknowledging the structural power of the United States is both necessary and insufficient to explain a certain policy decision, since, as standalone explanations material conditions do not effectively default a concrete policy response. In other words, although the United States could choose not to copy the European model and force the EC to arrive to another kind of compromise, it could have also simply chosen to copy it. The preference for not copying the European model is explained by previously taken American policy decisions regarding privacy and the Internet encompassed in the overarching deregulatory policy paradigm.

Of course, another plausible explanation of why the United States refused to do as other nations and copy the European privacy framework is that business lobbied the government against adopting the European system, and as Farrell demonstrates that such thing happened (H. Farrell, 2002). However, before weighing in business interests as the sole explanatory variable one must not forget that business had little convincing to do since the government also preferred to keep the existing institutions as unchanged as possible –business and government interests aligned. In simpler terms, businesses were preaching to the choir. The predominant institutions and ideas of the American policy system were biased against comprehensive privacy reform. And the structural position of the United States regarding the European Union allowed Washington to avoid drifting from its main policy preference: keeping the American privacy regime as a limited one.

The Framework for Global Electronic Commerce stated that "governments should refrain from imposing new and unnecessary regulations, bureaucratic procedures, or taxes and tariffs on commercial activities that take place via the Internet" of 1997 (*A Framework for Global Electronic Commerce*, 1997). As shown in the previous section, during the 1990s the overarching policy paradigm and Internet- and privacy-specific policies were biased against the kind of comprehensive privacy reform that copying the European privacy framework, as the rest of the world had done, would imply. In short, the

institutionalized policies and ideas about privacy and the Internet created in previous stages shaped the preferences of actors in the new itineration of the policy game created by the European Data Protection Directive.

Hence, America rejects copying the European privacy framework and negotiates an international agreement, Safe Harbor. Institutionally, the Safe Harbor agreement has both one intended and one unintended consequence. The intended consequence is that the 2000 Safe Harbor agreement allows American companies to voluntarily self-certify that they offer a European equivalent level of personal data protection by complying with the principles of notice, choice, onward transfer, security, data integrity, access and enforcement. The agreement purposely enabled American companies to trade with Europeans personal information without, at first glance, substantially modifying the America own privacy framework.

However, the unintended consequence of Safe Harbor is that American companies that adhere to the Safe Harbor List subject themselves to the supervision of the Federal Trade Commission (FTC), which oversees the compliance of the agreement, turning the FTC into a powerful institution that drifts away from its original purpose and starts advocating for privacy protection. While the FTC had been trying to expand its privacy protection agenda since 1995, when Congress asked it to investigate the privacy risks associated with computer databases (Hetcher, 2001, p. 2406), the Safe Harbor radically increases its supervisory scope and power. In fact, according to a 2013 report from the Future of Privacy Forum–a Washington DC based think tank supported by corporations like Facebook, Google, Apple, or AT&T—Safe Harbor resulted "in stronger investigatory and monitoring powers for the FTC" (Future of Privacy Forum, 2013, p. iv)

Thus, unexpectedly and unintentionally, Safe Harbor reinforced the FTC and transformed it into America's de facto privacy regulatory agency for the private sector by virtue of Section 5 of its 1914 foundational Act on Deceptive Practices that allows it to fine and oversee companies that make a promise to their consumers that they do not comply. Regarding rules compliance, American companies essentially self-regulate. In spite of the fact that in the last decade the FTC has been a strict punisher of corporations' broken promises, placing multi-million dollar fines on corporations such as Google, Facebook, and Snapchat, American corporations are by and large, only accountable for

their promises, and are not held accountable under national legislation. In other words: the FTC might be good at enforcing rules, but there are few rules to enforce.

Nevertheless, the crucial point is that the FTC has used its casually granted regulatory powers over the Internet and privacy to advocate for comprehensive legislation. In other words, the unintended institution created by Safe Harbor—namely the FTC as a privacy agency—began to drift away from its originally conceived goal of ensuring that companies do not use deceptive practices and started pushing for regulatory change. In fact, in 2000, the FTC published a report on Online Privacy, in which it asks Congress to enact legislation obliging all private corporations to adhere to the Fair Information Practices draw in the Privacy Act of 1974 (FTC, 2000), the equivalent of asking the Congress to enact a comprehensive privacy regime.

However, as the reader will see in the following section, privacy was not in the agenda of President George W. Bush, and the FTC chairman that called for new legislation was removed. Bush appointed Timothy Muris, whom declared shortly after taking office that "at the time we need more law enforcement, not more laws" (Muris, 2001). But not only was the Bush Administration not willing to regulate in favor of privacy, but the times would lead the Bush Administration and America in a new direction fundamentally opposed to privacy protection.

Second Paradigm: Privacy in the national security era

The 9/11 terrorists attacks in New York awoke an unusual feeling in a nation used to believing in its continental size, economic and military power, and geographical separation from the world invulnerability: fear. In response, the Bush administration offered a simple tradeoff: rights for security. The policy paradigm of America since the 2001 terrorist attacks has been one of overwhelming prioritization of national security over any other kind of issues, in the name of the "war on terror" (i.a. Astrada, 2010; Duffy, 2015; Lustick, 2006; M. I. Wright, 2011).

In 2001, the Bush administration proposed to the Congress and the American people the thesis that the tragic terrorist attacks on New York's World Trade Centre could have been avoided if the security services had more power to identify possible terrorists and prevent them from acting. Only a month after the Twin Towers disappeared and

without much debate, President Bush convinced the Congress to approve the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, or USA PATRIOT Act (known simply as the Patriot Act), against any possible prediction by the liberal traditions theory that remains incapable of explaining this turn in American politics. The terrorist attacks left the nation in high alert, and the administration responded with radical measures. In fact, from 2004 until 2013 a majority of Americans believed that the Government anti-terrorist policies have not gone far enough to protect the country (Pew Research Center, 2013). In a context of shock, the Bush Administration's ideas regarding national security did not find in the nature of American political institutions a deterrent for its reforms.

The broad Title II of the Patriot Act on Enhanced Surveillance Procedures amends the Foreign Intelligence Service Act (FISA) and the Electronic Communications Privacy Act of 1986, by – as it title explains – expanding the surveillance powers of the different state agencies. For example, Section 216 of the Patriot Act broadens the focus of traditional surveillance to include Internet communications. One of the main reforms introduced by the Patriot Act is an update to the 1978 FISA, a counter-intelligence law passed during the cold war. Section 103 of FISA gives the government permission to conduct electronic surveillance. Framed by its proponents as an exceptional measure to exceptional times, legislators originally expected that many of the extraordinary provisions of the Patriot Act would expire, unless renewed again by Congress. Section 224 contains a Sunset Clause that in successive reforms, the Bush and Obama administrations have each extended, enhancing the scope for unlimited surveillance by governmental agencies.

Many NGOs and experts would have liked the government to at least let the sunset clause take effect since they consider the influence of the Patriot Act to be enormous. According to the Electronic Frontier Foundation, a digital rights and privacy NGO, the Patriot ACT "gives sweeping search and surveillance to domestic law enforcement and foreign intelligence agencies and eliminates checks and balances that previously gave courts the opportunity to ensure that those powers were not abused" and it "threaten the basic rights of millions of Americans" (EFF, 2014). More critically, a report of the New America Foundation, a non-partisan think tank, found that "an in-depth analysis of 225 individuals recruited by al-Qaeda or a like-minded group or inspired by al-Qaeda's

ideology, and charged in the United States with an act of terrorism since 9/11, demonstrates that traditional investigative methods, such as the use of informants, tips from local communities, and targeted intelligence operations, provided the initial impetus for investigations in the majority of cases, while the contribution of NSA's bulk surveillance programs to these cases was minimal." (Bergen, Sterman, Schneider, & Cahall, 2014, p. 9)**.** But what does the Patriot Act mean in practice for the American people? In short, that everything that Google, Facebook, and Microsoft know about you, the NSA knows.

But let's illustrate the events with two examples. First, according to the Washington Post, PRISM (a surveillance program that collects personal information from the servers of the most important Internet companies) allows every government employee with clearance, anywhere in the world, to simply ask the system for information and then receive results from the Internet companies that participate in the program without further interaction with the company's staff (Ball, 2013). Second, according to documents revealed by Edward Snowden, between 2006 and 2008 the NSA and the FBI tracked the email accounts of Muslim American leaders –including a professor at Berkeley and a lawyer who served in the Department of Homeland Security (B. Bennett, 2014). Those are just some of multiple examples, brought to light by Edward Snowden, of the consequence of a lack of comprehensive privacy regime coupled with a policy of national security trumping civil rights protections.

The lack of a comprehensive privacy framework has allowed companies to collect massive amounts of personal data, facilitating the work of the NSA. The Intelligence Agencies need only to access to the information that companies collect to get their job done, and companies are collaborating. A comprehensive privacy framework that would have limited what companies could do with personal data and created an independent regulatory agency for both the public and the private sector would have probably minimized. Yet, the policy paradigm of post-9/11 America has again prevented any kind of legislation that might be interpreted as minimizing the tools for protecting the nation from terrorist attacks and thus any possibility for a comprehensive privacy regime.

Conclusion

Being the only advanced nation without a comprehensive privacy regime makes America exceptional. Yet, it is not because an exceptionally liberal traditions American culture that privacy is not protected in the United States. In the previous pages I have shown that polls demonstrate that Americans have manifested throughout time that they are concerned about their privacy, and they have done so in a similar fashion to the Europeans, and sometimes before them and with more intensity, as some commentators have pointed out (Hondius, 1975). I have also shown that comprehensive privacy has been debated in American politics. Yet, the predominant liberal traditions explanation of why America does not have a comprehensive privacy regime is limited in stating that Americans simply do not want that kind of legislation and creates a narrative fallacy that disregards events that do not fit in the defended framework, like the surveillance state created after the 2001 terrorist attacks.

I have argued that reading the evolution of the American privacy framework in a vacuum prohibits understanding the nature of the policy debate. As Steinmo points out, policy makers thinking "is fundamentally framed within the economic/intellectual climate in which they work" (Steinmo, 2003, p. 227). The predominant liberal traditions explanation is appealing and plausible at first glance, yet over-simplifies history and policy debates bringing the reader to wrong or insufficient conclusions. On the other hand, a reading that pays attention to the evolution of the American policy paradigm through ideas, interest, and institutions, offers a more nuanced and complex interpretation of history. By doing this, I explain why America does not have a comprehensive privacy regime.

The policy paradigm reading offered before helps to understand that American political culture is not intrinsically opposed to comprehensive privacy reform and has relevant implications for the policy debate and academic analysis. For academic researchers, the perspective I offered in this article pushes a reconsideration of why and how America is an outlier regarding privacy protection. I have shown that privacy policy in America cannot be understood outside of the overarching policy paradigm in which

takes place. The crises of 1973 and 2001 resulted in two policy paradigms (the deregulatory paradigm and the surveillance paradigm) that were biased against comprehensive privacy reform first because it implied creating regulatory burdens, and later because it would have created barriers to the massive surveillance goals. As I have shown, these policy paradigms created the institutional and cognitive locks to prevent comprehensive privacy reform. I have also shown that ideas and institutions have to be considered as necessary, integral, overlapping, and fractioning elements of political explanations, which on their own cannot explain the lack of a comprehensive privacy regime in the United States (Lieberman, 2002, p. 709).

For policymakers, especially considering that privacy has gained salience in American public debate due to the many Snowden revelations, is important to eliminate the misconception and prejudice that comprehensive privacy reform is something that it is un-American. As I show in the previous pages, up to the 1970s America had privacy debates prior to and with more intensity than Europe, even the Senate Bill of what would become the 1974 Privacy Act had designed a comprehensive privacy regime. Hopefully the policy paradigm of our times will turn in favor of comprehensive privacy reform, and Americans will be able to stop worrying about their privacy. American political institutions certainly would not make that change easy, and since 1974 innovation in privacy policy has been bounded against comprehensive reform. Yet, the historical learning of the consequences of the surveillance paradigm might push for the creation of a new paradigm capable of enacting protection for American's privacy.

IV. Article 3 – Willing to govern? Privacy protection implementation in Europe and the United States

This article argues that the American and the European privacy regimes do not provide their expected governance results since they have been poorly designed and implemented because legislators have no rational incentives to control intelligence agencies nor to provide the necessary resources to the implementing data protection authorities. If policymakers are unwilling to exercise effective governance in a certain policy area, the resulting governance arrangements will fail to provide the expected results due to being poorly designed and executed.

In more general terms, this article illustrates the importance of studying the implementation and design of policies to understand their effective governance effects. It also shows that the American and the European privacy policies have left a governance gap that ought be explored. Empirically, this article shows how European and American legislators identified the perils of unchecked government surveillance but failed to create effective oversight structures on the intelligence agencies despite much attention dedicated to their activities in several periods of time –particularly in the 1970s and since 2013. It is also argued that the regulatory interdependence between the EU and the US on consumer privacy negatively affects Europeans expectations of privacy because of a lack of enforcement of Safe Harbor. More generally this article makes the point that if a policy problem is poorly defined or a policy poorly implemented, the final outcome will not respond to the original goal.

Introduction

"Sunlight is said to be the best of disinfectants" – Louis Brandeis (2009, p. 92)

"If men were angels, no government would be necessary. If angels were to govern men, neither external nor internal controls on the government would be necessary" – James Madison (2005, p. 281)

The EU and the US have created radically different laws and bureaucracies for the governance of the collection and processing of the personal data of their citizens. The origins and institutional consequences of those institutions have been deeply explored in literature. With the adoption of the 1995 Data Protection Directive (hereon the 1995 Directive) the EU has become the central actor in the global privacy debate (i.a. Bennett & Raab, 2006; A. Newman, 2008; Swire & Litan, 1998), establishing what some have considered the "de facto international privacy standard" (Bach & Newman, 2007, p. 836; see also Schwartz, 2013, p. 1968) enforced by powerful independent national agencies, the Data Protection Agencies (DPAs). In contrast, the US maintains a limited privacy regime, or framework, composed of several sector specific privacy laws and statutes and without a dedicated agency for the protection of personal privacy – the Federal Trade Commission's (FTC) division on consumer privacy is the closest equivalent to the European DPAs. As a consequence, the US privacy framework has been often characterized as a patchwork of protections (Bennett & Raab, 2006; National Research Council, 2007; Regan, 1995, 2008) that allows Internet companies to "operate without specific statutory obligations to protect personal data", according to a 2010 green paper of the US' Department of Commerce (2010a, p. 12).

Studying the revelations of massive state-surveillance by former US National Security Agency (NSA) contractor Edward Snowden since the summer of 2013 (Glenn Greenwald, 2014; Poitras, 2015), the UN special rapporteur on counter-terrorism and human-rights concluded that "the hard truth is that the use of mass surveillance

technology effectively does away with the right to privacy of communications on the Internet altogether" (Emmerson, 2014). Also because of Snowden's revelations, the European Court of Justice (ECJ) declared Safe Harbor, the agreement that allowed American companies such as Google and Amazon to store and process Europeans data in the US, invalid for failing to protect European's privacy (ECJ, 2015). As a consequence of the Snowden revelations, European and American privacy advocates are demanding strengthening failed privacy policies that include the curbing of massive state surveillance (i.a. Albrecht, 2013; Shuster, 2013).

These recent events show that neither the EU nor the US privacy frameworks have protected citizens' privacy as the systems inherently intend. But why? Why did the privacy governance efforts of the EU and the US not provide the expected results? A possible explanation is that the intelligence agencies such as the NSA are ungovernable and out of control (i.a. P. Lewis, correspondent, & Oltermann, 2013; Norton-Taylor, 2013). Or they are behaving like "rogue elephants" as US Senator Church famously put it in the 1970s during a post-Watergate inquiry on the activities of the Central Intelligence Agency (CIA) (in Lathrop, 2008, p. 353). The "rogue elephants" explanation is convenient for politicians since it allows them to plausibly deny any responsibility of the excesses of the intelligence agencies' spies.

Instead, building on implementation literature (i.a. Hogwood & Gunn, 1984; Mazmanian & Sabatier, 1983; Pressman & Wildavsky, 1984) but fundamentally on Rothstein's critique and proposal for a general theory on implementation that enables researchers to explore policy design and execution (1998) I argue that the American and the European privacy regimes did not provide the expected results because policymakers are unwilling to control intelligence agencies or to provide the necessary resources to the implementing data protection authorities. As a consequence, the American and the European privacy governance schemes have been poorly designed and implemented. If policymakers are unwilling to exercise effective governance in a certain policy area, the resulting governance arrangements will fail to provide the expected results for being poorly designed and executed. While political scientist and privacy expert Colin Bennett has already briefly argued that "privacy protection is flawed" because "laws are often weakened by broad exemptions, especially for law enforcement, [and] the regulators have

few resources" (Colin J. Bennett, 2011, p. 493), this article offers a more detailed analysis of the origins of the flaws in privacy protection.

This is an article about what happens when politicians govern by enacting laws and building bureaucracies theoretically aimed to solve a problem, but without the will to effectively exercise steering in a certain policy area. In more abstract terms this article illustrates how vague legislative statutes and policy guidelines and a lack of legislative oversight generates mission drift in agencies (i.a. Halperin et al., 1974; Lipsky, 1983; Pressman & Wildavsky, 1984). Regarding data protection literature, this article contributes to filling the gap that exists in the study of the outcomes produced by the different privacy regimes and the study of variation of the protection of individual's privacy across jurisdictions (Colin J. Bennett & Raab, 2006) and bridging the gap between the literature on surveillance and the literature on privacy, which talk to each other less than would be expected (on this, see Colin J. Bennett, 2011a, 2011b).

Calling on paying more attention to how policies are designed and implemented, this article makes two contributions to the governance field. First, it is a partial response to the recent call for a third wave of global governance research (Coen & Pegram, 2015) by offering an operational way of researching the delivery of policy goals that allows understanding why and how approaches to governance work or not. Second, it contributes to rethinking the influence of states and state-centric institutions in the provision of Internet governance (Eeten & Mueller, 2013) by offering a way for studying their effective steering power. If by studying the design and implementation of state-centric governance arrangements we find that they fail to provide the anticipated steering then we can start questioning who is filling the governance gap, and how, with greater clarity. Methodologically, to identify the policy designs and the failures in implementation I use a policy-centered approach that takes the policies as dependent variables and then searches for the political processes behind them—hence the information processed by the policymaking system and its consequences become a central component in the narrative (Baumgartner & Jones, 2015, p. 24).

This article examines the development of the American and European privacy regimes. It shows how legislators have been unwilling to control or provide oversight of their executive agencies and how implementing agencies have failed to perform their

entrusted, and very difficult tasks because of a lack of resources from legislators who have no incentives to give them. Specifically, this article will attempt to explain: the design and the implementation limitations of the American and European privacy frameworks; the unwillingness of legislators to exercise control over intelligence agencies and give more scarce resources to implementing agencies; the violations of privacy committed by unchecked intelligence agencies; and the impossibility for privacy agencies to implement the law without the necessary resources.

Willing to govern?

It is possible to identify a democratic governance deficit in that American and European legislators have shown a lack of will to exercise oversight their intelligence agencies for understanding there are little political gains for them to do so (i.a. Olmsted, 2000; Zegart, 2013). Legislators perceive that there is no obvious connection between their own political lives and intelligence agencies—the spies—activity, cannot capitalize on their work inside confidential committees, risk being held responsible by the public if scandals involving the overseen intelligence agencies arise, and can be blamed by speakers or defenders of the intelligence agencies' spies if oversight curbs their tools and an accident or terrorist attack occurs (see for example Baker, 2013; Nelson, 2015; see also Olmsted, 2000, Chapter 4). Thus, for example, American legislators have found ways to avoid serving in the Intelligence committees (Zegart, 2013). In France, until 2007, the Parliament operated without a committee on intelligence, the only advanced democracy without such (FRA, 2015, p. 38; Lotz II, 2007, p. 124), and up to today French legislators' request for information are denied by their spies (Wills & Vermeulen, 2011). In the UK the intelligence agencies were legally unregulated and formally a secret to Parliament until the Security Service Act of 1989 and the six members of the intelligence parliamentary committee are chosen by the Prime Minister with the validation of the head of the opposition (i.a. Bigo et al., 2013; H. Born, Johnson, & Leigh, 2005; Leigh, 2007b). And in Germany, while there are is a formally strong oversight body in the Bundestag, evidence suggests that the intelligence agencies lied to its legislators (DW, 2014).

American and European legislators have also very few rational incentives for giving more scarce resources to their data privacy authorities, or even to create them. In

the US, policymakers have historically been resistant to the idea of a data privacy authority and the FTC only acts as a de facto privacy agency as consequence of the Safe Harbor agreement with the EU (H. Farrell, 2002a; Future of Privacy Forum, 2013). In the EU, Newman has explained how DPAs are widespread since the mid-late 1990s, not because of political will of European policymakers, but because some pre-existing national DPAs kept the EU integration process hostage by threatening to block intra-EU transfers of personal data if the European Institutions did not follow their demands of adopting a common EU data protection framework, the 1995 Directive (2008). Yet, likely because 65% of Europeans had not even heard about their existence according to a 2011 Eurobarometer (the results were consistent across different ages, educational backgrounds, usage of Internet, and countries) (Eurobarometer, 2011, p. 174), DPAs routinely object that they do not receive the necessary resources to do their job (FRA, 2013). After all, excluding scandals, privacy has in general been a relatively low salient issue in American and European politics—and in low salience scenarios, policymakers have very few incentives to take actions that might trigger divestment by corporations such as strengthening the public regulators (P. Culpepper, 2011; P. D. Culpepper & Reinke, 2014).

All the privacy policies created by advanced democracies contain exceptions to the work of intelligence agencies. Yet, surprisingly, the predominant narrative of the origins of post-Watergate privacy legislation in America is that its purpose is to protect American citizens' privacy from unwarranted massive surveillance by their authorities (Rule & Greenleaf, 2010, p. 5). Concurrently it is common to argue that Europeans care about their privacy because of the state-driven privacy invasions that occurred in the autocracies that governed most of Europe during the early 20th century (Lindsay, 2005; Mullerat, 2007). Why then, do the privacy policies of the EU and the US contain exceptions for national security and why are intelligence agencies effectively subject to no oversight?

There is no doubt that politicians have the elements to conceptually understand that there can be no privacy without having state structures under supervision. The legal reasoning behind the regulation that creates the EDPS (a DPA for the European institutions) reads: "is necessary to […] create an independent supervisory authority responsible for monitoring the processing of personal data by the Community institutions and bodies" (EP, 2000, p. i). For the defense of privacy, not even the European institutions

are to be trusted without supervision. Likewise, in an opinion written after the Snowden revelations, the Article 29 Working Party (WP29, a network of coordination and work of the EU DPAs) considered that "in order to ensure that intelligence services indeed do respect the limits imposed on surveillance programmes [by EU privacy laws], meaningful oversight mechanisms need to be implemented in the laws of all Member States. This should include fully independent checks on data processing operations by an independent body as well as effective enforcement powers" (WP29, 2014, p. 8). In other words, the regulators and policymakers repeatedly acknowledge that state surveillance must be addressed to protect privacy but then fail to put effective limits and oversight on the activities of their spies. However, it is precisely because of both the policy design failure of creating exceptions for intelligence agencies for the compliance with privacy policies and the lack of oversight that the ECJ declared Safe Harbor, the agreement for transfer of personal data between the EU and the US, invalid (2015). Rationally, politicians know they must act to keep the state from violating people's privacy. They also rationally chose not to control the part of the agencies that precisely enable the privacy violations people are scared of. Certainly, opting-out of controlling intelligence agencies is the result of political compromise. But such compromise has fundamental costs for the functioning of privacy policies.

As shown by previous research, in absence of appropriate oversight we can expect bureaucratic drift, when an agency pursues policies with consequences that "diverge from social and/or legislative goals" (De Mesquita & Stephenson, 2007, p. 605; also Epstein & O'Halloran, 1999, p. 25). Legislative oversight, concerning "whether, to what extent, and in what way Congress attempts to detect and remedy executive branch violations of legislative goals" (McCubbins & Schwartz, 1984, p. 165), is then fundamental since it is based upon the notion that for government to prosper in an orderly fashion, its institutions and the people that staff them must be accountable for their actions. Doing otherwise invites people in official positions to abuse their discretionary power to pursue particular interests instead of the common good. Legislative oversight of intelligence agencies ensures that they are not subject to political pressure or used to further particular political interests, helps to maintain public confidence in the spies (Bochel, Defty, & Kirkpatrick, 2014, p. 5), and guarantees that they have the necessary resources to perform their duties (Zegart, 2013). Fundamentally, as Leigh observes, legislative scrutiny of the intelligence

sector ensures that it does note become a "zone sanitaire for democratic scrutiny" (2007a, p. 71). However, as we will see in the following pages, the violations of privacy rights committed by European and American intelligence agencies revealed by Snowden have been enabled by lack of democratic oversight.

An alternative explanation: the intelligence agencies are out of control

Intelligence agencies are out of control. Or as Senator Church famously put it in 1975 they are behaving like "rogue elephant[s] on the rampage" (in Lathrop, 2008, p. 353) that act independently from any kind of government oversight setting their own political agenda. Surely, only conspiracy-theorists could believe that democratically elected leaders such as Eisenhower, Kennedy, Johnson, Nixon, Ford, Reagan, Bush, Obama, Cameron, Blair, Brown, or Merkel knew that their spies were snooping on civil society leaders for political reasons, or eavesdropping without warrants on their citizen's domestic communications, and not only did nothing to stop them but guided their conduct. On the contrary, one might think, modern governments are huge, complex apparatuses; where things can and will eventually go wrong, that the revelations of state-surveillance are exceptional aberrations that prove misconduct, and that misconduct—even if gross—is a fact of government. That executive's correct misconduct by reprimanding the bureaucrats or agencies that drifted from their mission is proof that the agencies were out of line. And even if correction comes ex-post and after a scandal, it is still the best proof that executives are doing the best they can to protect the constitutional rights that are the cornerstone of any democracy. The spies are as necessary as they are naturally difficult to govern.

However, there is ample evidence that intelligence agencies respond and report to their executives and that they are not rogue elephants (i.a. D. H. Born & Caparini, 2013; Bruneau & Dombroski, 2014; Olmsted, 2000; Prados, 2013; Prillaman & Dempsey, 2004; Theoharis & Immerman, 2006). In reality, the persistence of the rogue elephant myth is due to its political usefulness. Conveniently for politicians, the idea that agencies act independently allows them to plausibly deny any wrong doing, by claiming they did not know what was happening (D. H. Born & Caparini, 2013, p. 138). A prime example of politician's use of this narrative is the case of US Senator Church, a hopeful Democrat Presidential primary candidate chairing one of the inquisitive committees on the

intelligence agencies during the 1970s. He declared that the CIA—then at the epicenter of the Watergate investigations—had never committed illegal activity under the orders of the President of the US. Senator Church argued, then, that the illegal activities the CIA did commit were done so without the President's knowledge or control, calculating that this would help him in campaigning and to bring him to the political center (Olmsted, 2000, p. 87).

Church colleagues and executive officials dissented. So much so that Church's committee's final report concluded: "The Central Intelligence Agency, in broad terms, is not out of control" (US Senate, 1976, p. 27). Furthermore, when asked by Church himself if the CIA was a rogue elephant without control, Kennedy and Johnson's former Secretary of Defense Robert McNamara said: "I have stated before and I believe today that the CIA [during the Kennedy and Johnson administration] was a highly disciplined organization, fully under the control of senior officials of the government… I know of no major action taken by the CIA during the time I was in the government that was not properly authorized by senior officials" (US Senate, 1975, p. 158).

Furthermore, a set of internal secret reports conducted by the CIA in 1973 informally known as the *Family Jewels* reveals that the executive in fact supervised and directed the Agency's systematic violation of its charter from the 1950s to the 1970s by—among other things—spying on journalists and social activists, kidnapping defectors, and breaking into former employees houses (CIA, 2010 declasified). The report was partially leaked in 1974 to *The New York Times* (Hersh, 1974). Similarly, a book commissioned and published by the CIA in 2008 details the relationship between the executive and the CIA's operations since its creation in the 1940s (Snider, 2008). Likewise, it is certainly telling that the structures of the NSA, GCHQ or BND have not been reformed by their national executives following the revelations made by Edward Snowden. For if the agencies would truly be rogue elephants, the executive would be making some effort domesticate them.

As the previous paragraphs show, it is hard to argue that intelligence agencies are out of control—all evidence suggests that the American executive has governed its intelligence agencies, including through cases of nefarious action. Therefore, legislatures could technically exercise effective oversight and control over their intelligence agencies

because there is nothing in the field of governance of intelligence agencies preventing them from doing so. Rather, as it is argued in this article, legislatures chose not to control intelligence agencies as a response to a rational lack of will, whose consequences and origins deserve to be studied. Like all legislation, privacy policies are subject to tradeoffs. And the tradeoffs accepted by legislators have severe consequences of the functioning of privacy laws. The lack of will to control intelligence agencies and fund regulators, critically affects the design and the implementation of privacy policies. Before presenting the analytical framework, the literature on implementation is reviewed.

Implementation and policy design

Pressman and Wildavsky's *Implementation* (1984, first edition published in 1973) has often been considered the piece that kicks off of the discovery of research on implementation (i.a. Goggin, 1990; Parsons, 1995; Ryan, 1995), offering a first approach to the "missing link" of the policy process, the one that goes from policy enactment to reality (Hargrove, 1975). However, Hill and Hupe remind us that the translation of policy to action had been studied before Pressman and Wildavsky's time, albeit without using the word "implementation" itself (2014, p. 18).

Therefore, one should remember Blau's works on the general functioning of bureaucracies (1955), Kaufman's research on how the US Forest Rangers translate into actions the words of federal statutes and agency regulations on Forest services (1967), and "above all" (Hill & Hupe, 2014, p. 19) Selznick's research on how the use of cooptation recruiting mechanisms by public agencies perpetuates behaviors and attitudes identities in bureaucracies independently from popular mandate (1949). Under this broad understanding of what implementation means one should also consider Halperin's seminal *Bureaucratic politics and foreign policy* (1974) as a treaty on implementation. However it is clear that the research preceding Pressman and Wildavsky's *Implementation* (1984) on the translation of policy to action dealt with one very specific aspect of the various factors that affect policy implementation, the role of bureaucracies, and it was not trying to provide a broader understanding of how policies translate to reality after been promised by their makers. And, certainly, the behavior of bureaucrats will affect the final result of any policy.

The study of the role of bureaucracies has been fundamental in what has been defined as the bottom-up approach in the policy implementation debate, which briefly argues that the implementation of policy is mostly about street-level workers exercising discretion in a given institutional environment. Thus, referring to the street level bureaucrat, Lispky argues that they live "in a corrupted world of service" and do the best they can within the limits imposed to them by the structures of work to cope with pressure and provide services (Lipsky, 1983, p. xiii). It should be noted that Halperin, in contrast, denounces how unelected bureaucrats modify the implementation of foreign policy to follow their personal interest and promote the relevance of their individual agency (1974). Further empirically studying how these street-level bureaucrats take their decisions, Hjern and Porter propose constructing a root-level network analysis of the networks bureaucrats create (1981) as a strategy that might be useful for policymakers to understand how decisions actually happen. Likewise, Barret and Fudge argue that much of the actual action of agencies depends on the interactions and compromises between bureaucrats of one or more organizations (1981). In sum, considering existing literature, one has to consider that bureaucrats are both limited by their institutional environment and the goals policymakers establish and also might shape their day-to-day actions to achieve their own goals, especially regarding the survival of their position and hierarchy.

Then, what makes *Implementation* different from previous research on the functioning of bureaucracies and the bottom-up approach to policy analysis, is that it inaugurates an agenda of research that focuses in understanding why and how the decisions taken by key policymakers end up translated into action (Pressman & Wildavsky, 1984). Thus *Implementation* inaugurates the top-down approach to policy implementation. Empirically, *Implementation* explores how and why a federally mandated program of economic development in Oakland, California, did not live up to the expectations of the legislators that instructed it and by many accounts failed to provide the expected results (Pressman & Wildavsky, 1984). The authors argue that the success of a policy depends upon the perfect cooperation between the agencies that are in charge of implementing it, and that a lack of cooperation translates into an "implementation deficit" (Pressman & Wildavsky, 1984). They also develop a mathematical rational choice model to measure the cooperation between agencies. It should be noted that by the second edition of *Implementation* written after Pressman's death, Wildavsky co-authors with Majone a

new chapter to *Implementation* where the rational choice mathematical model is abandoned in favor of a more iterative understanding of policy implementation (Majone & Wildavsky, 1979).

A policy implication of Pressman and Wildavsky's (1984) first approach is that one should have a pessimistic expectation of any policy that requires the cooperation of multiple agencies. This has been a recurrent message of literature on implementation, despite evidence that supports the contrary, as Rothstein argues (1998). For example, Bowen points out that the interaction game between agencies is rarely one-off as the first theoretical framework of *Implementation* suggests, and that agencies have the opportunities to build cooperation and collaboration mechanisms through time (1982). In other words, agencies can get used to working with each other, as the EU DPAs did by creating the WP29. Despite Wildavskys and Majone's (1979) attempt to soften the point made in the first edition of *Implementation* addressed by Bowen, it remains true that the post-first edition additions to *Implementation* do not try to amend the existing text but to build up on it. In the case of the enforcement of privacy regulations among different jurisdictions then, one should not necessarily expect implementation failure if the agencies have the tools for coordination action, as they have.

Considering that studies such as *Implementation* (Pressman & Wildavsky, 1984) have been highly informative but also "have been limited by the absence of a theoretical perspective", Van Meter and Van Horn (1975) offer a complex theoretical model with six clusters of variables constantly interacting with each-other to provide a result. While the complexity of the model makes it hard to operate beyond the descriptive (on the complexity of analytical models see, for example, Rodrik, 2015), Van Meter and Van Horn make two fundamental contributions. First, they signal the importance of providing theoretical models for understanding reality and not just providing prescriptions to policymakers. Second, they stress the relevance of incorporating to the analysis of policy implementation the stage of policy definition.

Hogwood and Gunn's *Policy Analysis for the real world* (1984; see also Gunn, 1978) offer a set of conditions for the perfect implementation of a specific policy, which can be a useful guide to compare the implementation limitations of concrete policies (Hogwood & Gunn, 1984, pp. 198–199). First, that the physical or political external

conditions to the implementing agency or agencies do not impose crippling constrains. Second, that the policy program receives sufficient time and resources. Third, and in consequence, the necessary combination of resources is actually available. Fourth, the policy is implemented based upon a valid theory of cause and effect (in other words, that they are not "bad policies" (Hogwood & Gunn, 1984, p. 201)). Fifth, the relationship between the cause and effect of a policy approach is direct and minimizes intervening variables. Sixth, that the dependence relationships are minimal. Seventh, that all the parts understand and share the objectives of a policy. Eight, that the tasks are fully specified and in correct sequence. Ninth, that there is perfect communication and coordination between the involved agencies (Hogwood & Gunn, 1984, pp. 199–205). Mazmanian and Sabatier make a similar checklist, in both content and extension, of conditions for the implementation of policy (1983).

With most literature on implementation focused on the US, at the EU level most research has focused on the upper most formal level of implementation, the transposition of Directives (i.a. Bursens, 2002; Dimitrakopoulos, 2001; Mastenbroek, 2003), and questions of practical implementation have largely remain largely unexplored (exceptions being i.a. Demmke & Deakin, 2001; Falkner, 2005; Falkner, Hartlapp, Leiber, & Treib, 2004; Falkner, Hartlapp, & Treib, 2007; Versluis, 2007). As Versluis points out EU scholars tend to use the concept of implementation to explain two different processes. First EU scholars use implementation to explain the transposition of a Directive into national law. We can call this the formal implementation of EU law. Second, to explain the establishment of the administrative agencies, the enforcement by regulators (the monitoring and inspecting), and the compliance by the regulated (2007). Referring exclusively to EU policies, Versluis theorizes that the compliance and enforcement of directives at the national level *always* happen when the issue that the directive deals with becomes high salient – the question of what happens when the issue is not high salience remains open (Versluis, 2007, p. 63).

Understandably dissatisfied, Bo Rothstein calls the literature on implementation "misery research" and wonders if it is "a pathology of the social sciences", since it mostly focuses on cases of policy failure, in areas where policy has high chances of failing, and doing so with an excessively mechanistic and rationalistic view of the process of implementation (Rothstein, 1998, pp. 63–64).

Thus, Rothstein calls implementation researcher's often-made recommendation that policies must have clear and precise objectives (Mazmanian & Sabatier, 1983; Hill & Hupe, 2014) "at best naïve, at worst downright dangerous" (Rothstein, 1998, p. 77). He argues that sometimes, for example in events of changing technological development, policymakers are obliged to take measures with uncertain knowledge either about the direct effect that they might have or the prevailing conditions when those policies are applied. For example, no one would dispute that a state should not have a defense policy based on not knowing if such policy will help the country to win a war or defend itself from unknown threats or if the developed programs will still be relevant in an era of changing threats and technologies. Sometimes the most we can ask for a policy is both for to it be designed as flexible and adaptable, and for its implementation to be flexible and adaptable (Rothstein, 1998, p. 77). As Baumgartner and Jones's point out, *a priori* policy can only demand policymakers clarity and conciseness in engineering problems (such as building a bridge, when the technology to solve the problem is straightforward recognizable) and not for wicked more complex policy issues (2015, p. 32). For a policy that treats a complex issue as engineering one is destined to fail.

As Rothstein reflected, in dynamic and complex policy areas such as the regulation of privacy in the digital era, one cannot expect policymakers to foresee all possible risks and for the compliance of such policy to be perfect at all times, all the times (Rothstein, 1998). Granted, since implementation is an itinerary endeavor (Majone & Wildavsky, 1979), it would be unrealistic to consider that a policy did not achieve its goals if there were some cases of incompliance during some moments in time –after all, enforcement exists *to* guarantee compliance. However, if the failure in compliance is massive and extended in time, we can consider that a policy failed to achieve its goal.

More concretely referring to the checklists for the study of successful implementation that were and still are popular in implementation research, Rothstein criticizes that they say "nothing, for example, about which factors are more important than others, and under which conditions, or which types of programs are harder to implement than others, and it does not say much about which organizational forms are suitable for which tasks", since after all, the fact that programs that lack sufficient resources might fail is hardly a surprising notion (Rothstein, 1998, p. 69). But just as Rothstein (1998) fairly criticizes the checklists for implementation analysis (Gunn, 1978; Mazmanian & Sabatier,

1983) for not identifying which factors are more important than others, one should be cautious of more complex theoretical frameworks that include a multitude of layers and variables without making a clear distinction between critical and non-critical variables and relations (Hill & Hupe, 2014; Meter & Horn, 1975). After all, as Argentine novelist Jorge Luis Borges warned in *Del Rigor en la Ciencia* (1948) (translated to English as *On Exactitude in Science* or *On Rigor in Science*) a map of the Empire the size of the Empire is as useless as no map at all –in other words, if everything is important, nothing is.

Fortunately, Rothstein gives a first approach to a general theory of implementation that will be used in this paper (1998, Chapter 4).

Analytical framework

To "assist in the formulation of a more general theory of policy implementation", Rothstein (1998, p. 71) argues that it is possible to distinguish between two main factors deserving of research associated with a policy's failure to achieve the desired outcomes. First, the researcher should identify if the failures lie in the design of the program as such, and second if the failure lies in the organization of the implementation process. This is all made considering that "the basic idea is simple enough –that any program, however cleverly designed it may be, will fail if its implementation is entrusted to an organization unsuited to the purpose" (Rothstein, 1998, p. 71)[21].

These areas can be further divided into questions of process and substance. Substantive problems concern how the goals of the programs can be modified to accommodate the attempts of the clients of the program or the officials to achieve or obstruct its implementation. Process problems refer to how the different levels and the different agencies of the administration can be made to operate together. The analytical model has, then, four categories. First, the substance of policy design. Second, the process

[21] It should be noted that presenting his approach to a general theory of implementation in a book dedicated to the "moral and political logic of the universal welfare state", which discusses sensitive issues such as the targeting of social problems to vulnerable population (and the definitions and issues that might arise from such endeavor), Rothstein introduces the area of *political legitimacy* (Rothstein, 1998). *Political legitimacy*, he argues, is important since it calls into consideration that a policy might be perfectly designed and organizationally implemented but still fail if the target group resists or is hostile to its implementation. This area is not considered in this paper, since the policies that occupy it are not related to the welfare state.

of policy design. Third, the substance of the organization. And fourth, the process of the organization.

- First, the substance of policy design refers to the somehow obvious idea that no matter how much effort an organization or bureaucracy puts into implementing a policy, it will fail if it was poorly designed or conceived. In the broader implementation analysis world this is referred as the failure in the causal theory behind a policy (Hill & Hupe, 2014). And sure enough, if for example a job training policy for the unemployed instructs in professions not demanded by the market, it is destined to fail from the beginning. Similarly, as it is argued in this paper, a privacy policy that exempts the intelligence agencies from compliance and is not accompanied by meaningful democratic legislative oversight of the spies to prevent violations on citizen's privacy is also destined to fail.

Rothstein argues that another reason why a policy might be poorly designed is if it is result of symbolic policies. Sometimes programs are created under the assumption that the measures applied are not intended to have any other effect than showing to the public that something is being done to remedy a widely felt problem. When there is popular demand for state action, politicians feel they need to respond by offering a plan or a program. Such program serves thus the purpose of enabling politicians to show that something is being made, without the substance or the design of that something being carefully considered.

- Second, the process of policy design refers to how and in which context the decisions regarding the policy were made. Policies are usually the result of political negotiation and compromise that happens in a certain context with a certain understanding of how policies should look. More concretely, compromise can lead to three shortcomings. The first one is that the objectives of the policy are unclear or even impossible to understand. Sometimes politicians perceive that there are no costs in being more generous in the goals of a certain policy and turn bills into undeliverable wish lists. Other times politicians feel they need to act to show responsiveness to popular demand, but are less clear on what is that should be done to target a specific issue and that is reflected in the final legislation.

The second possible shortcoming is that legislators overestimate their capacity to foresee the future and possible implementation issues in dynamic policy areas and make overly prescriptive laws that make the task of the bureaucrats impossible –especially in dynamic policy areas, the legislators should provide with a framework for achieving the desired goal, not the impossible dream of providing precise answers to any possible scenario that might arise.

The third possible shortcoming is a product of the different levels of the political system, and the possible divergence of political majorities across them. The political opposition at the highest level might have the majority at a lower level closer to implementation and oppose the totality or the partiality of the policy restricting implementation. This kind of political conflict might derail the implementation of many policies at the EU, the US, and between them. Cooperation between different levels of governance and an iterative implementation process is then fundamental to guarantee correct implementation.

- Third, the organizations implementing a policy must count with the human, institutional and financial resources required to perform the task they are entrusted and that the resources must be allocated in a dynamic manner to be able to adapt to changing circumstances. This is simple enough: if the implementing organization does not have the necessary resources, in the right amount, and at the right moments, it does not matter how clever an institutional design might be, the implementation will not live to the expectations.
- Fourth, the organization as a process refers to how to best deal with responsibility drift, the situation in which the power over a decision on a policy drifts apart from the responsibility for carrying it out. Responsibility drift poses two main problems for policy implementation. First, that policymakers might be tempted to be overly ambitious or prescriptive with a policy since they might be far away from the implementing level, and opt to prescribe limits to the room for maneuver of bureaucrats. Especially in dynamic policy-areas legislators need to give the implementing agencies some maneuvering space to be able to adapt to changing circumstances.

The second is that that policymakers may neglect centralization in the implementation process regardless of how decentralized a policy system might be –in

other words, policymakers should remember that coordination among decentralized agencies is possible and might be desirable under certain scenarios. Especially in federal systems, but also in the EU, there are incentives for policymakers to demand results in the parts expecting a common outcome in the whole forgetting that coordination among the parts is fundamental for achieving the expected result. Policymakers should provide the sufficient tools for sub-national coordination.

The analytical narrative, following, describes first how both American and European legislators discovered state-surveillance but are unwilling to put checks on intelligence agencies either through privacy policies or by exercising effective oversight. The privacy policies and intelligence oversight mechanisms of the US, UK, France and Germany are analyzed. Oversight mechanisms are a fundamental part of the story since they could provide a complement to the exceptions created for intelligence agencies in privacy policies. The second part of the analytical narrative discusses the consumer privacy aspect of the American and the EU privacy regimes.

Analytical Narrative - Part 1: State Surveillance

Discovering Big Brother in America

Governments need information. Modern, complex welfare governments need lots of information. How to produce the information necessary for the needs of modern governing became an important issue for public officials across the Atlantic following World War II. Between 1950 and 1970 the amount of civilian employees of the US federal government had increased by 50% (Porter, 2002, p. 70), and similar trends were seen in Europe (Rose, 1985). Now in charge of providing all kind of services, from health and education to the masses to internal policing, governments started to look for mechanisms to be more efficient and effective in how they performed their tasks. And the computer was the answer (A. Newman, 2008, p. 44).

Like the modern complex state, the computer was largely a by-product of World War II. Companies and governments quickly adopted computers for their day-to-day operations, and eventually governments decided to create national data banks linking the information dispersed in different individual data banks to enhance efficiency and oversight of public and private services. In 1965 the US Social Science Research Council proposed to create one of the first data banks, to link the data collected by various

government agencies to centralize the access to that information, and one year later the Bureau of the Budget followed the lead and established the National Data Center to centralize twenty data banks of other agencies (Flaherty, 1979; Regan, 1995).

The public reacted with suspicion to the emergence of the powerful super-informed government. On the 27 of July 1966 *The Washington Post* dedicated part of its front-page to a Senate hearings on the creation of the Social Science Research Council data bank, explaining in an article entitled "Data Center Hearing Warned on Privacy" that some of the expert witnesses have described the plan as "a threat to individual liberty, a harbinger of Big Brother, and a mechanized suffocation of the American dream" (Lardner, 1966; see also Kreitner, 2015). But it was not until the eruption of scandals related to the new surveillance powers of the state that privacy entered the policy-agenda and politicians started to seriously debate the creation safeguards against massive personal data collection and processing.

The 1972 Watergate scandal, that obliged President Nixon to resign for being suspected of ordering spying on the opposition Democratic party (A. E. Lewis, 1972), triggered the 70s "Season of Inquiry" on the work of the surveillance agencies (Johnson, 2015; Olmsted, 2000). During the various hearings held by the Pike Committee and the Abzug Committee in the House and the Church Committee in the Senate, American legislators and the public learned about several invasions of their own privacy at the hands of the intelligence agencies created to protect them. The work of the Committees made for the first time official reference to the NSA revealing, among other things, joint NSA-FBI operations against US citizens, including civil rights activists such as Martin Luther King Jr. and Senator Church himself, and NSA's tapping of undersea cables for the telex communications of governments, business and private individuals (Burnett & Games, 2007, p. 946; Johnson, 2015, p. 81; Wood & Wright, 2015). The programs revealed in the 1970s were, hence, precursors of the programs discovered in the 1990s and the 2010s.

The shock caused by these massive revelations created an informational positive feedback loop (Baumgartner & Jones, 2015, p. 54; see also Pierson, 2004) that eventually lead to regulation to protect the privacy of Americans and attempt to control the intelligence agencies, principally in the 1974 Privacy Act. However, American legislators provided intelligence agencies with exceptions for compliance with the 1974 Privacy Act.

This could easily be understood as a substantive and conscious failure in the substance of the policy design: the problem (state-surveillance threatening citizen's privacy rights) is identified, but legislator's preference is to not address it. In fact, there is no evidence that the control of the intelligence agencies was ever considered as a possibility by policymakers. Even the vocal privacy advocate Senator Ervin (who during the 1970s defended a more stringent Privacy Act) defended exceptions for national security reasons for "national defense [and] criminal investigatory flies of Federal, State or local law enforcement agencies" (US Senate, 1974, p. 354). According to the existing evidence, policymakers were unwilling to exercise governance over the intelligence agencies.

Perhaps, given the dynamic nature of intelligence agencies, policymakers opted for other ways of governing their behavior to guarantee American's privacy. Thus, one could read the 1978 FISA or the 1980 Intelligence Oversight Act as complementary to the Privacy Act, since they provided formal controls over the intelligence agencies. However, the design and implementation of these laws reveal they were enacted without an equivalents at the state level—and thus more prone to fail. In theory, FISA precluded agencies such as the NSA from domestic surveillance, although the provision of very limited controls was "easily bypassed by the NSA" (Wood & Wright, 2015, p. 133) principally through cooperation with GCHQ, as all the evidence exposed by Snowden reveals (Glenn Greenwald, 2014; Poitras, 2015). FISA also established the Federal Intelligence Surveillance Court (FISC). Scholars have considered that the role of FISC is compromised since it is composed by handpicked judges that meet in secret in the Justice Department to decide on applications for surveillance that involve American citizens, permanent resident aliens or American companies (Mayer, 2002; Seamon & Gardner, 2004). All sources indicate that up through 2015, never has the FISC refused an application for surveillance (Glenn Greenwald, 2014; Mayer, 2002; Wood & Wright, 2015).

The Congress and the Senate have secret and classified committees on intelligence, which agencies are obliged to report to, keeping them currently and fully informed, thanks to the 1980 Oversight Act. However, there are notorious institutional shortcomings for the effective functioning of the committees. For example, serving Congressmen and Senators that are not members of those committees are barred from accessing to *any* information on

the work of the agencies or the FISC (Gleen Greenwald, 2013). There seems to be a clear lack of legislators' will for effectively overseeing the spies. For example, between 1974 and 1975, at the height of congressional inquiry over state surveillance, 200 proposals to increase oversight over intelligence agencies were presented in the US Congress and only one adopted (Kibbe, 2009, p. 26). In fact the flaccidity of congressional oversight is such that even former Directors of the CIA (DCI) criticize it (H. Born et al., 2005, p. 69). In a testimony to congress former DCI Colby said: "Congress is informed to the degree Congress wants to be informed" (US Congress, 1984, p. 33).

In sum, the previous paragraphs have shown how the United States established privacy rules with exceptions for intelligence agencies after discovering privacy invasions enabled by privacy agencies. The United States also created oversight mechanisms to guarantee that intelligence agencies respect American's privacy. However, there are several limitations in the functioning of oversight structures. How does Europe compare to America? The next section explores how the European Union and its member states protect their citizen's privacy from state-surveillance.

Europe

In France, between 1972 and 1974 the media reported on the secret existence of the SAFARI project. The heir of the Vichy's regime created SAFARI as an attempt to centralize the governmental database of personal data, and was perceived as an intrusion of people's privacy (Mattelart, 2010, p. 121). The debate generated by SAFARI culminated in the creation of a privacy watchdog, the *Commision Nationale de l'Informatique et des Libertés* (CNIL) with the goal of enforcing a law on technology and freedom, *Loi Informatique et Libertés*, passed in 1978 (Mattelart, 2010, p. 122; A. Newman, 2008, p. 46).

The 1978 *Loi Informatique et Libertés* can be considered a precursor of the 1995 Directive for two reasons. First, being the cornerstone of a comprehensive privacy framework, it mandated the creation of an independent DPA (the CNIL) in charge of guaranteeing the protection of privacy rights in the process of personal data made by public or private agents (Vitalis, 2008). Second, despite being a reaction to what seemed to be an intrusion of the powerful state machinery in people's lives, the law allowed the

government to use personal files when it was necessary for national security reasons, without any of the stipulated controls and safeguards. As *Le Monde* noted in 1980, after the publication of the first CNIL report: "one of the weaknesses of the *Loi Informatique et Libertés* is that it allows the administration to use personal files without any real controls when those files are of interest to defense and 'public safety', in the broad sense of the term" (Le Gendre, 1980). Again, we identify a failure in the substance of the policy design.

As a remedy, since 1991 the office of the Primer Minister has available the advice of an oversight body, the *Commission nationale de contrôle des interceptions de sécurité* (CNCIS). The CNCIS has structural difficulties to act as an oversight executive agency for the French surveillance agencies: it is composed by three judges, one secretary, and one driver (Johannès, 2015) that according to experts probably was not consulted on the Internet surveillance activities committed by the French secret service agency in collaboration with the NSA during the 2000s (in Bigo et al., 2013, p. 52). In this case, we see a failure in the substance of the policy design and in the allocation of resources to the implementing organization.

In general, the majority of French legislators never have shown a strong will to gain oversight power over the intelligence agencies. Between 1985, 1989, and 1999 the biggest French political parties (including the Socialists and the *Gaullist* conservatives) declined to include in the parliamentary agenda four bills aimed to create intelligence oversight committees presented in the 1980s by the Communist Party and in the 1990s by some Socialist and conservatives legislators acting as independent political entrepreneurs (Lotz II, 2007, p. 134; Wills & Vermeulen, 2011, p. 207). The former Chairman of the Senate Defense and Foreign Affairs expressed this lack of will and "denounced public oversight of the secret services through parliament as nonsense. Parliamentary control is too dangerous" (Porch, 2003, p. 466). Only in 2007 the French assembly received some control powers over its intelligence services (FRA, 2015, p. 38) Hence, according to the French Government, the lack of regulation and oversight of the French intelligence services largely continued until the 30 of June of 2015 with the approval of an Intelligence law modeled in the American Patriot Act, to correct the fact "that France was one of the last Western democracies not to have a comprehensive and consistent legal framework to govern the activities of its intelligence services" (Gouvernment.fr, 2015).

According to reports commissioned by the EP's Committee on Civil Liberties, Justice and Home Affairs (LIBE), the French Parliament oversight of its intelligence services is defined as "relatively weak" since all requests for classified documents are rejected by the agencies –who argue that they cannot share that information since it was shared to them by other agencies- and parliamentarians have "no right to hear or question a member of a defined intelligence service", and only the directors can be subject to official hearing (Bigo et al., 2013, p. 52; see also Wills & Vermeulen, 2011). The French political system never even seriously considered the alternative of more regulation over its intelligence agencies.

At the European level, by the early 1990s Germany, Sweden, France, the United Kingdom and the Netherlands had adopted comprehensive privacy frameworks, but other important countries such as Spain and Italy had not (Rule & Greenleaf, 2010). As recounted by Newman, the DPAs of the countries, with comprehensive protection threatening to blocking the transfers of personal data of their citizens to other countries that did not count with a privacy framework, effectively putting at risk the European Single Market and blocking the European integration process, to achieve a common European framework: the 1995 Directive (A. Newman, 2008). Like all the precedent European privacy laws, the 1995 Directive establishes clear rules for the processing and collection of personal data by public and private actors, and it contains explicit exceptions for law enforcement or national security reasons, among other things because national security was outside the regulatory scope of the EU (Bignami, 2007). Therefore, for the compliance with the principle of exceptionality of the 1995 Directive to surveillance agencies and for avoiding a policy design failure, European legislators had to rely on their national peers, which a priori supposes a serious challenge to the ambitious goals of Directive and opens the door for a possibly fatal responsibility drift. Hence the importance of revising the oversight mechanisms of such agencies in the UK and Germany, having already done so for France and thus covering the most important EU intelligence actors.

The UK's 2000 Regulation of Investigatory Powers Act (RIPA) establishes a framework for the regulation of the intelligence agencies such as the GCHQ or the MI5 and MI6. RIPA demands that agencies get a warrant approval by the Secretary of State for spying on UK nationals, but allows agencies to indiscriminately collect information that has origin outside the UK or that involves at least one non-UK national by just getting a

certificate signed by one of the members of the Cabinet (Bigo et al., 2013, p. 44; MacAskill, Borger, Hopkins, Davies, & Ball, 2013b).

The oversight of the UK's intelligence services falls onto the Parliament's Committee of the Intelligence and Security (ISC, consisting of nine members of both chambers), the Interception of Communications Commissioner (IoCC) the Investigatory Powers Tribunal (IPT, an institution similar to the FISA Court that cannot initiate its own investigations), and the National Security Council (NSC, a Cabinet committee in charge of all issues regarding national security). Regarding the NSC, former member Secretary of Energy and MP Chris Huhne (2010-2012) declared that "the cabinet was told nothing about GCHQ's Tempora or its US counterpart, the NSA's PRISM, nor about their extraordinary capability to hoover up and store personal emails, voice contact, social networking activity and even internet searches […] If anyone should have been briefed on PRISM and Tempora, it should have been the NSC" (Hopkins & Taylor, 2013). As for the ISC, regarding the NSA's PRISM program (Ball, 2013), it "concluded that GCHQ has not circumvented or attempted to circumvent UK law" (ISC, 2013, p. 2).

Concerning the IPT, GCHQ consider the body as friendly in internal communications to the NSA, arguing that "so far they have always found in our favor" (MacAskill, Borger, Hopkins, Davies, & Ball, 2013a). However, in a recent ruling, the tribunal considered that GCHQ's access to data collected by the NSA in the PRISM program was unlawful for seven years, until December 2014 when the previously secret intelligence data agreement between the UK and the US was made public—the IPT ruling did not mention any possible violation of privacy or call for and end to the program or to the cooperation between GCHQ and NSA (IPT, 2015).

In Germany, the oversight function of the secret service agencies falls principally in the G-10 Committee, named after the 10th Article of the German Constitution and composed by four members of the German Parliament that not only authorize surveillance requests, but also check *how* the collection, storage and analysis of personal data is carried out –something that the other European and the American oversight systems do not do. The Parliament has also its own Control Committee independent from the G-10, PKGr, composed by 11 members and with the prerogative of obtaining all the information it considers necessary from the executive (Bigo et al., 2013, p. 56), and is obliged to report

at least once every six months to the PKGr on the activities of the agencies. Likewise, the PKGr can request to make its otherwise confidential deliberations public with a two-thirds majority (Heumann & Scott, 2013, p. 13). Nevertheless, it is important to mention that in the parliamentary inquiries following the revelations of cooperation between the NSA and the BND, it was revealed that the Chancellery intervened and prevented the G-10 and the PKGr from investigating BND's tapping one of Europe's most important infrastructures used by Internet Service Providers to exchange Internet traffic between their networks located in Frankfurt (Frankfurt's Internet exchange point), for sharing information of German citizens to the NSA (DW, 2014).

Networks of spies

As a consequence of lack of effective oversight on their activities, surveillance agencies' cooperation has gone beyond the links so far illustrated between the NSA and its European partners. Intelligence agencies have built formal and informal networks between them to increase their geographical and technical reach beyond what is permitted by their resources economic, human or technological (Rudner, 2004; Sepper, 2010). Born out of need during the World War II and the Cold War (Aid & Wiebes, 2013), these networks have evolved and now permit the agencies to by-pass their legislative limitations on domestic surveillance by accessing data of their nationals collected by other agencies (Heumann & Scott, 2013; as recognized in a report of the EP, Schmid, 2001, p. 134). The lack of active oversight allows this networks to exist without legislative control.

The most well-known of this networks is the Five Eyes alliance between the NSA, GCHQ and the intelligence agencies of Canada (that temporary suspended its participation in the network in January 2016 (CBC News, 2016)), New Zealand and Australia. Formally called the 1974 UKUSA Agreement, the Five Eyes are known to be behind the infamous ECHELON network, a global system for the interception of private and commercial communications that caught the attention of the EP in the late 1990s and early 2000s (Perrone, 2001; Schmid, 2001; Wright, 2002) and that is a predecessor to PRISM and TEMPORA. Once again, we have evidence of information of European policymakers regarding state surveillance.

Sepper reminds us that Five Eyes is "an aberration both in its formality and its degree of integration" (2010, p. 157), since otherwise there is a plurality of ad-hoc informal networks between agencies that go unreported to the national oversight bodies for being usually constituted through memorandums of understanding (MoUs) that specify the modalities of information exchange (Lefebvre, 2003). Being non-binding, soft-law agreements MoUs serve to regularize the contacts and cooperation between individual agencies without requiring the approval of oversight bodies or Parliaments (Slaughter, 2001, p. 359). For the intelligence agencies these networks are fundamental since they allow them to access to information they otherwise could not get for legal reasons or for lacking the resources. Usually, the agencies cannot disclose to third parties the information given by them by other agency in virtue of an agreement or network.

Product of those intelligence cooperation networks the German BND and the NSA have a joint eavesdropping station in the Bavarian town of Bad Aibling (Gude, Poitras, & Rosenbach, 2013), used by the NSA to spy on German and European companies at BND's complains (Spiegel, 2015). Furthermore, documents leaked by Snowden to *The Guardian* reveal that GCHQ has "been assisting the BND […] in making the case for reform or reinterpretation of the very restrictive interception legislation in Germany" (Borger, 2013) and that the French agency DGSE was meeting with GCHQ to assist it with decrypting technology developed by France (Borger, 2013).

Final remarks

The three presented papers of this dissertation are stand-alone, distinct contributions each addressing different, but closely related, empirical puzzles that contribute to the literature on Internet privacy. The first article starts by exploring some of the tangible consequences of the Snowden revelations and challenges the common-wisdom culturalist theories of Europe's privacy regime. Then, the second article offers a new explanation of the origins of America's privacy framework that also defies conventional culturalist explanations. Finally, the third article closes by offering a novel implementation and policy design analysis of the American and European privacy regimes.

Each article employs slightly different research methods and uses different yet compatible and complementary theoretical frameworks. In general, this dissertation adopts an

institutionalist perspective studying how and why certain institutions change, and "why some flourish in some context and/or why some die out in others" (Steinmo, 2003a). The first article focuses on institutional reform, and resistance to institutional reform by corporate actors, following Culpepper's quiet politics framework (2011). The second article, borrowing from Steinmo (2003b) and Blyth (2002, 2011), discusses the interaction between ideas and institutions, following perhaps the clearest institutionalist narrative of all the pieces of this dissertation. The third article, building on Rothstein's general theory on implementation (Rothstein, 1998) discusses the implementation and policy design of the European and American institutions for the protection of privacy.

Analytical Narrative - Part 2: Consumer privacy

An American problem?

The three presented papers of this dissertation are stand-alone, distinct contributions each addressing different, but closely related, empirical puzzles that contribute to the literature on Internet privacy. The first article starts by exploring some of the tangible consequences of the Snowden revelations and challenges the common-wisdom culturalist theories of Europe's privacy regime. Then, the second article offers a new explanation of the origins of America's privacy framework that also defies conventional culturalist explanations. Finally, the third article closes by offering a novel implementation and policy design analysis of the American and European privacy regimes.

Each article employs slightly different research methods and uses different yet compatible and complementary theoretical frameworks. In general, this dissertation adopts an institutionalist perspective studying how and why certain institutions change, and "why some flourish in some context and/or why some die out in others" (Steinmo, 2003a). The first article focuses on institutional reform, and resistance to institutional reform by corporate actors, following Culpepper's quiet politics framework (2011). The second article, borrowing from Steinmo (2003b) and Blyth (2002, 2011), discusses the interaction between ideas and institutions, following perhaps the clearest institutionalist narrative of all the pieces of this dissertation. The third article, building on Rothstein's general theory on implementation (Rothstein, 1998) discusses the implementation and policy design of the European and American institutions for the protection of privacy.

Endogenous European limitations

At this point it would be easy to argue that the problems with European's consumer privacy are solely due to the lack of enforcement of rules by American authorities. However, privacy experts have highlighted several times the "structural difficulties" of EU DPAs (Bowden, 2013, p. 31; see also FRA, 2013; IAPP, 2012). Both the American and the European agencies lack the appropriate resources to implement the 1995 Directive and Safe Harbor. In a report commissioned by the EP, Bowden reflects, "DPAs clearly lack capacities in technical expertise. Only a few dozen DPA staff (out of about two thousand across Europe) have an informatics background, let alone a post-graduate degree related to the computer and engineering science of privacy. There is a deeply-rooted view that because in general it is preferable to draft laws in a technology-neutral way, this excuses regulators from understanding technical matters" (2013, p. 31). These findings are consistent with those of the latest available global survey of Data Protection Authorities of the International Association if Privacy Professionals (IAPP) of 2011 (IAPP, 2012), that show that only 10% of the resources of the DPAs go to investigation or enforcement and with survey by the FRA (FRA, 2013). Likewise, it is telling that in 2004, 2011, and 2015 the WP29 has denounced the lack of consistency in the enforcement of the 1995 Directive for lack of powerful DPAs equipped with the necessary resources (WP29, 2004, 2011, 2011). Without adequate resources we cannot expect implementing agencies to deliver the goals of any policy.

EU legislation in general is highly exposed to responsibility drift failures, which makes efficient and effective cooperation between agencies even more important. National and subnational agencies often implement the decisions taken in Brussels and are almost completely unaccountable to the supranational institutions. When Brussels legislates through Directives, these national and subnational agencies follow *national* interpretations of the policies designed in Brussels. In some policy areas the EU had attempted to solve this responsibility drift, as is the case of competition. The EC centralizes the responsibility of implementing EU-wide regulation in competition when there is a conflict that affects more than one Member State (Barros, Clougherty, & Seldeslachts, 2012). Regarding privacy protection, EU legislators have expected to find in the WP29 a network of coordination among regulators to solve the responsibility drift issue. However, as denounced by the DPAs themselves, the lack of resources of the different DPAs has made cooperation difficult and insufficient to overcome the many challenges of implementing

national and transnational privacy policies in the digital age (FRA, 2013; IIEA, 2015). And while a new European Data Protection Board is supposed to replace and strengthen the WP29, it is still to early to say if this institutional innovation will suffice to solve EU's DPAs problems.

It is also possible to see divergence among the EU member states and the EU DPAs through Ireland's implementation of the Directive (i.a. Fleisher, 2015; Tighe, 2012), because until 2013 it was assumed that the Irish DPA was the *sole* authority with power over companies located in the country regardless of where in Europe they would operate (Piltz, 2013). And while that assumption has been challenged by two ECJ rulings (2014 and 2015) that determined that DPAs have authority over companies operating in their territory regardless of the location of their headquarters (De Miguel Asensio, 2015; Lynskey, 2015), the proposal for a General Data Protection Regulation (GDPR) to replace the 1995 Directive includes a provision for a "one-stop shop" that promises business that they will have to deal only with the authority of the country were their main European office is (EC, 2015; see also Kuner, 2012) –nevertheless, the fine print of the one-stop shop mechanism remains to be seen.

Concerns about the Irish DPA enforcement capabilities have existed for a long time. The Irish DPA is in charge of guaranteeing the compliance with the privacy rules to many Internet giants such as Facebook for all Europe, and many observers believe that it is not a strict enforcer of Europe's privacy rules. For example, Max Schrems, the activist who brought the case that triggered the invalidation of Safe Harbor by the ECJ, considered that "the Irish authority is miles away from other European data protection authorities in its understanding of the law, and failed to investigate many things" (in BBC, 2012). While thanks to a 2015 decision by the Irish government to strengthen it, the DPA now has offices in Dublin, a considerably bigger budget and consequently a larger staff, until that year the Irish DPA was exclusively located in Portarlington, a small town 80km from Dublin, and operated with a very small and unspecialized personnel (Fleisher, 2015).

Ireland, has performed audits on companies such as Facebook and obliged them to make changes in their privacy policies for European users (O'brien, 2012). However, the problems generated by the location of the authority and its lack of resources were acknowledged by the head of the Irish DPA, Helen Dixon, in a 2015 keynote speech to an Irish think-tank: "criticism about the [DPA] being located exclusively in Portalington, are

probably merited. The [DPA] needs to have premises in Dublin in order to effectively deal face to face with the many government tech quarters and also companies that are located in the capital […]"(in IIEA, 2015). She also added that "the [DPA] office has been under-resourced in terms of staff quantity terms but also in terms of specialists skills over the last number of years and in addition we have had insufficient investment in terms of the back office systems that we are using" (in IIEA, 2015). Dixon also attributed insufficient resources to the lack of effective cooperation with other EU DPAs in the framework of the WP29, and with the FTC for international enforcement (IIEA, 2015).

After all, it is worth noting that in 1996, when less than 3% of the Irish had access to the Internet and Facebook's founder Mark Zuckerberg was only twelve years-old, the budget of the Irish DPA was of an equivalent of 2015 1,2 million euros (Irish Data Protection Commissioner, 1998) and in 2012, the budget had only grown by less than a million euros (Irish Data Protection Commissioner, 2013). The evident and acknowledged material limitations of the Irish DPA clearly negatively affected its capacity to cooperate with its peers and enforce the EU privacy laws on large Internet companies. Peter Schaar, former head of the German DPA, perfectly summed up this distrust of many Continental regulators on their Irish peer: "Of course Facebook would go to a country with the lowest levels of data protection […] It's natural they would choose Ireland" (in Scott, 2015).

The lack of resources of DPAs fatally intensifies some of the intrinsic challenges of the 1995 Directive – including the fact that is a Directive. Directives are clearly exposed to failure due to responsibility drift. As mentioned, experts have long criticized the lack of resources of the American and European privacy agencies (i.a. Adriance, 2015; Bowden, 2013; Chris Connolly, 2013; FRA, 2013; Hartzog & Solove, 2014; Maass, 2012). A recent FRA report found that lack of resources, particularly human talent, impedes DPAs from enforcing legislation for consumer privacy: "Some of the representatives of the DPAs stated that the amount of work that the DPA currently had was at the upper limit, and they could not handle more with the resources available (e.g. DPA staff from Finland, Poland, Portugal and the United Kingdom)". (2013, p. 46). For example, a staffer of the Dutch DPA declared: "it is sometimes frustrating that we cannot process certain things just because we do not have the capacity" (in FRA, 2013, p. 46).

In sum, as it was shown, the lack of resources of DPAs together with Safe harbor has impeded the 1995 Directive from achieving its policy goals.

Conclusion

This article has shown how the design and implementation of the American and European privacy frameworks explain why they did not achieve their expected goals. Policymakers might enact legislation that creates governance structures without being willing to either address some important issues in a certain policy area (in the case of data protection, the role of intelligence agencies) or without giving sufficient resources to the implementing agencies. This might create formal governance institutions that, upon closer examination, do not provide the expected level of steering of a certain field. The study of the variation in policies among and within jurisdictions gives researchers important information about political processes in an attempt to provide governance insights. But too often we only tend to assume that variation in policies translates in divergence in results without clear evidence.

The study of policy design and implementation efforts is fundamental for understanding governance. Only by studying the actual steering capacity of identified governance schemes we can conclude that, effectively, we are correctly identifying the actors exercising governance. In the case of data protection, this article shows that more attention should be given to understanding *who* and *how* governance gaps left by the European and American privacy policies are filled. By better understanding the limits of state-driven governance we can start understanding Internet governance beyond the state (Eeten & Mueller, 2013) and building a third wave of global governance research that is more capable of identifying effective governance structures for the provision of policy goals (Coen & Pegram, 2015).

More concretely, this article has proven how given the lack of oversight, European and American intelligence agencies have chosen to create informal alliances between themselves to overcome domestic limitations and maximize their power and internal interests at the expense of their own citizen's privacy. The previous pages have also shown how this turn of events was foreseeable by policymakers who, after being alerted to the massive surveillance programs of their own intelligence agencies, many times triggered the design of privacy rules only to then exclude the intelligence agencies them from regulation.

This article has not tried to discredit political compromise. Many times politicians do not enact the laws they would like to enact, but they laws they can enact. This paper does call to question what are the consequences and the origins of political compromise. Perhaps the kind of flawed privacy policies presented in this article are the best policymakers can offer. But then the study and analysis of such policies should be revised in the light of the consequences of the compromises that shaped them.

V. Concluding remarks

What can this dissertation contribute to the common understanding of Internet privacy in the wider field of Internet governance? In general, this dissertation proposes that more studies on implementation and on the relation between privacy and surveillance are necessary to understand what are the effects of privacy laws and bureaucracies. It also argues that relying solely in cultural understandings of societies is important but is also incomplete in explaining institutional change. Neither the changes in the EU privacy framework or the origins of the US privacy framework can be explained relaying solely in culture. The first article has argued that in absence of the Snowden revelations the EU would not have strengthen its privacy rules. The second article that political culture is not responsible for the lack of a comprehensive privacy regime America. The reason why America is an outlier in privacy protection is because the predominant policy paradigms that determine what is possible and desirable were biased against comprehensive privacy reform.

Furthermore, the study of the implementation and policy design of the American and European privacy frameworks calls to question the meaning in practice of the contrasted variation in bureaucracies and laws for privacy protection. American and European legislators have no rational incentives to control their intelligence agencies or to provide with more resources to data protection authorities. As a consequence, neither the American nor the European privacy regimes have the expected governance effects. Therefore, while it is true that America and Europe have radically different laws and bureaucracies to protect the privacy of their citizens it is less clear if Americans and Europeans have different expectations of privacy –since as I argue both regimes are seriously flawed.

Empirical contributions

Although each article was intended as an independent stand-alone piece on different empirical puzzles that contribute to the field of Internet privacy there are some important points in the studies that I would like to point out.

First, the papers show the limitations of primalist culturalist accounts for understanding the American and the European Internet privacy regimes. Although

Newman and Farrell had already established that the origins of the European privacy regime cannot be attributed solely to the lessons of the fascist governments that ruled Europe in the 20th century (H. Farrell, 2002b; A. Newman, 2008) the idea that America is an outlier in privacy protection because of the underlying individualism and anti-statism of American culture is still widespread. The first article explains how Europeans only reacted against corporate attempts to water-down their privacy rights because of the revelations made by Snowden. The second article argues that America could have had a comprehensive privacy regime like all other advanced nations would not have been the overarching policy paradigm in which legislation was proposed.

Second, this dissertation has shown one of the explicit and concrete effects of the Snowden revelations: the approval of a privacy-strengthening GDPR by the EP. Unlike the predictions of cultural accounts, I have shown how privacy advocates leveraged on the Snowden revelations to beat the organized corporate interests that heavily lobbied against the GDPR. The first article showed how corporations influenced the EP during the GPDR parliamentary process and also how the Global Surveillance Revelations made by Snowden tangibly affected the Internet privacy debate in Europe. The Snowden revelations increased the salience of Internet privacy issues in European public debate.

The second paper provides new empirical insights into how ideas and institutions interact to condition which policy proposals are considered possible and desirable by policy-makers. The overarching policy paradigms that dominated American politics since the 1970s is what explains why America does not have a comprehensive privacy regime like the rest of the world. Whereas previous research has overemphasized the importance of the American 'Liberal Traditions' to explain America's privacy regime, I argue that to rely solely on this line of analysis is over-simplified and in the end, wrong.

Finally, the third paper explains how the design and implementation of the American and European privacy frameworks explain why they did not achieve their expected goals. Policy-makers might enact legislation that creates governance structures without being willing to either address some important issues for a certain policy area (in the case of data protection, the role of intelligence agencies) and without giving sufficient resources to the implementing agencies. This might create formal governance institutions

that upon closer examination do not provide with the expected level of steering of a certain field.

Theoretical contributions

In addition to the empirical contributions, this thesis also makes a number of theoretical contributions to the study of Internet privacy. The first paper argues that using historical institutionalism and incorporating power, political salience and institutions to our analyses we can understand the effects of policy shocks in ways that culturalist readings do not allow for. The paper argues that the fact that Europeans were outraged by the Snowden revelations and that many policy-makers changed their position regarding the GDPR when they realized that their constituencies deeply cared about the issue reveals that under some scenarios European's privacy culture has political effects. But by failing to account for political processes and variation in time of the position of political actors, cultural theories tend to fall in a static confirmation bias built upon the narrative fallacy of only accounting for positive outcomes.

The second paper shares the skepticism with cultural explanations of the first article and also contributes to understanding why sometimes policy proposals fail. Analyzing why America does not have a comprehensive privacy regime through an institutionalist reading that considers ideas and institutions as interacting variables, it is shown that the further a policy proposal depart from what is considered to be possible and desirable from the dominant policy paradigm in which it operates, the less likely its passage will be. Policies, in sum, cannot be understood outside the overarching policy paradigm in which they operate.

Reading the evolution of policies in a vacuum prohibits understanding the nature of any given policy debate. As Steinmo points out, policy makers thinking "is fundamentally framed within the economic/intellectual climate in which they work" (Steinmo, 2003, p. 227). A political readings that pay attention to the evolution of policies paradigms through ideas, interest, and institutions, offers a more nuanced and complex interpretation of history.

The third article showed how the study of policy designs and implementation efforts is fundamental for understanding governance. Only by studying the actual steering capacity of identified governance schemes we can conclude that, effectively, we are correctly identifying the actors exercising governance. In the case of data protection, the third article shows that more attention should be given to understanding *whom* and *how* is filling the governance gaps left by the European and American privacy policies. By better understanding the limits of state driven governance we can start understanding Internet governance beyond the state (Eeten & Mueller, 2013) and building a third wave of global governance research that is more capable of identifying effective governance structures for the provision of policy goals (Coen & Pegram, 2015).

Blueprints for future research

The findings outlined in each paper provide blueprints for future research. First, it is necessary to continue exploring the ways in which Silicon Valley corporations exercise their political power. Silicon Valley corporations are extremely powerful political actors and potentially capable of winning many political battles, especially those that happen out of the public spotlight. It is important to remember that these corporations have announced in recent years their willingness to influence a broad range of policies, not only the ones that we can automatically associate them to. For example, Silicon Valley companies are lobbying the US Congress to pass immigration reform (Rushe, 2013). Are they succeeding? What else are they achieving? How?

Future research should also keep rethinking why America is an outlier regarding privacy protection and what are the consequences of this phenomenon. In this dissertation I showed the limitations of the prevalent culturalist explanation and propose an alternative. I show that ideas and institutions have to be considered as necessary integral overlapping and fractionating elements of political explanations, that separately cannot explain the lack of a comprehensive privacy regime in the United States (Lieberman, 2002, p. 709). What is the nature of the political conflict over privacy rules in the United States? Cultural explanations are clearly insufficient to explain why America is an outlier in privacy protection and consequently more attention should be given to particular privacy debates in the United States that are now only told using a culturalist narrative.

Finally, this dissertation has invited to expand the research on the implementation and consequences of the American and the European privacy regimes. The third paper argues that since American and European legislators are unwilling to control intelligence agencies and provide with resources to implementing agencies the privacy frameworks they create are flawed. The flaws of the American and European privacy regimes creates a governance gap that exists between what the governance effects that it is assumed this regimes provide and what their actual steering capacity. Who and how is filling this governance gap? How does that affect the institutional regimes? If state-centric institutions are not providing the expected governance over the Internet who is providing the effective governance? Are we correctly identified the sources of Internet governance and the actors and process that provide it? The findings of article 3 invite to revise the answers we think we have for all those questions.

So what is next for Internet privacy?

The EU is entering the post-Snowden era reaffirming its commitment to the defense of privacy as a fundamental right. The EU will adopt new privacy rules, but much like with the adoption of the old-ones in 1995, European policy-makers have conveniently forgotten to deal with intelligence agencies and to take decisive action regarding the identified enforcement and compliance problems with the current framework. Understandably, this is the reality of contemporary European politics, only capable of offering than 2nd or 3rd best compromises. Some, especially in Brussels, will argue that European integration history is made of such kind of compromises. Nothing denies the truth of such statement. One should be able to question, however, the effects and consequences of this patchwork practices. In other words, while all politics are partly symbolic, we should be able to start questioning the consequences of symbolism in privacy protection policies.

In the US it seems highly unlikely that the outgoing Obama administration is going to reform America's privacy regime and curb state-surveillance. After the experiences of 9-11 President Obama seems convinced that his goals in the domestic politics' front are only feasible if Americans feel safe at home. In other words, Obama seems convinced that Americans will only talk about healthcare and the economy if they are not worried about national security. Obama's defense of the NSA programs evidence that meaningful reform

of surveillance is not a priority (Gorman, 2013). This is problematic for the whole world, for while European intelligence agencies also spy on telecommunications, the role of America as birthplace of the Internet, home of Silicon Valley, and global intelligence and surveillance superpower makes its approaches to privacy and surveillance important for every person in the planet. If America does not curb state-surveillance, the reforms that other jurisdictions might enact matter less.

As America walks towards its next presidential election everything might change. For the first time in decades populists can win the nominations for Republican and Democratic presidential candidates and disturb the post-1970s status quo. The consequences of such change, if it happens, are unpredictable. The only predictable thing is that populist change will mean two very different things if it comes from the left or the right, and that the understanding of privacy and surveillance will change if a populist makes it to the White House.

American and European societies need to seriously discuss how to protect the privacy of their citizens and at what costs. Perhaps presented to the trade-offs of regulating intelligence agencies, people will prefer to leave them unsupervised. Maybe, people will prefer to have free email and social networks to having more control over their personal information. Modern societies can only know the answers to those trade-offs by having a long-due public debate about privacy, surveillance and the Internet. Hopefully that debate will come soon.

Bibliography and references

Abbate, J. (2000). *Inventing the Internet*. The MIT Press.

Accis. (2012, April). Proposal for amendments to the proposed review of the EU's Data Protection Legal Framework.

Adriance, S. (2015). Who Makes the Rules?: American Data Protection Regulation and the FTC. *American Data Protection Regulation and the FTC (April 15, 2015)*.

A Framework for Global Electronic Commerce. (1997). White House.

Aid, M. M., & Wiebes, C. (2013). *Secrets of Signals Intelligence During the Cold War: From Cold War to Globalization*. Routledge.

Albrecht, J.-P. (2013, June 11). U.S. surveillance leaks and the EU data protection reform [Blog]. Retrieved from https://www.janalbrecht.eu/themen/datenschutz-und-netzpolitik/us-surveillance-leaks-and-the-eu-data-protection-reform.html

Amazon. (2013). Proposed amendments to MEP Gallo's opinion on data protetion. Amazon.

AmCham EU. (2012a). AmCham EU Proposed Amendments on the General Data Protection Regulation.

AmCham EU. (2012b, July 11). AmCham EU position on the General Data Protection Regulation. AmCham EU. Retrieved from https://dataskydd.net/sites/default/files/wp-content/uploads/2013/01/AmCham-EU_Position-Paper-on-Data-Protection-20120711.pdf

AmCham Romania. (2012). AmCham Romania Position Paper on the New EU Data Protection Regulation.

Arthur, C. (2014, April 8). EU court of justice overturns law that would enable "snoopers" charter'. *The Guardian*. London. Retrieved from http://www.theguardian.com/technology/2014/apr/08/eu-court-overturns-law-snoopers-charter-data-phones-isps

Astrada, M. L. (2010). *American Power After 9/11*. Palgrave Macmillan.

Atkinson, M. L., Lovett, J., & Baumgartner, F. R. (2014). Measuring the Media Agenda. *Political Communication*, *31*(2), 355–380. http://doi.org/10.1080/10584609.2013.828139

Bach, D., & Newman, A. L. (2007). The European regulatory state and global public policy: micro-institutions, macro-influence. *Journal of European Public Policy*,

14(6), 827–846. http://doi.org/10.1080/13501760701497659

Baker, J. (2013, May 20). Google, Microsoft and Yahoo are secret backers behind European Privacy Association. *Computerworld*. Retrieved from http://www.computerworld.com/article/2497928/it-management/google--microsoft-and-yahoo-are-secret-backers-behind-european-privacy-association.html

Baker, S. (2013, December 19). Report on the N.S.A.: A Battle That Snowden Is Not Winning - Room for Debate. *The New York Times*. New York. Retrieved from http://wayback.archive.org/web/20131222000429/http://www.nytimes.com/roomfordebate/2013/12/19/has-snowden-been-vindicated/report-on-the-nsa-a-battle-that-snowden-is-not-winning

Balboni, P. (2013, June). Highlights: Paolo Balboni -. Retrieved from http://www.paolobalboni.eu/wp-content/uploads/2013/06/highlights_paolo_balboni.pdf

Balboni, P., Cooper, D., Imperiali, R., & Macenaite, M. (2013). Legitimate interest of the data controller New data protection paradigm: legitimacy grounded on appropriate protection. *International Data Privacy Law*, ipt019. http://doi.org/10.1093/idpl/ipt019

Balboni, P., & Macenaite, M. (2013). Privacy by design and anonymisation techniques in action: Case study of Ma3tch technology. *Computer Law & Security Review*, *29*(4), 330–340. http://doi.org/10.1016/j.clsr.2013.05.005

Ball, J. (2013, June 8). NSA's Prism surveillance program: how it works and what it can do. *The Guardian*. Retrieved from http://www.guardian.co.uk/world/2013/jun/08/nsa-prism-server-collection-facebook-google

Ball, J., Borger, J., & Greenwald, G. (2013, September 6). Revealed: how US and UK spy agencies defeat internet privacy and security. *The Guardian*. Retrieved from http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security

Barabas, J., & Jerit, J. (2009). Estimating the Causal Effects of Media Coverage on Policy-Specific Knowledge. *American Journal of Political Science*, *53*(1), 73–89. http://doi.org/10.1111/j.1540-5907.2008.00358.x

Barlow, J. P. (1996, April 8). A declaration of independence of cyberspace. Retrieved from https://projects.eff.org/~barlow/Declaration-Final.html

Barrett, S., & Fudge, C. (1981). *Policy and Action: Essays on the Implementation of Public Policy*. Methuen.

Barros, P., Clougherty, J., & Seldeslachts, J. (2012, July 18). Europeanization of EU member-state competition policy: The commission's leadership role. Katholieke Universiteit Leuven. Retrieved from https://lirias.kuleuven.be/bitstream/123456789/358671/1/MSI_1218.pdf%20).

Baumgartner, F. R., Boef, S. L. D., & Boydstun, A. E. (2008). *The Decline of the Death Penalty and the Discovery of Innocence*. Cambridge University Press.

Baumgartner, F. R., & Jones, B. D. (2010). *Agendas and Instability in American Politics, Second Edition*. University of Chicago Press.

Baumgartner, F. R., & Jones, B. D. (2015). *The Politics of Information: Problem Definition and the Course of Public Policy in America*. University of Chicago Press.

Baumgartner, F. R., & Leech, B. L. (2001). Interest Niches and Policy Bandwagons: Patterns of Interest Group Involvement in National Politics. *The Journal of Politics*, *63*(04), 1191–1213. http://doi.org/10.1111/0022-3816.00106

BBC. (2012, December 4). Student group to take Facebook to task in Irish court. *BBC News*. Retrieved from http://www.bbc.com/news/technology-20592799

Beignier, B. (1992). *Le Droit de la personnalité*. Presses Universitaires de France - PUF.

Bennett, B. (2014, July 9). NSA tracked email accounts of leading Muslim Americans, report says. *Los Angeles Times*. Retrieved from http://www.latimes.com/nation/la-na-nsa-surveillance-muslims-20140709-story.html#page=1

Bennett, C. J. (1992). *Regulating privacy: data protection and public policy inEurope and the United States*. Ithaca: Cornell University Press.

Bennett, C. J. (2008). *The Privacy Advocates: Resisting the Spread of Surveillance*. MIT Press.

Bennett, C. J. (2011). In Defense of Privacy: The Concept and the Regime. *Surveillance & Society*, *8*(4), 485–496.

Bennett, C. J., Haggerty, K. D., Lyon, D., & Steeves, V. (2014). *Transparent Lives: Surveillance in Canada*. Athabasca University Press.

Bennett, C. J., & Raab, C. D. (2006). *The Governance of Privacy: Policy Instruments in Global Perspective*. MIT Press.

Bergan, D. E. (2009). Does Grassroots Lobbying Work? A Field Experiment Measuring

the Effects of an e-Mail Lobbying Campaign on Legislative Behavior. *American Politics Research, 37*(2), 327–352. http://doi.org/10.1177/1532673X08326967

Bergen, P., Sterman, D., Schneider, E., & Cahall, B. (2014, January). Do NSA's bulk surveillance programs stop terrorists? New America Foundation. Retrieved from http://www.newamerica.net/sites/newamerica.net/files/policydocs/Bergen_NAF_NSA%20Surveillance_1_0_0.pdf

Berman, S. (2013). Ideational Theorizing in the Social Sciences since "Policy Paradigms, Social Learning, and the State." *Governance, 26*(2), 217–237. http://doi.org/10.1111/gove.12008

Beyers, J. (2004). Voice and Access Political Practices of European Interest Associations. *European Union Politics, 5*(2), 211–240. http://doi.org/10.1177/1465116504042442

Bignami, F. (2007). Privacy and law enforcement in the european union: the data retention directive. *Chicago Journal of International Law, Spring*.

Bigo, D., Carrera, S., Hernanz, N., Jeandesboz, J., Parkin, J., Ragazzi, F. R., & Scherrer, A. (2013). Mass Surveillance of Personal Data by EU Member States and its Compatibility with EU Law. *Liberty and Security in Europe Papers*, (61).

Blau, P. M. (1955). *The dynamics of bureaucracy; a study of interpersonal relations in two government agencies.* [Chicago: University of Chicago Press.

Blink, B. (2014, September). Interview with Ben Blink.

Block, F. (1987). *Revising State Theory Essays in Politics and Postindustrialism.* Philadelphia: Temple University Press. Retrieved from http://public.eblib.com/choice/publicfullrecord.aspx?p=534247

Blühdorn, I. (2007). Sustaining the unsustainable: Symbolic politics and the politics of simulation. *Environmental Politics, 16*(2), 251–275. http://doi.org/10.1080/09644010701211759

Blyth, M. (2002). *Great Transformations: Economic Ideas and Institutional Change in the Twentieth Century*. Cambridge: Cambridge University Press. Retrieved from http://ebooks.cambridge.org/ref/id/CBO9781139087230

Blyth, M. (2011). The Transformation of the Swedish Model: Economic Ideas, Distributional Conflict, and Institutional Change. *World Politics, 54*(01), 1–26. http://doi.org/10.1353/wp.2001.0020

Bochel, H., Defty, A., & Kirkpatrick, J. (2014). *Watching the Watchers: Parliament and*

the Intelligence Services. Palgrave Macmillan.

Boghosian, H. (2013). *Spying on Democracy: Government Surveillance, Corporate Power and Public Resistance*. City Lights Publishers.

Borger, J. (2013, November 1). GCHQ and European spy agencies worked together on mass surveillance,. *The Guardian*. London. Retrieved from http://www.theguardian.com/uk-news/2013/nov/01/gchq-europe-spy-agencies-mass-surveillance-snowden

Borges, J. L. (1948). *Los Anales de Buenos Aires.* Buenos Aires: Los Anales de Buenos Aires.

Born, D. H., & Caparini, M. M. (2013). *Democratic Control of Intelligence Services: Containing Rogue Elephants*. Ashgate Publishing, Ltd.

Born, H., Johnson, L. K., & Leigh, I. (2005). *Who's watching the spies?: establishing intelligence service accountability*. Potomac Books.

Bowden, C. (2013). The US surveillance programmes and their impact on EU citizens' fundamental rights. EP.

Bowden, C. (2014, March 12). Safe Harbour. Oral Evidence and Written Submissions. House of Lords.

Bowen, E. R. (1982). The Pressman-Wildavsky Paradox: Four Addenda or Why Models Based on Probability Theory Can Predict Implementation Success and Suggest Useful Tactical Advice for Implementers. *Journal of Public Policy*, *2*(1), 1–21.

Boydstun, A. E. (2013). *Making the News: Politics, the Media, and Agenda Setting*. University of Chicago Press.

Brandeis, L. D. (2009). *Other People's Money: And How the Bankers Use It*. Martino Publishing.

Broder, J. M. (1997, June 30). Ira Magaziner Argues for Minimal Internet Regulation. *The New York Times*. Retrieved from http://www.nytimes.com/1997/06/30/business/ira-magaziner-argues-for-minimal-internet-regulation.html

Bruneau, T. C., & Dombroski, K. R. (2014). Reforming Intelligence: The Challenge of Control in New Democracies.

Burnett, T., & Games, A. (2007). *Who Really Runs the World?: The War Between Globalization and Democracy*. Red Wheel Weiser.

Bursens, P. (2002). Why Denmark and Belgium have different implementation records: on transposition laggards and leaders in the EU. *Scandinavian Political Studies, 25*(2), 173–195.

BusinessEurope. (2012, October 17). Position Paper - Commission proposal on a General Data Protection Regulation.

Cairncross, F. (2001). *The Death of Distance: How the Communications Revolution is Changing Our Lives*. Harvard Business Press.

Cannon, J. (2013). *Gerald R. Ford: An Honorable Life*. University of Michigan Press.

Carpenter, D., & Moss, D. A. (2013). *Preventing Regulatory Capture: Special Interest Influence and How to Limit it*. Cambridge University Press.

Carter, J. (1980). *Public Papers of the Presidents of the United States: Jimmy Carter, 1979*. Best Books on.

Cate, F. H. (1998). *The Internet and the First Amendment: Schools and Sexually Explicit Expression*. Phi Delta Kappa International.

CBC News. (2016, January 28). Spy agency stops sharing some data with international partners. Retrieved January 28, 2016, from http://www.cbc.ca/news/politics/spy-canada-electronic-metadata-1.3423565

Checkel, J. T. (2005). It's the Process Stupid! Process Tracing in the Study of European.

CIA. (2010). *The Family Jewels: Declassified Documents Released by the CIA Under the Freedom of Information Act, June 2007*. Nimble Books LLC.

Clinton, B. (1993, March 3). Remarks Announcing the Initiative To Streamline Government. GPO.

Clinton, B. (1998). *Public Papers of the Presidents of the United States: William J. Clinton, 1997*. Best Books on.

Clinton, B. (2005). *My Life*. Vintage Books.

Coen, D., & Pegram, T. (2015). Wanted: A Third Generation of Global Governance Research. *Governance*, *28*(4), 417–420. http://doi.org/10.1111/gove.12164

Cohn, C. (2010). Lawless Surveillance, Warrantless Rationales. *Journal on Telecommunications and High Technology Law*, *8*, 351.

Collier, D. (2011). Understanding Process Tracing. *PS: Political Science & Politics, 44*(04), 823–830. http://doi.org/10.1017/S1049096511001429

Collins, T. A., & Cooper, C. A. (2012). Case Salience and Media Coverage of Supreme

Court Decisions Toward a New Measure. *Political Research Quarterly*, *65*(2), 396–407. http://doi.org/10.1177/1065912911398047

Connolly, C. (2008). *The US Safe Harbor - Fact or Fiction?* Galexia. Retrieved from http://www.galexia.com/public/research/assets/safe_harbor_fact_or_fiction_2008/safe_harbor_fact_or_fiction.pdf

Connolly, C. (2013, October 7). EU/US Safe Harbor – Effectiveness of the Framework in relation to National Security Surveillance. Galexia.

CQ. (1974). Privacy: Congress Expected to Vote Controls. *Congreesional Quarterly*, p. 2613.

Culpepper, P. (2011). *Quiet politics and business power : corporate control in Europe and Japan*. New York: Cambridge University Press. Retrieved from http://encore.eui.eu/iii/encore/record/C__Rb1682556__Squiet+politics__Orightresult__X5?lang=eng&suite=def

Culpepper, P. D., & Reinke, R. (2014). Structural Power and Bank Bailouts in the United Kingdom and the United States. *Politics & Society*, 0032329214547342. http://doi.org/10.1177/0032329214547342

Dahl, R. A., & Lindblom, C. (1976). *Politics, Economics, and Welfare*. Transaction Publishers.

Dallek, R. (1984). *Ronald Reagan: The Politics of Symbolism : with a New Preface*. Harvard University Press.

Dembosky, A. (2013, January 24). Facebook spending on lobbying soars. *Financial Times*. London. Retrieved from http://www.ft.com/intl/cms/s/0/cfaf0c78-65b2-11e2-a17b-00144feab49a.html#axzz33aMjmgfM

De Mesquita, E. B., & Stephenson, M. C. (2007). Regulatory Quality Under Imperfect Oversight. *American Political Science Review*, *null*(03), 605–620. http://doi.org/10.1017/S0003055407070359

De Miguel Asensio, P. A. (2015). Aspectos internacionales de la protección de datos: las sentencias Schrems y Weltimmo del Tribunal de Justicia. *La Ley Unión Europea*, (31). Retrieved from http://eprints.ucm.es/34706/

Demmke, C., & Deakin, S. F. (2001). *Towards effective environmental regulation: innovative approaches in implementing and enforcing European environmental law and policy*. Harvard Law School Cambridge, MA.

DeNardis, L. (2009). *Protocol Politics: The Globalization of Internet Governance*. Cambridge, Mass. ; London: MIT Press.

Department of Commerce. (2010a). Commercial data privacy and innovation in the Internet economy: A dynamic policy framework. Retrieved from http://www.commerce.gov/sites/default/files/documents/2010/december/iptf-privacy-green-paper.pdf

Department of Commerce. (2010b, December). Commercial Data Privacy and Innovation in the Internet Economy: a Dynamic Policy Framework. Department of Commerce. Retrieved from http://www.commerce.gov/sites/default/files/documents/2010/december/iptf-privacy-green-paper.pdf

Der Spiegel. (2013, July 8). Edward Snowden Interview: The NSA and Its Willing Helpers. *Spiegel Online*. Retrieved from http://www.spiegel.de/international/world/interview-with-whistleblower-edward-snowden-on-global-spying-a-910006.html

Derthick, M., & Quirk, P. J. (2001). *The Politics of Deregulation*. Brookings Institution Press.

Digital Europe. (2012, March 12). Comments on Proposed European Commission's Regulation on Data Protection. Digital AEurope. Retrieved from https://wiki.laquadrature.net/images/1/1f/DIGITALEUROPE-priorities-of-Data-Protection-Regulation_March-2012.pdf

DigitalEurope. (2012a, July). Interconnecting the digital world, MEP Axel Voss talks about data protection. Retrieved October 23, 2015, from http://www.digitaleurope.org/DigitalHeadlines/Story.aspx?newsID=75

DigitalEurope. (2012b, November). DIGITALEUROPE data protection trip to Strasbourg. Retrieved October 23, 2015, from http://www.digitaleurope.org/DigitalHeadlines/Story.aspx?newsID=133

Dijkstra, G., Fenger, M., Bekkers, V., & Edwards, M. A. (2013). *Governance and the Democratic Deficit: Assessing the Democratic Legitimacy of Governance Practices*. Ashgate Publishing, Ltd.

Dimitrakopoulos, D. G. (2001). The transposition of EU law:"post-decisional politics" and institutional autonomy. *European Law Journal, 7*(4), 442–458.

Doctorow, C. (2013, June 5). Data protection in the EU: the certainty of uncertainty. *The Guardian*. Retrieved from http://www.theguardian.com/technology/blog/2013/jun/05/data-protection-eu-anonymous

Drezner, D. W. (2004). The global governance of the Internet: bringing the state back in. *Political Science Quarterly*, *119*(3), 477–498.

Drozdiak, N., & Schechner, S. (2015, October 6). EU Court Says Data-Transfer Pact With U.S. Violates Privacy. *Wall Street Journal*. Retrieved from http://www.wsj.com/articles/eu-court-strikes-down-trans-atlantic-safe-harbor-data-transfer-pact-1444121361

Duffy, H. (2015). *The "War on Terror" and the Framework of International Law*. Cambridge University Press.

Duhigg, C. (2012, February 16). How Companies Learn Your Secrets. *The New York Times*. Retrieved from http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html

Dunn, B. N. (2015). *What Do MEPs Do ?: a snapshot of work in the 2009-2014 European Parliament*. Allendale Publishing.

DW. (2014, 10). German citizens' communication data reportedly passed to NSA. *DW.COM*. Berlin. Retrieved from http://www.dw.com/en/german-citizens-communication-data-reportedly-passed-to-nsa/a-17973165

eBay. (2012, November). eBay Inc. position - Legal Affairs Committee draft opinion on the General Data Protection Regulation.

EC. (2013a, June 6). Vice-President Reding's intervention during Justice Council Press Conference. Retrieved from http://europa.eu/rapid/press-release_SPEECH-13-514_en.htm

EC. (2013b, July 19). European Commission - PRESS RELEASES - Press release - Informal Justice Council in Vilnius. European Commission. Retrieved from http://europa.eu/rapid/press-release_MEMO-13-710_en.htm

EC. (2015, December 15). Press release - Agreement on Commission's EU data protection reform will boost Digital Single Market. European Commission. Retrieved from http://europa.eu/rapid/press-release_IP-15-6321_en.htm

ECJ. (2014, May 13). Press Release No 70/14 Judgment in Case C-131/12 Google Spain

SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González. ECJ.

ECJ. (2015, October 6). Press Release: The Court of Justice declares that the Commission's US Safe Harbour Decision is invalid. ECJ.

EDPS. (2012a, March 7). Opinion of the European Data Protection Supervisor. EDPS. Retrieved from https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-03-07_EDPS_Reform_package_EN.pdf

EDPS. (2012b, March 7). Opinion of the European Data Protection Supervisor on the data protection reform package. EDPS.

EDPS. (2013a, June 10). Statement: EDPS following the NSA story. EDPS.

EDPS. (2013b, October 22). EDPS/2013/09 - Press Release - An important and welcome step towards stronger and more effective data protection in Europe. EDPS.

EDPS. (2015, July 27). Opinion 3/2015 Europe's big opportunity - EDPS recommendations on the EU's options for data protection reform. EDPS.

EDRi. (2012, February 1). ENDitorial: EDRi's initial comments on the Data Protection Regulation. Retrieved from https://edri.org/edrigramnumber10-2edri-comments-on-data-retention/

Edwards, G. C. I., & Wood, B. D. (1999). Who Influences Whom? The President, Congress, and the Media. *American Political Science Review*, *93*(02), 327–344. http://doi.org/10.2307/2585399

Eeten, M. J. van, & Mueller, M. (2013). Where is the governance in Internet governance? *New Media & Society*, *15*(5), 720–736. http://doi.org/10.1177/1461444812462850

EFF. (2014). PATRIOT Act. Retrieved December 7, 2014, from https://www.eff.org/issues/patriot-act

EIF. (2013, March 19). EIF Dinner Debate. Retrieved October 22, 2015, from https://www.eifonline.org/component/events/event/125-data-protection.html

EIF. (2014). European Internet Forum - ABOUT US. Retrieved October 22, 2015, from https://www.eifonline.org/about-us.html

Eisner, M. A. (2000). *Regulatory Politics in Transition*. JHU Press.

Eisner, M. A. (2013). *The American Political Economy: Institutional Evolution of Market and State*. Routledge.

Emmerson, B. (2014, September 23). Promotion and protection of Human Rights and Fundamental freedoms while countering terrorism. United Nations Publications. Retrieved from https://theintercept.com/document/2014/10/15/un-report-human-rights-terrorism/

Enzensberger, H. M. (2013, October 26). Le terrorisme publicitaire. *Le Monde*. Paris. Retrieved from http://www.lemonde.fr/idees/article/2013/10/26/le-terrorisme-publicitaire_3503506_3232.html

EP. (2000, December 18). Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data. European Parliament.

EP. (2014). *Video Minutes Plenary session from 10/03/2014 to 13/03/2014.* European Parliament.

EPP Group EP. (2013, June 19). Press release: PRISM: we want introduction of "Anti net tapping clause." EPP Group EP. Retrieved from http://www.eppgroup.eu/press-release/PRISM%3A-we-want-introduction-of-'Anti-net-tapping-clause'

Epstein, D., & O'Halloran, S. (1999). *Delegating Powers: A Transaction Cost Politics Approach to Policy Making Under Separate Powers*. Cambridge University Press.

Epstein, L., & Segal, J. A. (2000). Measuring Issue Salience. *American Journal of Political Science*, *44*(1), 66–83. http://doi.org/10.2307/2669293

Esping-Andersen, G. (2013). *The Three Worlds of Welfare Capitalism*. John Wiley & Sons.

EU Commission. (2012, January 25). Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses (Press release). Retrieved from http://europa.eu/rapid/pressReleasesAction.do?reference=IP/12/46

Eudes, Y. (2013, June 2). Très chères données personnelles. *Le Monde.fr*. Retrieved from http://www.lemonde.fr/a-la-une/article/2013/06/02/tres-cheres-donnees-personnelles_3422477_3208.html

Eurobarometer, S. (2011). Special Eurobarometer 359 - Attitudes on Data Protection and Electronic Identity in the European Union.

Eurocommerce. (2012a). 10 Recommendations for A Data Protection Regulation.

Eurocommerce.

Eurocommerce. (2012b, September 7). Draft EuroCommerce position on the European Commission proposal for a General Data Protection Regulation, COM(2012) 11. Eurocommerce.

European Council. (2012, December 3). 16525/1/12 - Rev 1 - Data protection package - Report on progress achieved under the Cyprus Presidency.

European Council. (2013, February 22). 6607/13 (Note). Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). European Council.

European Parliament. (2011, July 6). (2011/2025(INI) - European Parliament resolution of 6 July 2011 on a comprehensive approach on personal data protection in the European Union. European Parliament.

European Parliament. (2013a, January 28). Opinion of IMCO to LIBE on the General Data Protection Regulation.

European Parliament. (2013b, February 26). Opinion of ITRE to LIBE on the General Data Protection Regulation.

European Parliament. (2013c, March 4). Opinion of EMPL to LIBE on the General Data Protection Regulation.

European Parliament. (2013d, March 25). Opinion of JURI to LIBE on the General Data Protection Regulation.

EU Transparency Register. (2015, August 27). Kreab - Transparency Register. Retrieved October 24, 2015, from http://ec.europa.eu/transparencyregister/public/consultation/displaylobbyist.do?id=1078390517-54&locale=en#en

Facebook. (2012a, March 30). Facebook's view on EU Data Protection Regulation. Facebook.

Facebook. (2012b, March 30). Facebook's views on the EU Data Protection Regulation. Facebook.

Facebook. (2013). Facebook recommendations on the IMCO draft opinion on the European Commission's proposal for a General Data Protection Regulation.

Fairfield, T. (2010). Business Power and Tax Reform: Taxing Income and Profits in

Chile and Argentina. *Latin American Politics and Society*, *52*(2), 37–71. http://doi.org/10.1111/j.1548-2456.2010.00081.x

Falkner, G. (2005). *Complying with Europe: EU harmonisation and soft law in the member states*. Cambridge University Press.

Falkner, G., Hartlapp, M., Leiber, S., & Treib, O. (2004). Non-Compliance with EU directives in the Member States: Opposition through the Backdoor? *West European Politics*, *27*(3), 452–473.

Falkner, G., Hartlapp, M., & Treib, O. (2007). Worlds of compliance: Why leading approaches to European Union implementation are only "sometimes-true theories." *European Journal of Political Research*, *46*(3), 395–416.

Falque-Pierrotin, I. (2014, April 10). Letter Ares(2014)1139376.

Farrell, H. (2002a). Negotiating Privacy across Arenas: The EU-US. *Common Goods: Reinventing European and International Governance*, 105.

Farrell, H. (2002b). Negotiating Privacy across Arenas: The EU-US. *Common Goods: Reinventing European and International Governance*, 105.

Farrell, H., & Newman, A. (2015). Structuring power: business and authority beyond the nation state. *Business and Politics*, *17*(3), 527–552.

Federal Information Policies. (1990). Library of Congress.

Flaherty, D. H. (1979). *Privacy and government data banks: an international perspective*. Mansell.

Flaherty, D. H. (1992). *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States*. University of North Carolina Press.

Fleisher, L. (2015, May 1). Ireland Beefs Up Data Privacy Office. *Wall Street Journal*. Retrieved from http://www.wsj.com/articles/irelands-data-protection-agency-to-boost-staff-and-double-budget-1430488864

Fleming, J. (2013, October 25). Data protection rules delayed at EU summit talks. *EurActiv*. Brussels. Retrieved from http://www.euractiv.com/specialreport-digital-single-mar/france-germany-form-anti-spy-pac-news-531306

Fontanella-Khan, J. (2013, June 26). Brussels: Astroturfing takes root. *Financial Times*. Retrieved from http://www.ft.com/intl/cms/s/0/74271926-dd9f-11e2-a756-00144feab7de.html#axzz32k3XTloT

FoP. (2013, January). White Paper - The Definition of Persona Data: Seeing the Complete Spectrum.

FoP. (2014, January 1). Privacy Papers for Policy Makers 2013. Future of Privacy Forum. Retrieved from http://www.futureofprivacy.org/privacy-papers-2013/

FoP. (2015). Supporters. Retrieved from http://www.futureofprivacy.org/about/supporters/

Ford, G. (1975). *Public Papers of the Presidents of the United States: Gerald R. Ford, 1974*. Best Books on.

Fosburgh, L. (1970, September 12). Nader Fears Computer Will Turn Us Into 'slaves. *New York Times*, p. 18. New York.

FRA. (2013). Access to data protection remedies in EU member States. Publications office of the European Union.

FRA. (2015). Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU. Publications office of the European Union.

Friedman, M. (2009). *Capitalism and Freedom: Fortieth Anniversary Edition*. University of Chicago Press.

Fromholz, J. M. (2000). European Union Data Privacy Directive, The. *Berkeley Technology Law Journal*, *15*, 461.

FTC. (2000). *Privacy online fair information practices in the electronic marketplace : a report to Congress*. FTC.

FTC. (2013, June 27). FTC Signs Memorandum of Understanding with Irish Privacy Enforcement Agency. FTC. Retrieved from https://www.ftc.gov/news-events/press-releases/2013/06/ftc-signs-memorandum-understanding-irish-privacy-enforcement

Fung, B. (2013, August 23). The NSA paid Silicon Valley millions to spy on taxpayers. *The Washington Post*. Retrieved from https://www.washingtonpost.com/news/the-switch/wp/2013/08/23/the-nsa-paid-google-and-facebook-millions-to-spy-on-taxpayers/

Future of Privacy Forum. (2013, December). The US-EU Safe Harbor - An analysis of the framework's effectiviness in protecting personal privacy. Future of Privacy Forum.

Gallagher, R. (2014, June 18). How Secret Partners Expand NSA's Surveillance Dragnet. *The Intercept*. Retrieved from https://firstlook.org/theintercept/2014/06/18/nsa-

surveillance-secret-cable-partners-revealed-rampart-a/

Garton Ash, T. (2013a, June 27). If Big Brother came back, he'd be a public-private partnership. *The Guardian*. London. Retrieved from http://www.theguardian.com/commentisfree/2013/jun/27/big-brother-public-private-partnership-nsa

Garton Ash, T. (2013b, July 1). El Gran Hermano con la ayuda de Google. *EL PAÍS*. Retrieved from http://elpais.com/elpais/2013/06/28/opinion/1372411847_928983.html

Gellman, B., & Poitras, L. (2013, June 7). U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program. *The Washington Post*. Retrieved from http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html

Gellman, R. M. (1993). Fragmented, Incomplete, and Discontinuous: The Failure of Federal Privacy Regulatory Proposals and Institutions. *Software Law Journal*, *6*, 199.

Glickman, L. B. (2009). *Buying Power: A History of Consumer Activism in America*. University of Chicago Press.

Goggin, M. L. (1990). *Implementation theory and practice: toward a third generation*. Scott, Foresman/Little, Brown Higher Education.

Goldsmith, J., & Wu, T. (2006). *Who Controls the Internet?: Illusions of a Borderless World*. Oxford University Press, USA.

Google. (2012, February). Preliminary Views on the Proposed Data Protection and Privacy Regulation in the European Union. Google.

Gore, A. (1993). Step 5: Eliminating Regulatory Overkill. Retrieved March 24, 2015, from http://www.ibiblio.org/npr/npr-1/npr-1-5.html

Gorman, P. N. A. S. (2013, June 8). Obama Defends Surveillance. *Wall Street Journal*. Retrieved from http://www.wsj.com/articles/SB10001424127887324299104578531742264893564

Gorman, S., & Valentino-DeVries, J. (2013, August 21). New Details Show Broader NSA Surveillance Reach. *Wall Street Journal*. Retrieved from http://www.wsj.com/articles/SB10001424127887324108204579022874091732470

Gormley, W. T., Jr. (1986). Regulatory Issue Networks in a Federal System. *Polity*, *18*(4), 595–620. http://doi.org/10.2307/3234884

Gouvernment.fr. (2015, June 30). Parliament adopts the intelligence bill [Official]. Retrieved from http://www.gouvernement.fr/en/parliament-adopts-the-intelligence-bill

Greenleaf, G. (2012). Global Data Privacy Laws: 89 Countries, and Accelerating. *SSRN eLibrary*. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2000034

Greenleaf, G. (2014). *Asian Data Privacy Laws: Trade and Human Rights Perspectives*. Oxford University Press.

Greenleaf, G. (2015). *Global Data Privacy Laws 2015: Data Privacy Authorities and Their Organisations* (SSRN Scholarly Paper No. ID 2641772). Rochester, NY: Social Science Research Network. Retrieved from http://papers.ssrn.com/abstract=2641772

Greenwald, G. (2013, August 4). Members of Congress denied access to basic information about NSA. *The Guardian*. Retrieved from http://www.theguardian.com/commentisfree/2013/aug/04/congress-nsa-denied-access

Greenwald, G. (2014). *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. Metropolitan Books.

Greenwald, G., & MacAskill, E. (2013, June 7). NSA Prism program taps in to user data of Apple, Google and others. *The Guardian*. Retrieved from http://www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data

Greenwald, G., MacAskill, E., & Poitras, L. (2013, June 11). Edward Snowden: the whistleblower behind the NSA surveillance revelations. *The Guardian*. Retrieved from http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance

Greenwood, J. (2003). *Interest representation in the European Union*. Houndmills, Basingstoke, Hampshire; New York: Palgrave Macmillan.

Greer, D. (2011). Safe Harbor—a framework that works. *International Data Privacy Law*, *1*(3), 143–148. http://doi.org/10.1093/idpl/ipr010

Guarascio, F. (2012, February 21). US lobbying waters down EU data protection reform.

EurActiv. Retrieved from http://www.euractiv.com/specialreport-data-protection/us-lobbying-waters-eu-data-prote-news-510991

Gude, H., Poitras, L., & Rosenbach, M. (2013, August 5). Mass Data: Transfers from Germany Aid US Surveillance. *Spiegel Online*. Retrieved from http://www.spiegel.de/international/world/german-intelligence-sends-massive-amounts-of-data-to-the-nsa-a-914821.html

Gunn, L. A. (1978). Why is implementation so difficult. *Management Services in Government*, *33*(4), 169–176.

Günter, O., Hornung, G., Rannenberg, K., Roßnagel, A., Spiekermann, S., & Waider, M. (2013, February 14). Datenschutz-Verordnung. *Die Zeit*. Hamburg. Retrieved from http://www.zeit.de/digital/datenschutz/2013-02/stellungnahme-datenschutz-professoren

Hacker, J. S., & Pierson, P. (2002). Business Power and Social Policy: Employers and the Formation of the American Welfare State. *Politics & Society*, *30*(2), 277–325. http://doi.org/10.1177/0032329202030002004

Hall, P. (2003). Aligning Ontology and Methodology in Comparative Politics. In J. Mahoney & D. Rueschemeyer (Eds.), *Comparative Historical Analysis in the Social Sciences* (pp. 373–404). Cambridge: Cambridge University Press. Retrieved from http://www.eui.eu/SeminarMaterial/SPS/2011-12-FirstTerm/Culpepper/Session-05-03-Nov-2011/AligningOntologyandMethodologyinComparativePolitics.pdf

Hall, P. A. (1993). Policy Paradigms, Social Learning, and the State: The Case of Economic Policymaking in Britain. *Comparative Politics*, *25*(3), 275–296. http://doi.org/10.2307/422246

Hall, P. A. (2006). Systematic process analysis: when and how to use it. *European Management Review*, *3*(1), 24–31.

Halperin, M. H., Clapp, P., & Kanter, A. (1974). *Bureaucratic politics and foreign policy*. Washington: The Brookings Institution.

Hanus, J. J., & Relyea, H. C. (1975). Policy Assessment of the Privacy Act of 1974, A. *American University Law Review*, *25*, 555.

Hargrove, E. C. (1975). *The missing link: the study of the implementation of social policy*. Urban Institute.

Harris Interactive. (1999, October). IBM Mult-National Consumer Privacy Survey. IBM.

Retrieved from ftp://www6.software.ibm.com/software/security/privacy_survey_oct991.pdf

Hartz, L. (1991). *The Liberal Tradition in America*. Houghton Mifflin Harcourt.

Hartzog, W., & Solove, D. J. (2014). The Scope and Potential of FTC Data Protection.

Harvey, D. (2005). *A Brief History of Neoliberalism*. Oxford University Press.

Hattam, V. C. (1992). Institutions and Political Change: Working-Class Formation in England and the United States, 1820-1896. *Politics & Society*, *20*(2), 133–166. http://doi.org/10.1177/0032329292020002002

Heath, N. (2013, January 10). EU privacy laws to spell an end to Facebook for free? *ZDNet*. Retrieved from http://www.zdnet.com/article/eu-privacy-laws-to-spell-an-end-to-facebook-for-free/

Hecking, C. (2013, December 2). EU-Ministerrat: Deutsche Beamte bremsen Europas Datenschutz aus. *Spiegel Online*. Retrieved from http://www.spiegel.de/artikel/a-936704.html

Hennigan, R. (2013, May 24). IAB Europe awards MEP Sean Kelly for standing up for data privacy rights. Retrieved October 24, 2015, from http://iabireland.ie/iab-europe-awards-mep-sean-kelly-for-standing-up-for-data-privacy-rights/

Hersh, S. (1974, December 22). Huge C.I.A. operation reported in U.S. against antiwar forces, other dissidents in nixon years. *The New York Times*, p. 26. New York.

Hetcher, S. A. (2001). *The FTC as Internet Privacy Norm Entrepreneur* (SSRN Scholarly Paper No. ID 253317). Rochester, NY: Social Science Research Network. Retrieved from http://papers.ssrn.com/abstract=253317

Heumann, S., & Scott, B. (2013, September). Law and Policy in Internet Surveillance Programs: United States, Great Britain and Germany. Stifting Neue Verantwortung and New America Foundation.

Hidalgo, D. (2014, April 10). Césped artificial: todo empezó en Texas | Mas Futbol | AS.com. *AS*. Madrid. Retrieved from http://futbol.as.com/futbol/2014/04/10/mas_futbol/1397144148_588041.html

Higgins, J. (2013, June 19). Data protection: One law should cover EU, governments and private sector. EurActiv. Retrieved from http://www.euractiv.com/infosociety/data-protection-law-cover-eu-gov-analysis-528711

Hillman, A. J., Keim, G. D., & Schuler, D. (2004). Corporate Political Activity: A

Review and Research Agenda. *Journal of Management*, *30*(6), 837–857. http://doi.org/10.1016/j.jm.2004.06.003

Hill, M., & Hupe, P. (2014). *Implementing Public Policy: An Introduction to the Study of Operational Governance*. SAGE.

Hix, S. (2013). *What's Wrong with the Europe Union and How to Fix It*. John Wiley & Sons.

Hix, S., & Marsh, M. (2007). Punishment or Protest? Understanding European Parliament Elections. *Journal of Politics*, *69*(2), 495–510. http://doi.org/10.1111/j.1468-2508.2007.00546.x

Hix, S., Noury, A., & Roland, G. (2006). Dimensions of Politics in the European Parliament. *American Journal of Political Science*, *50*(2), 494–520. http://doi.org/10.1111/j.1540-5907.2006.00198.x

Hjern, B., & Porter, D. O. (1981). Implementation Structures: A New Unit of Administrative Analysis. *Organization Studies*, *2*(3), 211–227.

Hogwood, B. W., & Gunn, L. A. (1984). *Policy Analysis for the Real World*. Oxford University Press.

Hondius, F. W. (1975). *Emerging data protection in Europe*. Amsterdam : New York: North-Holland Pub. Co. ; American Elsevier Pub. Co.

Hopkins, N., & Taylor, M. (2013, October 6). Cabinet was told nothing about GCHQ spying programmes, says Chris Huhne. *The Guardian*. Retrieved from http://www.theguardian.com/uk-news/2013/oct/06/cabinet-gchq-surveillance-spying-huhne

Horne, J. R. (2001). *A Social Laboratory for Modern France: The Musée Social and the Rise of the Welfare State*. Duke University Press.

Hrebenar, R. J., & Morgan, B. B. (2009). *Lobbying in America: A Reference Handbook*. ABC-CLIO.

Hudson, A. (2013, February 23). European Parliament Deputy President injured in car crash. *Reuters*. Berlin. Retrieved from http://www.reuters.com/article/2013/02/23/us-germany-alvaro-crash-idUSBRE91M0B620130223

Hughes, K. H. (2005). *Building the Next American Century: The Past and Future of American Economic Competitiveness*. Johns Hopkins University Press.

IAPP. (2012). Data Protection Authorities 2011 Global Survey. IAPP. Retrieved from https://www.privacyassociation.org/media/pdf/knowledge_center/DPA11_Survey_final.pdf

IIEA. (2015). *Helen Dixon - Privacy and Data Protection - 07 January 2015*. Retrieved from https://www.youtube.com/watch?time_continue=816&v=P3HdJduRatw

IPT. (2015, February). Liberty V GCHQ. Investigatory Powers Tribunal.

Irish Data Protection Commissioner. (1998, November). NInth Annual Report of the Data Protection Commissioner 1997.

Irish Data Protection Commissioner. (2013, May). Twenty-Fourth Annual Report of the Data Protection Commissioner 2012.

ISC. (2013, July 17). Statement on GCHQ's alleged interception of communications under the US PRISM Programme. Parliament of the United Kingdom - Intelligence and Security Committee. Retrieved from http://isc.independent.gov.uk/news-archive/17july2013

Jay, A. H. James Madison, John, & Pole, J. R. (2005). *The Federalist*. Hackett Publishing.

Johannès, J. F. et F. (2015, January 12). La tentation d'un « Patriot Act » à la française. *Le Monde.fr*. Retrieved from http://www.lemonde.fr/police-justice/article/2015/01/12/la-tentation-d-un-patriot-act-a-la-francaise_4554308_1653578.html

Johnson, L. K. (2015). *A Season of Inquiry: The Senate Intelligence Investigation*. University Press of Kentucky.

Johnson, T. J. (2013). *Agenda Setting in a 2.0 World: New Agendas in Communication*. Routledge.

Jones, B. D., & Baumgartner, F. R. (2005). *The Politics of Attention: How Government Prioritizes Problems*. University of Chicago Press.

Josefsson, E. (2013, April). Interview with Erik Josefsson, Senior Advisor of European Green Party.

Judge, D., & Earnshaw, D. (2008). *The European Parliament, Second Edition*. Palgrave Macmillan.

Kanter, J., & Sengupta, S. (2013, June 6). Europe Still Wrangling Over Online Privacy Rules. *The New York Times*. Retrieved from

http://www.nytimes.com/2013/06/07/technology/europe-still-wrangling-over-online-privacy-rules.html

Katz, J. E., & Tassone, A. R. (1990). A Report: Public Opinion Trends: Privacy and Information Technology. *The Public Opinion Quarterly*, *54*(1), 125–143.

Kaufman, B. I. (2009). *The Carter Years*. Infobase Publishing.

Kaufman, H. (1967). *The Forest Ranger: A Study in Administrative Behavior*. Resources for the Future.

Kellstedt, P. M. (2003). *The Mass Media and the Dynamics of American Racial Attitudes*. Cambridge University Press.

Kelly, K. (1995). *Out of Control: The New Biology of Machines, Social Systems and the Economic World*. Basic Books.

Kennard, W. (2013, April 2). Remarks by U.S. Ambassador to the EU, William E. Kennard, at Forum Europe's 3rd Annual European Data Protection and Privacy Conference. US Embassy to the EU. Retrieved from http://useu.usmission.gov/kennard_120412.html

Kibbe, J. (2009). *Congressional Oversight of Intelligence: Is the Solution Part of the Problem?* (SSRN Scholarly Paper No. ID 1451861). Rochester, NY: Social Science Research Network. Retrieved from http://papers.ssrn.com/abstract=1451861

Kilian, W. (2008). Germany. In J. B. Rule & G. W. Greenleaf (Eds.), *Global privacy protection: the first generation* (pp. 80 – 106). Cheltenham: Edward Elgar.

Kim, W., & Law, M. S. of. (2009). *A Study on how Regulatory Capture Caused the Subprime Mortgage Crisis and what to Do for Robust Consumer Protection*. Indiana University.

King, A. (1973). Ideas, Institutions and the Policies of Governments: a Comparative Analysis: Part III. *British Journal of Political Science*, *3*(04), 409–423. http://doi.org/10.1017/S000712340000795X

Kolko, G. (2008). *Triumph of Conservatism*. Free Press.

Kollman, K. (1998). *Outside Lobbying: Public Opinion and Interest Group Strategies*. Princeton University Press.

Kreab. (2009, November 16). Press Release: Former Member of the European Parliament Karin Riis-Jørgensen joins Kreab Gavin Anderson. Retrieved from http://pr.euractiv.com/pr/former-member-european-parliament-karin-riis-j-rgensen-

joins-kreab-gavin-anderson-89391

Kreitner, R. (2015). *Smoking Gun, The Nation on Watergate, 1952-2010*. The Nation Co. LP.

Kuner, C. (2012). *The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law* (SSRN Scholarly Paper No. ID 2162781). Rochester, NY: Social Science Research Network. Retrieved from http://papers.ssrn.com/abstract=2162781

Landes, D. (2013, January 21). Sweden enters fray in EU data privacy fight - The Local. *The Local*. Retrieved from http://www.thelocal.se/20130121/45734

Langenderfer, J., & Cook, D. L. (2004). Oh, what a tangled web we weave: The state of privacy protection in the information economy and recommendations for governance. *Journal of Business Research*, *57*(7), 734–747. http://doi.org/10.1016/S0148-2963(02)00359-4

Lardner, G. (1966, July 27). Data Center Hearing Warned on Privacy. *Washington Post*. Washington, D.C.

Lathrop, C. E. (2008). *The Literary Spy: The Ultimate Source for Quotations on Espionage & Intelligence*. Yale University Press.

Lefebvre, S. (2003). The Difficulties and Dilemmas of International Intelligence Cooperation. *International Journal of Intelligence and CounterIntelligence*, *16*(4), 527–542. http://doi.org/10.1080/716100467

Le Gendre, B. (1980, December 10). Le premier rapport de la commission "informatique et libertés." *Le Monde*, p. 11. Paris.

Lehmann, W. (2009). The European Parliament. In J. Richardson & D. Coen (Eds.), *Lobbying the European Union: Institutions, Actors, and Issues* (pp. 39–69). OUP Oxford.

Leigh, I. (2007a). The accountability of security and intelligence services. In L. K. Johnson, *Handbook of Intelligence Studies*. Routledge.

Leigh, I. (2007b). The UK's Intelligence and Security Committee. In H. Born & T. M. Wetzling (Eds.), *Democratic Control of Intelligence Agencies* (pp. 177–195).

Lelieveldt, H., & Princen, S. (2015). *The Politics of the European Union*. Cambridge University Press.

Lewis, A. E. (1972, June 18). 5 Held in Plot to Bug Democrats' Office Here. *The*

Washington Post. Retrieved from http://www.washingtonpost.com/wp-dyn/content/article/2002/05/31/AR2005111001227.html

Lewis, P., correspondent, W., & Oltermann, P. (2013, October 27). NSA denies discussing Merkel phone surveillance with Obama. *The Guardian*. Retrieved from http://www.theguardian.com/world/2013/oct/27/barack-obama-nsa-angela-merkel-germany

Lieberman, R. C. (2002). Ideas, institutions, and political order: Explaining political change. *American Political Science Review*, *96*(04), 697–712.

Lindblom, C. E. (1977). *Politics and Markets: The World's Political Economic Systems*. New York: Basic Books.

Lindblom, C. E. (1982). The Market As Prison. *The Journal of Politics*, *44*(02), 323–336. http://doi.org/10.2307/2130588

Lindsay, D. (2005a). An exploration of the conceptual basis of privacy and the implications for the future of Australian privacy law. *Melbourne University Law Review*, *29*(1), 131.

Lindsay, D. (2005b). An Exploration of the Conceptual Basis of Privacy and the Implications for the Future of Australian Privacy Law'(2005) 29. *Melbourne University Law Review*, *131*.

Lipset, S. M. (1971). *Agrarian Socialism: The Cooperative Commonwealth Federation in Saskatchewan : a Study in Political Sociology*. University of California Press.

Lipset, S. M. (1979). *The First New Nation: The United States in Historical and Comparative Perspective*. Transaction Publishers.

Lipset, S. M. (1996). *American Exceptionalism: A Double-edged Sword*. W.W. Norton.

Lipset, S. M. (1997). *American Exceptionalism: A Double-Edged Sword*. W. W. Norton & Company.

Lipsky, M. (1983). *Street-Level Bureaucracy: The Dilemmas of the Individual in Public Service: The Dilemmas of the Individual in Public Service*. Russell Sage Foundation.

Lischka, K., & Stöcker, C. (2013, January 18). Data Protection: All You Need to Know about the EU Privacy Debate. *Spiegel Online*. Retrieved from http://www.spiegel.de/international/europe/the-european-union-closes-in-on-data-privacy-legislation-a-877973.html

Lotz II, G. B. (2007). Checks and imbalances?: intelligence governance in contemporary

France. In H. Born & T. M. Wetzling (Eds.), *Democratic Control of Intelligence Agencies* (pp. 109–125).

Louis Harris and Associates. (1992, February 23). Americans are concerned about threats to their personal privacy. Louis Harris and Associatioes.

Louis Harris and Associates. (1997). Our privacy in Danger. Privacy and American Business.

Louis Harris and Associates. (1998). Privacy Concenrs & Consumer Choice. Privacy and American Business.

Lovells, H. (2013, January 23). EU Senior Privacy Officials Share Views on Draft Regulation [Corporate]. Retrieved October 23, 2015, from http://www.hldataprotection.com/2013/01/articles/consumer-privacy/hogan-lovells-privacy-leader-convenes-eu-privacy-officials-for-lively-discussion-of-proposed-regulation/

LQDN. (2013a, January 23). Press Release: US Corporations Win Against Privacy in EU Parliament Consumer Committee. Retrieved from https://www.laquadrature.net/en/us-corporations-win-against-privacy-in-eu-parliament-consumer-committee

LQDN. (2013b, February 21). Press Release: Citizens' Privacy Jeopardized in EU Parliament Committees Again. Retrieved from https://www.laquadrature.net/en/citizens-privacy-jeopardized-in-eu-parliament-committees-again

LQDN. (2013c, March 19). Press Release: Will You Let Protection of Your Data Go Down the Drain? Retrieved from https://www.laquadrature.net/en/will-you-let-protection-of-your-data-go-down-the-drain

Lustick, I. (2006). *Trapped in the War on Terror*. University of Pennsylvania Press.

Lynn, C. J. H. L. E. (2000). *Governance and Performance: New Perspectives*. Georgetown University Press.

Lynskey, O. (2015). Control over Personal Data in a Digital Age: Google Spain v AEPD and Mario Costeja Gonzalez. *The Modern Law Review*, *78*(3), 522–534. http://doi.org/10.1111/1468-2230.12126

Lyon. (2001). *Surveillance Society*. McGraw-Hill Education (UK).

Maass, P. (2012, 28). Your FTC Privacy Watchdogs: Low-Tech, Defensive, Toothless.

Wired. Retrieved from http://www.wired.com/threatlevel/2012/06/ftc-fail/3/

MacAskill, E. (2013, August 23). NSA paid millions to cover Prism compliance costs for tech companies. *The Guardian*. Retrieved from http://www.theguardian.com/world/2013/aug/23/nsa-prism-costs-tech-companies-paid

MacAskill, E., Borger, J., Hopkins, N., Davies, N., & Ball, J. (2013a, June 21). GCHQ taps fibre-optic cables for secret access to world's communications. *The Guardian*. Retrieved from http://www.guardian.co.uk/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

MacAskill, E., Borger, J., Hopkins, N., Davies, N., & Ball, J. (2013b, June 21). The legal loopholes that allow GCHQ to spy on the world. *The Guardian*. Retrieved from http://www.theguardian.com/uk/2013/jun/21/legal-loopholes-gchq-spy-world

MacAskill, E., Davies, N., Hopkins, N., Borger, J., & Ball, J. (2013, June 17). GCHQ intercepted foreign politicians' communications at G20 summits. *The Guardian*. Retrieved from http://www.theguardian.com/uk/2013/jun/16/gchq-intercepted-communications-g20-summits

Mahoney, C. (2007). Lobbying Success in the United States and the European Union. *Journal of Public Policy*, *27*(01), 35–56. http://doi.org/10.1017/S0143814X07000608

Mahoney, C. (2008). *Brussels Versus the Beltway: Advocacy in the United States and the European Union*. Georgetown University Press.

Majone, G., & Wildavsky, A. (1979). Implementation as Evolution. In *Implementatino* (Second, pp. 163 – 180). Berkeley, California.

Martin, H.-J. (1995). *The History and Power of Writing*. University of Chicago Press.

Marx, K., & Engels, F. (1967). The communist manifesto (1848). *Trans. AJP Taylor. London: Penguin*.

Mastenbroek, E. (2003). Surviving the deadline the transposition of EU directives in the Netherlands. *European Union Politics*, *4*(4), 371–395.

Mattelart, A. (2010). *The Globalization of Surveillance*. Polity.

Mayer, J. D. (2002). 9-11 and the secret FISA court: From watchdog to lapdog. *Case W. Res. J. Int'l L.*, *34*, 249.

Mazmanian, D. A., & Sabatier, P. A. (1983). *Implementation and Public Policy*. Scott,

Foresman.

McConnell, G. (1966). *Private Power & American Democracy*. New York: Vintage Books.

McCraw, T. K. (1994). Business & government, the origins of the adversary relationship. *The New Deal and Corporate Power : Antitrust and Regulatory Policies during the Thirties and World War II / Edited with Introductions by Robert F. Himmelberg*.

McCraw, T. K. (2009). *Prophets of Regulation*. Harvard University Press.

McCubbins, M. D., & Schwartz, T. (1984). Congressional oversight overlooked: Police patrols versus fire alarms. *American Journal of Political Science*, 165–179.

McGrath, C. (2005). *Lobbying in Washington, London, and Brussels: The Persuasive Communication of Political Issues*. E. Mellen Press.

McNutt, J., & Boland, K. (2007). AstroTurf, Technology and the Future of Community Mobilization: Implications for Nonprofit Theory. *Journal of Sociology and Social Welfare*, *34*, 165.

McNutt, J. G. (2010). Researching Advocacy Groups: Internet Sources for Research about Public Interest Groups and Social Movement Organizations. *Journal of Policy Practice*, *9*(3-4), 308–312. http://doi.org/10.1080/15588742.2010.487247

Meter, D. S. V., & Horn, C. E. V. (1975). The Policy Implementation Process A Conceptual Framework. *Administration & Society*, *6*(4), 445–488. http://doi.org/10.1177/009539977500600404

Microsoft. (2012, February). The EU's Proposed Data Protection Regulation: Microsoft's Position.

Miliband, R. (2009). *The State in Capitalist Society*. Merlin Press.

Mills, C. W. (1999). *The Power Elite*. Oxford University Press.

Mirowski, P., & Plehwe, D. (2009). *THE ROAD FROM MONT PÈLERIN*. Harvard University Press.

Moravcsik, A. (2014, February). Review of The Art of Lobbying the EU: More Machiavelli in Brussels. Retrieved October 2, 2015, from https://www.foreignaffairs.com/reviews/capsule-review/2013-12-17/art-lobbying-eu-more-machiavelli-brussels

Mueller, M. (2002). *Ruling the Root: Internet Governance and the Taming of Cyberspace*. Cambridge, Mass: MIT Press.

Mullerat, R. (2007). EU-US Data Protection: Vindicating Rights to Privacy. *European Union Miami Analysis*, *4*(14).

Muris, T. (2001, October 4). Protecting Consumers' Privacy: 2002 and Beyond. FTC. Retrieved from https://www.ftc.gov/public-statements/2001/10/protecting-consumers-privacy-2002-and-beyond

National Research Council. (2007). *Engaging Privacy and Information Technology in a Digital Age*. National Academies Press.

Negroponte, N. (1996). *Being Digital*. Vintage Books.

Nelson, F. (2015, October 22). British spies need our data, and we should let them have it. Retrieved from http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/11949030/British-spies-need-our-data-and-we-should-let-them-have-it.html

Neuhold, C., & Settembri, P. (2007). The role of European Parliament committees in the EU policy-making process. In T. Christiansen & T. Larsson, *The role of committees in the policy-process of the European Union legislation, implementation and deliberation* (pp. 152–181). Cheltenham, UK; Northampton, MA: Edward Elgar. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=198760

Newman, A. (2008). *Protectors of Privacy: Regulating Personal Data in the Global Economy*. Cornell University Press.

Newman, A. (2010). Innovating European Data Privacy Regulation: Unintended Pathways to Experimentalist Governance. In *Experimentalist Governance in the European Union: Towards a New Architecture* (p. Ch.2). OUP Oxford.

Newman, A. (2011a). Transatlantic flight fights: multi-level governance, actor entrepreneurship and international anti-terrorism cooperation. *Review of International Political Economy*, *18*(4), 481–505. http://doi.org/10.1080/09692291003603668

Newman, A. (2011b). Watching the Watchers: Transgovernmental Implementation of Data Privacy Policy in Europe. *Journal of Comparative Policy Analysis: Research and Practice*, *13*(2), 181–194. http://doi.org/10.1080/13876988.2011.555997

Newman, A. L., & Bach, D. (2004). Self-Regulatory Trajectories in the Shadow of Public Power: Resolving Digital Dilemmas in Europe and the United States. *Governance*,

17(3), 387–413. http://doi.org/10.1111/j.0952-1895.2004.00251.x

Nicholson-Crotty, S. (2009). The Politics of Diffusion: Public Policy in the American States. *The Journal of Politics*, *71*(01), 192–205. http://doi.org/10.1017/S0022381608090129

Nielsen, N. (2013, May 29). New EU data law could end up weaker than old one. Retrieved June 3, 2014, from http://euobserver.com/justice/120301

Norton-Taylor, R. (2013, June 11). Intelligence-gathering by British state out of control. *The Guardian*. Retrieved from http://www.theguardian.com/world/defence-and-security-blog/2013/jun/11/gchq-nsa-intelligence

Obama "We don't have a domestic spying program." (2013). Retrieved from http://www.youtube.com/watch?v=BSODrUHHuv0&feature=youtube_gdata_player

O'Brien, C. (2013, December 9). Apple, Facebook, Google call for government surveillance reform. *Los Angeles Times*. Los Angeles. Retrieved from http://www.latimes.com/business/technology/la-fi-tn-apple-facebook-google-call-for-government-surveillance-reform-20131209-story.html

O'brien, K. J. (2012, April 12). Facebook Offers More Disclosure to Users. *The New York Times*. Retrieved from http://www.nytimes.com/2012/04/13/technology/facebook-offers-more-disclosure-to-users.html

O'brien, K. J. (2013, January 25). European Privacy Proposal Lays Bare Differences With U.S. *The New York Times*. Retrieved from http://www.nytimes.com/2013/01/26/technology/eu-privacy-proposal-lays-bare-differences-with-us.html

OECD. (1975). Developments in Data Protection and Privacy. OECD.

Olmsted, K. S. (2000). *Challenging the Secret Government: The Post-Watergate Investigations of the CIA and FBI*. Univ of North Carolina Press.

Oppermann, K., & Viehrig, H. (2011). *Issue Salience in International Politics*. Routledge.

Packer, G. (2013, June 17). Big Brother and Silicon Valley. *The New Yorker*. Retrieved from http://www.newyorker.com/news/daily-comment/big-brother-and-silicon-valley

Parsons, D. W. (1995). *Public policy: an introduction to the theory and practice of policy*

analysis. Edward Elgar.

Paster, T. (2015). *Bringing power back in: A review of the literature on the role of business in welfare state politics* (No. 15/3). MPIfG Discussion Paper. Retrieved from http://www.econstor.eu/handle/10419/109041

Pearce, G., & Platten, N. (1998). Orchestrating Transatlantic Approaches to Personal Data Protection: A European Perspective. *Fordham International Law Journal*, *22*(5), 2024.

Peel, Q., & Fontanella-Khan, J. (2013, July 14). Angela Merkel calls for EU-wide agreement on data protection. *Financial Times*. London. Retrieved from http://www.ft.com/intl/cms/s/0/7a4b26d8-eca6-11e2-a0a4-00144feabdc0.html#axzz3z8lVzcz1

Penn Schoen Berland. (2014). Views from Around the Globe: 2nd Annual Poll on How Personal Technology is Changing our Lives. Microsoft.

Perrone, J. (2001, May 29). The Echelon spy network. *The Guardian*. Retrieved from http://www.theguardian.com/world/2001/may/29/qanda.janeperrone

Persily, N. (2015). *Solutions to Political Polarization in America*. Cambridge University Press.

Pertschuk, M. (1982). *Revolt Against Regulation: The Rise and Pause of the Consumer Movement*. University of California Press.

Petrison, L. A., & Wang, P. (1995). Exploring the dimensions of consumer privacy: an analysis of coverage in british and american media. *Journal of Direct Marketing*, *9*(4), 19–37. http://doi.org/10.1002/dir.4000090404

Pew Research Center. (2010, April 18). The People and Their Government. Distrust, discontent, anger and partisan rancor. Pew Resear. Retrieved from http://www.people-press.org/files/legacy-pdf/606.pdf

Pew Research Center. (2013, July 26). Few See Adequate Limits on NSA Surveillance Program. Pew Research Center. Retrieved from http://www.people-press.org/files/legacy-pdf/7-26-2013%20NSA%20release.pdf

Pierson, P. (2000). Increasing returns, path dependence, and the study of politics. *American Political Science Review*, 251–267.

Pierson, P. (2004). *Politics in Time: History, Institutions, and Social Analysis*. Princeton University Press.

Piltz, C. (2013). Facebook Ireland Ltd. / Facebook Inc. v Independent Data Protection Authority of Schleswig-Holstein, Germany—Facebook is not subject to German data protection law. *International Data Privacy Law*, *3*(3), 210–212. http://doi.org/10.1093/idpl/ipt007

Poitras, L. (2015). *Citizenfour*.

Poitras, L., Rosenbach, M., & Stark, H. (2013, June 30). Partner and Target: NSA Snoops on 500 Million German Data Connections. *Spiegel Online*. Retrieved from http://www.spiegel.de/international/germany/nsa-spies-on-500-million-german-data-connections-a-908648.html

Porch, D. (2003). *The French Secret Services: A History of French Intelligence from the Drefus Affair to the Gulf War*. Macmillan.

Porter, B. D. (2002). *War and the Rise of the State*. Simon and Schuster.

Prados, J. (2013). *The Family Jewels: The CIA, Secrecy, and Presidential Power*. Austin: University of Texas Press.

Prasad, M. (2006). *The Politics of Free Markets: The Rise of Neoliberal Economic Policies in Britain, France, Germany, and the United States*. University of Chicago Press.

Pressman, J. L., & Wildavsky, A. B. (1984). *Implementation: How Great Expectations in Washington are Dashed in Oakland : Or, why It's Amazing that Federal Programs Work at All, this Being a Saga of the Economic Development Administration as Told by Two Sympathetic Observers who Seek to Build Morals on a Foundation of Ruined Hopes*. University of California Press.

Prillaman, W. C., & Dempsey, M. P. (2004). Mything the Point: What's Wrong with the Conventional Wisdom about the C.I.A. *Intelligence and National Security*, *19*(1), 1–28. http://doi.org/10.1080/0268452042000222902

Privacy International. (2012, September 19). Summary analysis of European Commission proposal for a general Data Protection Regulation. Privacy International. Retrieved from http://www.statewatch.org/news/2012/sep/eu-dp-reg-pi.pdf

Przeworski, A., & Wallerstein, M. (1988). Structural Dependence of the State on Capital. *The American Political Science Review*, *82*(1), 11–29. http://doi.org/10.2307/1958056

Rainie, L., Kiesler, S., Kang, R., & Madden, M. (2013). *Anonymity, Privacy, and*

Security Online. Pew Research Center. Retrieved from http://www.pewinternet.org/files/old-media//Files/Reports/2013/PIP_AnonymityOnline_090513.pdf

Regan, P. (1995). *Legislating Privacy: Technology, Social Values, and Public Policy*. Univ of North Carolina Press.

Regan, P. (1999). American business and the European Data Protection Directive: Lobbying strategies and tactics. In R. Grant & C. Bennett, *Visions of privacy: Policy choices for the digital age* (pp. 217–228). Toronto: University of Toronto Press.

Regan, P. (2008). The United States. In J. B. Rule & G. W. Greenleaf (Eds.), *Global privacy protection: the first generation* (pp. 50 – 79). Cheltenham: Edward Elgar.

Roberts, J. (2005, September 30). Poll: Privacy Rights Under Attack. Retrieved January 23, 2015, from http://www.cbsnews.com/news/poll-privacy-rights-under-attack/

Rodrik, D. (2015). *Economics Rules: The Rights and Wrongs of the Dismal Science*. W. W. Norton & Company.

Rose, R. (1985). *Public Employment in Western Nations*. Cambridge University Press.

Rossi, A. (2014). Internet Privacy: Who Sets the Global Standard? *The International Spectator*, *49*(1), 65–80. http://doi.org/10.1080/03932729.2014.875823

Rotenberg, M., & Jacobs, D. (2013). Updating the Law of Information Privacy: The New Framework of the European Union. *Harvard Journal of Law & Public Policy*, *36*, 605.

Rothstein, B. (1998). *Just Institutions Matter: The Moral and Political Logic of the Universal Welfare State*. Cambridge University Press.

Rudner, M. (2004). Hunters and Gatherers: The Intelligence Coalition Against Islamic Terrorism. *International Journal of Intelligence and CounterIntelligence International Journal of Intelligence and CounterIntelligence*, *17*(2), 193–230.

Rule, J. B., & Greenleaf, G. W. (2010). *Global Privacy Protection: The First Generation*. Edward Elgar Publishing.

Rushe, D. (2013, April 12). Zuckerberg and Silicon Valley leaders launch immigration reform group. *The Guardian*. Retrieved from http://www.theguardian.com/world/2013/apr/11/mark-zuckerberg-launches-immigration-group

Ruyver, B., Vermeulen, G., & Beken, T. (2002). *Strategies of the EU and the US in*

Combating Transnational Organized Crime. Maklu.

Ryan, N. (1995). *Program Implementation in the Public Sector: Cases in Australian Industry Policy*. Royal Institute of Public Administration Australia.

Scanlon, C. (2001). A Step to the Left? Or Just a Jump to the Right? Making Sense of the Third Way on Government and Governance. *Australian Journal of Political Science*, *36*(3), 481–498. http://doi.org/10.1080/10361140120100677

Scheer, D. (2003, October 10). Europe's New High-Tech Role: Playing Privacy Cop to World. *Wall Street Journal*. New York. Retrieved from http://www.wsj.com/articles/SB106574949477122300

Schendelen, M. P. C. M. van, & Schendelen, R. V. (2010). *More Machiavelli in Brussels: The Art of Lobbying the EU*. Amsterdam University Press.

Schmid, G. (2001, July 11). Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098(INI)). European Parliament.

Schwartz, P. M. (2013). *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures* (SSRN Scholarly Paper No. ID 2290261). Rochester, NY: Social Science Research Network. Retrieved from http://papers.ssrn.com/abstract=2290261

Scott, M. (2015, May 25). Who's the Watchdog? In Europe, the Answer Is Complicated. Retrieved from http://bits.blogs.nytimes.com/2015/05/25/whos-the-watchdog-in-europe-the-answer-is-complicated/

Seamon, R. H., & Gardner, W. D. (2004). Patriot Act and the Wall between Foreign Intelligence and Law Enforcement, The. *Harv. JL & Pub. Pol'y*, *28*, 319.

Selznick, P. (1949). *TVA and the Grass Roots: A Study of Politics and Organization*. University of California Press.

Senior Advisor. (2016, January). Interview with anonymous Senior Advisor European Parliament.

Senior EU NGO Official. (2013, April). Interview with Senior Advisor of the European Green Party.

Senior Official EC Justice. (2013, April). Interview with European Justice Commission Senior Officials (off the record).

Sepper, E. (2010). Democracy, human rights, and intelligence sharing. *Tex. Int'l LJ*, *46*, 151.

Servent, A. R. (2013). Holding the European Parliament responsible: policy shift in the Data Retention Directive from consultation to codecision. *Journal of European Public Policy*, *20*(7), 972–987. http://doi.org/10.1080/13501763.2013.795380

Shaffer, B. (1995). Firm-level Responses to Government Regulation: Theoretical and Research Approaches. *Journal of Management*, *21*(3), 495–514. http://doi.org/10.1177/014920639502100305

Shuster, S. (2013, October 21). E.U. Pushes for Stricter Data Protection After Snowden's NSA Revelations. *Time*. Retrieved from http://world.time.com/2013/10/21/e-u-pushes-for-stricter-data-protection-after-snowden-nsa-revelations/

Sims, C. (1992, October 29). Silicon Valley Takes a Partisan Leap of Faith. *The New York Times*. Retrieved from http://www.nytimes.com/1992/10/29/business/silicon-valley-takes-a-partisan-leap-of-faith.html

Sinclair, M. (1985, February 7). Consumer Groups Seek New Focus For Action. *The Washington Post*, p. 1. Washington, D.C.

Slaughter, A.-M. (2001). The accountability of government networks. *Indiana Journal of Global Legal Studies*, 347–367.

Smith, M. A. (2010). *American Business and Political Power: Public Opinion, Elections, and Democracy*. University of Chicago Press.

Snider, L. B. (2008). *The Agency and the Hill*. Government Printing Office.

Spar, D. (1999). Lost in (Cyber)space. In A. C. Cutler, V. Haufler, & T. Porter, *Private Authority and International Affairs* (pp. 31–48). SUNY Press.

Spiegel. (2012, October 17). "The Right to Be Forgotten": US Lobbyists Face Off with EU on Data Privacy Proposal. *Spiegel Online*. Retrieved from http://www.spiegel.de/international/business/us-government-and-internet-giants-battle-eu-over-data-privacy-proposal-a-861773.html

Spiegel. (2015, April 24). Spying Close to Home: German Intelligence Under Fire for NSA Cooperation. *Spiegel Online*. Retrieved from http://www.spiegel.de/international/germany/german-intelligence-agency-bnd-under-fire-for-nsa-cooperation-a-1030593.html

Sprenger, P. (1999, January 26). Sun on Privacy: "Get Over It." *Wired*. Retrieved from http://www.wired.com/politics/law/news/1999/01/17538

Steiner, P. (1993, 05). On the Internet, Nobody Knows You're a Dog. *The New Yorker,*

69(20).

Steinmo, S. (1994). American exceptionalism reconsidered: culture or institutions. *The Dynamics of American Politics: Approaches and Interpretations*, *106*, 117–24.

Steinmo, S. (1996). *Taxation and Democracy: Swedish, British and American Approaches to Financing the Modern State*. Yale University Press.

Steinmo, S. (2003a). New institutionalism. In P. B. Clarke & J. Foweraker (Eds.), *Encyclopedia of Democratic Thought* (pp. 462 – 464). London: Routledge.

Steinmo, S. (2003b). The evolution of policy ideas: tax policy in the 20th century. *The British Journal of Politics & International Relations*, *5*(2), 206–236. http://doi.org/10.1111/1467-856X.00104

Steinmo, S., & Watts, J. (1995). It's the Institutions, Stupid! Why Comprehensive National Health Insurance Always Fails in America. *Journal of Health Politics, Policy and Law*, *20*(2), 329–372. http://doi.org/10.1215/03616878-20-2-329

Strauss, J., & Rogerson, K. S. (2002). Policies for online privacy in the United States and the European Union. *Telematics and Informatics*, *19*(2), 173–192. http://doi.org/10.1016/S0736-5853(01)00012-0

Swank, D. (1992). Politics and the Structural Dependence of the State in Democratic Capitalist Nations. *The American Political Science Review*, *86*(1), 38–54. http://doi.org/10.2307/1964014

Swire, P. P., & Litan, R. E. (1998). *None of your business: world data flows, electronic commerce, and the European privacy directive*. Brookings Institution Press.

The Atlantic. (2013, September 18). Facebook Nation: Mr. Zuckenberg goes to Washington [Interview]. Washington, D.C. Retrieved from http://www.theatlantic.com/technology/archive/2013/09/watch-mark-zuckerberg-talk-with-i-atlantic-i-editor-in-chief-james-bennet/279787/

Theoharis, A. G., & Immerman, R. H. (2006). *The Central Intelligence Agency: Security Under Scrutiny*. Greenwood Publishing Group.

Thomas, C. S. (2004). *Research Guide to U.S. and International Interest Groups*. Greenwood Publishing Group.

Tighe, M. (2012, January 7). Data commissioner: I was not too soft on Facebook. *The Sunday Times*. Dublin, Ireland. Retrieved from http://www.thesundaytimes.co.uk/sto/news/ireland/News/Irish_News/article853298.

ece

Tocqueville, A. de. (2004). *Democracy in America*. Library of America.

Tower, J. (1991). *Consequences: A Personal and Political Memoir*. Little, Brown.

Traynor, I. (2013, October 24). Angela Merkel: NSA spying on allies is not on. *The Guardian*. London. Retrieved from http://www.theguardian.com/world/2013/oct/24/angela-merkel-nsa-spying-allies-not-on

Traynor, I. (2014, May 8). 30,000 lobbyists and counting: is Brussels under corporate sway? *The Guardian*. London. Retrieved from http://www.theguardian.com/world/2014/may/08/lobbyists-european-parliament-brussels-corporate

Traynor, I., Olterman, P., & Lewis, P. (2013, October 24). Angela Merkel's call to Obama: are you bugging my mobile phone? *The Guardian*. Retrieved from http://www.theguardian.com/world/2013/oct/23/us-monitored-angela-merkel-german

United States. (1984). *Privacy and 1984: public opinions on privacy issues: hearing before a subcommittee of the Committee on Government Operations, House of Representatives, Ninety-eighth Congress, first session, April 4, 1984.* Washington: U.S. G.P.O. Retrieved from http://catalog.hathitrust.org/Record/007609593

United States, & Privacy Protection Study Commission. (1977). *Personal privacy in an information society: the report of the Privacy Protection Study Commission.* [Washington]: The Commission : For sale by the Supt. of Docs., U.S. Govt. Print. Off.

UPI. (1975, April 1). It's hard to overcome government regulation. *The Dispatch*, p. 11. Lexington.

US Congress. (1984). *Congressional Oversight of Covert Activities: Hearings Before the Permanent Select Committee on Intelligence, House of Representatives, Ninety-eighth Congress, First Session, September 20, 21, 22, 1983*. U.S. Government Printing Office.

US Senate. (1974a). *Privacy. Collection, use, and computerization of personal data. Joint hearings before the Ad Hoc Subcommittee on Privacy and Information Systems of the Committee on Government Operations and the Subcommittee on Constitutional*

Rights of the Committee on the Judiciary. Washington: US Government Priting Office. Retrieved from http://hdl.handle.net/2027/uc1.b5140223

US Senate. (1974b). Protecting Individual Privacy in Federal Gathering, Use and Disclosure of Information. Report of the Committee on Government Operations United States Senate to accompany S. 3418. US Government Priting Office.

US Senate. (1975a). *Alleged assassination plots involving foreign leaders: an interim report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities, United States Senate : together with additional, supplemental and separate views*. U.S. Govt. Print. Off.

US Senate. (1975b). *Oversight of Civil Aeronautics Board practices and procedures - hearings before the Subcommittee on Administrative Practice and Procedure of the Committee on the Judiciary, United States Senate*. Washington : Retrieved from http://hdl.handle.net/2027/uiug.30112106910083

US Senate. (1976). *Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities, United States Senate: Foreign and military intelligence*. U.S. Government Printing Office.

Van Der Valk, T. (2016, January 29). Interview with Thomas Van Der Valk, assistant of MEP Shopie in 't Velt (ALDE).

Various. (2009). *U.S. Presidential Inaugural Addresses from Washington to Obama*. The Floating Press.

Varoufakis, Y. (2011). *The Global Minotaur: America, The True Origins of the Financial Crisis and the Future of the World Economy*. Zed Books.

Versluis, E. (2007). Even rules, uneven practices: Opening the "black box"of EU law in action. *West European Politics*, *30*(1), 50–67.

Vitalis, A. (2008). France. In J. B. Rule & G. W. Greenleaf (Eds.), *Global privacy protection: the first generation* (pp. 80 – 106). Cheltenham: Edward Elgar.

Vogel, D. (1987). Political Science and the Study of Corporate Power: A Dissent from the New Conventional Wisdom. *British Journal of Political Science*, *17*(04), 385–408. http://doi.org/10.1017/S0007123400004841

Vogel, D. (2003). *Fluctuating Fortunes: The Political Power of Business in America*. Beard Books.

Walker, E. (2013). Grassroots mobilizations and outside lobbying. In *New Directions in*

Interest Group Politics (pp. 44–59). Routledge.

Walker, E. T. (2012). Putting a Face on the Issue: Corporate Stakeholder Mobilization in Professional Grassroots Lobbying Campaigns. *Business and Society*, *51*(4), 561–601. http://doi.org/10.1177/0007650309350210

Walker, E. T. (2014). *Grassroots for Hire: Public Affairs Consultants in American Democracy*. Cambridge University Press.

Walker, E. T., & Rea, C. M. (2014). The Political Mobilization of Firms and Industries. Retrieved from http://papers.ssrn.com/abstract=2475570

Warman, M. (2012, February 8). EU Privacy regulations subject to "unprecedented lobbying." Retrieved from http://www.telegraph.co.uk/technology/news/9070019/EU-Privacy-regulations-subject-to-unprecedented-lobbying.html

Warmund, J. (2000). Can COPPA Work-An Analysis of the Parental Consent Measures in the Children's Online Privacy Protection Act. *Fordham Intell. Prop. Media & Ent. LJ*, *11*, 189.

Weidenbaum, M. (1997). Regulatory Process Reform: From Ford to Clinton. *Regulation*, *20*, 20.

Weir, M. (1992). Ideas and the politics of bounded innovation. In *Structuring politics*. Cambridge University Press. Retrieved from http://dx.doi.org/10.1017/CBO9780511528125.008

Werner, T. (2012). *Public Forces and Private Politics in American Big Business*. Cambridge University Press.

West, H. (2014, September). Interview with Heather West.

WGIG. (2005, June). Report of the Working Group on Internet Governance. United Nations. Retrieved from http://www.wgig.org/docs/WGIGREPORT.pdf

Whitman, J. Q. (2004). The Two Western Cultures of Privacy: Dignity versus Liberty. *The Yale Law Journal*, *113*(6), 1151. http://doi.org/10.2307/4135723

Wills, A., & Vermeulen, M. (2011). Parliamentary oversight of security and intelligence agencies in the European Union. European Parliament.

Wilson, J. Q. (1974). *Political Organizations*. Princeton University Press.

Wilson, J. Q. (1980). *The Politics of regulation*. Basic Books.

Wolfe, H. P., & NewMyer, D. A. (1985). *Aviation Industry Regulation*. SIU Press.

Wonka, A. (2008). Europeanized Convergence? British and German Business Associations' European Lobbying Strategies in the Formulation of REACH. In J. R. Grote, A. Lang, & V. Schneider (Eds.), *Organized Business Interests in Changing Environments* (pp. 179–199). Palgrave Macmillan UK. Retrieved from http://link.springer.com/chapter/10.1057/9780230594913_9

Wood, D. M., & Wright, S. (2015). Before and After Snowden. *Surveillance and Society, 13*(2), 132–138.

World Bank. (2015, May 17). Internet users (per 100 people) [Database]. Retrieved March 14, 2015, from http://data.worldbank.org/indicator/IT.NET.USER.P2

World Economic Forum, & Bain & Company, Inc. (2011). Personal Data Report 2011. World Economic Forum. Retrieved from http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf

WP29. (2004, November 25). 12067/04/EN WP 101 - Declaration of the Article 29 Working Party on Enforcement. WP29.

WP29. (2009, February 10). 00350/09/EN WP 159 Opinion 1/2009 on the proposals amending Directive 2002/58/EC on privacy and electronic communications (e-Privacy Directive). Retrieved from http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2009/wp159_en.pdf

WP29. (2011, October 20). Press Release - 82nd meeting WP29. WP29.

WP29. (2012a, January 25). Press Release: Chairman of the Article 29 Working Party: Proposals a chance for better protection. WP29.

WP29. (2012b, October 5). Opinion 08/2012 providing further input on the data protection reform discussions.

WP29. (2013, December 4). Press release: Article 29 Working Party calls for swift adoption of the data protection reform package. WP29.

WP29. (2014a, April 10). 819/14/EN Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes. WP29. Retrieved from http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp191_en.pdf

WP29. (2014b, December 5). 14/EN WP 288 Working Document on surveillance of electronic communications for intelligence and national security purposes. WP29.

Retrieved from http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp191_en.pdf

WP29. (2015a, March 17). Press release on Chapter II of the draft regulation for the March JHA Council. WP29.

WP29. (2015b, June 17). Letter to Mr. Jan Philipp Albrecht. Retrieved from http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150617_letter_from_the_art29_wp_on_trilogue_to_mralbrecht_en.pdf

Wright, D., & Kreissl, R. (2014). *Surveillance in Europe*. Routledge.

Wright, M. I. (2011). *Surveillance Means Security: Remixed War Propaganda*. Seven Stories Press.

Wright, S. (2002). The ECHELON trail: An illegal vision. *Surveillance & Society*, *3*(2/3).

Yahoo! (2012, December). Rationale for amendments to draft Data Protection Regulation as relate to pseudonymous data.

Zaller, J. (1992). *The Nature and Origins of Mass Opinion*. Cambridge University Press.

Zegart, A. B. (2013). *Eyes on Spies: Congress and the United States Intelligence Community*. Hoover Press.

Ziegler, M. (2008). Pay No Attention to the Man behind the Curtain: the Government's Increased Use of the State Secrets Privilege to Conceal Wrongdoing. *Berkeley Technology Law Journal*, *23*, 691.