8-13-2019

The Development of Digital Human Rights in the European Union: How Key Interests Shape National and Regional Data Governance

Rebekah Dowd
Georgia State University

THE DEVELOPMENT OF DIGITAL HUMAN RIGHTS IN THE EUROPEAN UNION: HOW KEY INTERESTS SHAPE NATIONAL AND REGIONAL DATA GOVERNANCE

by

REBEKAH DOWD

Under the Direction of Charles Hankla, PhD

ABSTRACT

The European Union has the most restrictive data protection policies among democracies today, having created a regime of digital human rights. Yet what contributed to the decision by EU policy-makers to place supranational constraints upon personal and cyber data use? At the national level, Member States' preferences were influenced by three structural factors: domestic security threats, the growing digital economy, and the work of human rights advocates around data privacy. Law enforcement and security officials sought access to data for criminal prosecution and anti-terrorism purposes. Multinational firms asked for the freedom to transport data across borders, treating it as an economic commodity. Legal rights actors pressed for data privacy and protections. While none of these preferences have been mutually exclusive, EU policy convergence upon the digital human rights model is the result of pressure exerted by key states. Most particularly, epistemic experts and key political elites acted on behalf of the UK,

Germany, and France to turn the EU Commission and the Council in the direction of their national preferences for data governance. However, whether the EU can successfully maintain digital human rights as it attempts to export these norms to the global community remains to be seen. What is framed as human rights protections for data continues to give considerable leverage to data brokers and law enforcement officials to use data as they wish.

INDEX WORDS: personal data, privacy, human rights, data surveillance, security, anti-terrorism

THE DEVELOPMENT OF DIGITAL HUMAN RIGHTS IN THE EUROPEAN UNION: HOW KEY INTERESTS SHAPE NATIONAL AND REGIONAL DATA GOVERNANCE

by

REBEKAH DOWD

A Dissertation Submitted in Partial Fulfillment of the Requirements for the Degree of

Doctor of Philosophy

in the College of Arts and Sciences

Georgia State University

2019

THE DEVELOPMENT OF DIGITAL HUMAN RIGHTS IN THE EUROPEAN UNION: HOW KEY INTERESTS SHAPE NATIONAL AND REGIONAL DATA GOVERNANCE

by

REBEKAH DOWD

Committee Chair: Charles Hankla

Committee: Jelena Subotic

Toby Bolsen

Electronic Version Approved:

Office of Graduate Studies

College of Arts and Sciences

Georgia State University

August 2019

DEDICATION

To my family - Doyle, Jenson, Sydney, Ethan, Lily - who believed in me and this project, especially on the days when I believed in neither. I am forever grateful for the faith you placed in me. To my parents and siblings, who always said I was different; now I can prove it! To God, for giving me an insatiable curiosity about learning new things within the sociopolitical world, and for making a way for me to do just that.

ACKNOWLEDGEMENTS

This project would never have been completed, nor would have achieved the level of excellence that it did, without the wisdom, encouragement, and expert guidance given by my committee: Dr. Charles Hankla, Dr. Jelena Subotic, and Dr. Toby Bolsen. Dr. Hankla, thanks for being ever patient with my methodological questions and always keeping the theoretical argument before me. Dr. Subotic, your professional advice has been invaluable, and when I grow up I want to be as fearless as you are with your approach to life and research. Dr. Bolsen, thank you for signing onto a project out of your comfort zone; your positive attitude and content analysis suggestions helped me finish on time and with sound methodology. I will endeavor to be the kind of scholar my committee members modeled through their examples.

Next, an enormous thanks to my PhD cohort and colleagues. Only those who walk a mile in your shoes can possibly understand the challenges of finishing a dissertation. Richard - I love your dry sense of humor and your absolutely perfect work ethic. Tahmina - keep up the excellent fight for minority scholars everywhere. Recha – your ability to listen and offer analytical insight has helped me through writing blocks multiple times. Adnan - you are an amazing researcher, and I am so thankful you met me for many cups of coffee and patiently proof-read way too many documents.

Finally, to those who offered timely support at crucial times in my academic career, a thousand thanks to your timely support. Dr. Rik Newtson wrote a key letter of recommendation for me as a non-traditional student that generated opportunities for me in Oxford and changed the trajectory of my life to dream academic dreams. Dr. Lynn Robson opened the door to my many Oxford experiences and showed me by her example what it meant to encourage others to achieve

those dreams. Dr. Ian Finlay taught me how to write more rigourously; most importantly, he offered a word of affirmation in person and via email when it was most needed.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 INTRODUCTION: WHAT IS YOUR DATA:

1.1 Economic Commodity, Security Asset, or a Protected Human Right?

In mid-March 2018, the Cambridge Analytica data scandal broke onto the international news cycle. Over 50 million social media users in the U.S. and Europe had information about their internet behavior collected, analyzed, and catalogued for political use by candidates during recent elections, via the meta-data they generated while online with Facebook.[1] Facebook executive Mark Zuckerberg was called to task during subsequent hearings held by Congress and the European Parliament. In contrast to the limited or lack of data protections in many regions, when Members of the European Parliament (MEPs) met with Zuckerberg, they cited actual violations of legal protections for data that had been breached. Yet, one has to ask, why had Europe, and the EU in particular, established a more aggressive policy stance toward protecting personal data than did other regions?[2] This dissertation argues that protection of personal and internet-based data as a fundamental human right, which I call "digital human rights", emerged as a result of domestic and international pressures placed on EU policymakers. Domestically three key structural factors influenced national data laws. At the international level, membership in multiple international organizations caused states to comply with policy recommendations that led to data protection. In both scenarios, the strategic placement of legal and human rights scholars contributed to the expanding scope of digital human rights.

Digital human rights protections concern two types of data. Personal data can be data that exists in manual forms such as in traditional paper records, or in computerized databases. A

[1] Granville 2018

[2] Fuster 2016; EU policies over data began in 1973 with the *Community policy on data processing*. US action began with the 1977 US Privacy Protection Study Commission, resulting in no legally binding legislation. As of this writing, there remains no single comprehensive federal law that constrains data collection and use (see Jolly and Loeb 2017).

specific subtype of personal data is "cyber data." Cyber data describes information that is collected about individuals, including their personal internet preferences and habits, as well as private financial or personal information collected while they use the internet for any purpose. Both personal and cyber data involve information regarding individuals' demography, personal beliefs, and behaviors. Data governance has varied among EU states from the 1970s-1990s, falling into three main policy areas: treating personal data as an economic commodity, seeing it as a surveillance tool to protect national security, or tying personal data to privacy and identity rights. However, since the mid 1990s, the European Union (EU) has passed supranational data policies resulting in convergence around a largely protective data regime. The resulting complex institutional environment calls for uniformity of protection in some areas, but leaves policy gaps open to state interpretation in other areas.

Political science research examining data has explained policy-making in some areas areas, but has not addressed the motivations for creating digital human rights in the European Union. One group of literature has examined the treatment of data as an economic commodity and has looked at its impact upon the larger global economy.[3] Other research has treated data as a byproduct of larger internet governance, focusing on early internet infrastructure policies,[4] attempts to explain the securitization of the internet for military purposes,[5] or projects that identified the use of information distribution on the internet as a civil society space.[6] Each of these bodies of research have *not* answered the question as to why digital human rights emerged to be a mandate for the entire EU, despite the variance in national policy preferences over data governance. This project seeks to amend this gap in understanding of how and why the European

[3] Mayer-Schönberger and Cukier 2013; Mayer-Schönberger and Ramge 2018.
[4] Mueller 2010
[5] Choucri 2012
[6] Powers 2015

Union policy has trended toward a particularly rights-based stance on personal and cyber data, the phenomenon of digital human rights.

1.2 Theoretical Foundation

This dissertation posits that the origin of digital human rights in the EU began in the 1970s with the national level policies set by individual states. During Phase 1 (1970s-1990s), the public and private sector use of computerizing personal data expanded rapidly. Individual states had to decide how to treat the rapid growth of databank creation, automatic processing of data, and data storage. Policies varied in three distinct directions. Some states saw personal data as important to the flow of business in the Single Area Market, so these states sought freedom of movement for data as a good or service. Some states also identified data as a tool to be used by law enforcement; these states legalized access to personal data by various sections of security-focused officials. Finally, some EU states added legislated protection of personal and later cyber data, linking these protections to the larger human rights regime of privacy for individuals. None of these policies are mutually exclusive, but when these interests came into conflict, each state had to choose a hierarchical preference for how data would be treated, essentially generating a normative and therefore legislated policy preference that drove other interests into secondary positions.

At the beginning of Phase 2 (mid 1990s), the widespread diffusion of internet use forced all advanced economies to acknowledge the need to set cyber data policies. As noted, individual EU states had been legislating at the national level, but little region-wide coherence existed. In fact, in some cases, the Phase 1 national data policies across the European Union worked in conflict with one another during times of data transfer in business or during security cooperation events. International governmental organizations (IGOs) such as the Organisation for Economic

Cooperation and Development (OECD) and the Council of Europe (CoE) offered suggested a series of protective frameworks for member states to adopt as national policies on the treatment of all types of data that would reduce the policy confusion and facilitate better cooperation between states. The European Commission responded to this pressure by opening opportunities for data governance to be moved onto the wider EU legislative agenda. Following the logic of the national laws that treated data as an economic commodity, a security tool, or an identity-based and protected human right, the EU Commission, Council, and Parliament faced policy convergence challenges related to the differing state preferences for data treatment. During the legislative process, the EU Commission and Council relied upon epistemic, or legal professionals who provided advice on policy options for the Union. The preferences of particularly influential states such as Germany (rights-based protections) and the U.K. (data commodification as an economic tool), prevailed at the supranational level. Despite increased numbers of EU data laws, the evolution of data protection policies remains a little understood phenomenon in the Union, leaving scholars and laypersons alike with a lack of information on how we got to where we are and the wider implications this stance may have not only for EU politics, but for regional and global data governance.

The recent Cambridge Analytica scandal exemplifies the core dilemma I address in this dissertation: *How and why do personal and cyber data policies get created in relation to states' interests for data securitization, data commodification, or protection of digital human rights?* I propose that the answer to this and related questions can be answered using international relations scholarship. By using a theory-based approach, understanding can be found. All democracies exist within a dense environment of multiple stakeholders when they make policies involving multiple countries. European Union states are no exception to this.

When these states also happen to be members of international organizations outside the EU, the process of policy-making gets even more complex, due to the multiplicity of membership commitments. What we see today is a relatively aggressive and unique policy style by the EU regarding the governance of data that emerged from this intensely pressurized policy space. First and foremost, this dissertation proposes that data legislation in the European Union happened at two levels.[7] National policymakers were constrained by the wishes of domestic interest groups. These groups organized and advocated for laws that would be most beneficial to them. Second, national governments were expected to abide by the constraints of membership in a variety of international governmental organizations (IGOs) which also placed demands on member states to pass certain types of data laws.

1.3 The Role of Regimes

The formalization of a set of laws about an issue is known as an institution, or *regime*. Stephen Krasner defined regimes as, "principles, norms, rules, and decision-making procedures around which actor expectations converge in a given issue-area."[8] Regimes have been created to handle the treatment of personal and cyber data at the national level in all EU states. However, regimes also exist at the international level which also impact national and regional data legislation. European states have joined a variety of international regimes, which include but are not limited to, the United Nations (UN), the Organization for Economic Cooperation and Development (OECD), and the European Union, each of which have suggested policies for states in the areas of concern to the IGO and its larger mission. Over time, a regime complex emerged, with potential overlap of national and international policies on data treatment. Thus, important

[7] Putnam 1988; Milner 1997.
[8] Krasner 1983, p. 185

point one is: **personal and cyber data policies set by individual EU states were created in an environment of regime membership and regime complexity.[9]**

Each regime had different goals which shaped the resulting laws. In the 1970s, personal data was moved from paper or manual form to computerized and automatically-processed data. National regimes (data legislation) in this period were designed to preserve the ability of companies to collect and store computer-based, or stationary, yet nationally-networked data in the most secure manner possible. In the 1980s, international data protection regimes were formed. The OECD began to encourage policy convergence designed to protect data privacy, but also asked states to allow the movement of computerized data across national borders to facilitate economic growth and business transactions.[10] EU states generally complied by adopting legislation at the national and EU level to free transnational data flows required by economies increasingly reliant upon service-based and technology industries. By the mid 1990s, data transmission via the internet was treated similarly to other data, and existing policies for computer data banks, and personal data treatment were applied to the management of this new type of data: cyber data.

Thus I will show that the initiative behind the early days of EU data governance policies was rooted in **the economic commodification of data, and this became the first widespread EU regime for data governance**. Internet access was increasingly linked with other economic commodities in the minds of both corporate leaders and governments, as well as in the minds of economic development researchers. ICT products and/or services were believed to hold latent

[9] To make this dissertation more manageable, and to comply with the rigors of qualitative and quantitative methodology, I will limit this evaluation to EU Member States, rather than the entire list of European states. A regime complex can be defined as an overlap of multiple national, regional, or international regimes that involve shared issue concerns and at times, policy coordination.
[10] Fuster 2016; OECD 2009, 2011

potential for contributing to economic growth.[11] In time, cyber data became economically commodified, or identified as a value-based commodity, within the ICT sector. As mentioned, cyber data was treated as an extension of general data, to be managed with the discretion of data processors and controllers, and policies were set to cover its use.[12] The links between internet access and economic growth, and later the role that cyber data could play in that growth was an important aspect of policy that corporations would aggressively defend in years to come, when the economic protections of data would be threatened by increased technological change and demands for protection coming from the legal and human rights communities. The most significant challenge to the commodification of data occurred in the began in the 1970s but grew exponentially in the early 2000s.

In the mid 1970s and 1980s, several EU states experienced domestic terror attacks by radical leftist, separatist, or Palestinian sympathetic groups. These attacks diminished somewhat in the 1990s. However, law enforcement, criminal prosecutors, and national security officials expanded efforts to use personal data as information-gathering mechanisms to prevent, track, and prosecute domestic terrorists attacks that occurred during this period. Data collection and monitoring was also seen as an additional way to ensure border security from outside terrorists coming in.[13] Many legislatures argued for data collection privileges to be legalized for law enforcement during debates on data legislation. Such efforts intensified following the September 11, 2001 terrorist attack in the U.S**.,** and the subsequent attacks to London and Madrid in 2004 and 2005. EU officials realized the expanded regional risk of threats to public spaces, as well as to important data and financial infrastructures.[14] Securitizing data became the new buzzwords

[11] Meijers 2014
[12] Fuster 2016
[13] Choucri 2012; Longo 2018; Wallace, Pollack and Young 2015
[14] Franda 2001

among government and academic researchers alike.[15] The **heighted security concerns opened an additional data regime space in which personal and later cyber data would be simultaneously protected while also serving as a surveillance tool by state authorities**. Areas of securitized data legislation were broad. Early years it was as simple as giving law enforcement access to public databanks. From the 2000s, legislative regimes were created to govern internet infrastructure, and internet practices, including those that generate finance-based data.[16] Access to the meta-data generated by internet or mobile phone use was another part of the package of approaches used.[17] Further laws covered cyber space and telecom technology[18] and clamped down on online counter-narratives used in terrorist or anti-state propaganda flows online. [19] Personal and cyber data were securitized.[20]

Lastly, I propose that a **third data regime exists in the European Union, in which the framing of human rights protections has been extended over personal and cyber data to create a digital human rights regime.** At the national level, I show in my case country studies that several EU states had histories of establishing privacy protection for personal data. In Sweden, data protection legislation arose due to an extensive history of open access to government records. When government records were computerized in the 1960s and 1970s, the public and government wanted data protection legislation to ensure certain information was not open to public scrutiny. In Germany, the public insisted on data protection as a part of a larger effort to constrain government surveillance tendencies. As government databanks shared information across sectors, regional governments in the *Länders* created personal data protection

[15] Mueller 2010
[16] Lynn III 2010
[17] Meta-data: "data about the data", R. J. Deibert, 2013.
[18] Choucri 2012; Rosecrance 1996
[19] Goldsmith and Wu 2006
[20] Cavelty 2013; Mueller 2010 – Chapter 8.

laws in the 1970s. The Hessian law in particular influenced the federal framework adopted in the 1977 federal data protection law. Finally, in the UK, human rights-minded advocates had pushed for data legislation to no avail for over a decade. Following recommendations made by the Council of Europe, the UK signed but had not ratified a convention calling for national data protection which would provide regionally similar laws during transborder data flows. Only when economic interests pushed the Thatcher government in the 1980s to either legalize personal data protection or risk business volume loss in a competitive European environment did the government pass such a law.

Though several bodies within the EU had proposed an EU law for data protection since the 1980s, the momentum was slow in building.[21] The Single Market initiative and technology catch-up programs fueled enough momentum for EU data legislation in the 1990s to finally yielded some results. The Commission issued a recommendation for a directive to cover the matter in 1990. The Maastricht Treaty included clauses to protect data secrecy, but allow for data exchange during police cooperation.[22] Directive 95/46/EC established the first supranational EU legislation on data protection, and served as the core basis for data protection in the region until it was replaced in 2018. From 1997-2018 when Directive 95 was enforce, EU states' harmonized their national protections in accordance with the directive. Occasionally, the Commission, Council of Ministers, or Parliament would ask for updates or amendments. Any amendments were subject to or at times originated from a permanent working committee, the Article 29

[21] 1973 Commission call for Community policy on data processing – SEC 73 (final); 1979 Parliament Resolution on the protection of the rights of the individual in the face of technical developments in data processing; Commission Recommendation of 29 July 1981 relating to the Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data – OJ L247/31, recital 5; Commission EC Adoption of Directive Proposal Com (90) 0314-C3-0232/090-SYN 287.
[22] See Article 20.
[22] Maastricht Treaty, p. 108, 92/C 191/01 (Council of the European Communities, Commission of the European Communities 1992)

Working Committee, whose sole job it was to oversee data legislation implications for the EU. This body would vastly expand the notion of data protection rights in ways that created the digital human rights regime referred to earlier. This committee provided core and substantial support for the replacement law, the General Data Protection Regulation (GDPR). The GDPR has fundamentally altered the global landscape for legislating data protection by not only updating and expanded data protection, but by insisting that third countries abide by EU data protection mandates.

In summary, the data **regime complex of the EU is due to a combination of national, regional, and international influences.**[23] National laws, EU level data regulations, and the recommendations by the OECD and Council of Europe regarding data protection generated a data regime complex. Furthermore, EU states have had national data laws that rivalled or competed with neighbor states, which also conflicted with the recommendations of the IGOs.[24] This dissertation will explain how the data regime complex evolved in the EU, and how policy compromise has been reached in the wake of changing internal and external conditions.

As complex as the regimes themselves are, the research literature on the topic of data governance has produced a variety of research on data governance. There have been three primary turns of scholarship regarding these policies. They include the treatment of data as an economic commodity, the securitization of the internet and internet-generated data, and the freedom of access to data and information as a public good. By outlining the findings of this literature, I show that the contributions of this literature to the theory of this dissertation and also

[23] Orsini, Morin and Young 2013, pg. 6; definition: A *regime complex* occurs when, "a network of three or more international regimes that relate to a common subject matter [exist and] exhibit overlapping membership, and generate substantive, normative, or operative interactions recognized as potentially problematic whether or not they are managed effectively."
[24] Drezner 2007

the areas in which this literature failed to explain the origin of digital human rights in the European Union.

1.4 Internet and Internet Data as an Economic Commodity

First, researchers have shown that data is linked to economic development potential. Going back the the 1980s, the OECD promoted the idea that data commodification (treatment of data as an economic commodity) was crucial to economic growth among its member states. Later, it would promote internet expansion as a crucial link to improve communication and therefore grow business volume, two key barriers to economic growth in low development states.[25] Lumping data mobility and internet access with access to telephone, electricity, or banking services, developmental economists emphasized the importance allowing developing states to generate economic opportunities and facilitate growth via data processing and internet diffusion.[26] A smaller section of this research disagreed with that notion, by showing that ICT expansion, including internet connection, did not contribute directly to larger economic growth, but rather improved trade.[27] Increased trade then led to expanded growth. Cast as facilitators of other business activity, data and internet diffusion were viewed as highly important to economic growth according to this literature.

In a slightly different look at the financial impact of the data, newer work focused on the economic value of "big data" generated through internet use.[28] Identification of big data as an economic commodity, similar to labor or capital, has shaped the business model of successful

[25] https://www.oecd-ilibrary.org/science-and-technology/oecd-digital-economy-papers_20716826?page=16 ; OECD 2009.
[26] Oyedemi 2015
[27] Meijers 2014
[28] Big data includes cyber data generated by mass volume of internet use on mobile and internet-ready devices. Big data includes the front end data (personal details that are divulged, text typed) as well as meta-data (likes, content visited, internet use patterns, internet profiling of users).

multinational corporations such as Google and Apple.[29] These huge online companies whose services generate big data have produced the largest amount of growth in technological and service-based economies.[30] As states attempt to securitize or protect cyber data, including data managed by big data firms like Microsoft and Amazon, these corporations pushed back to ensure that their freedom to operate a data profiteering business model was protected.[31] Data-based companies initially hid the fact that their profits depended on the continued ability to collect data from consumers without restriction and then sell this data to other corporations. They proposed that internet freedom is a human right of access to information, when in fact what these firms offer is the right to access the internet marketplace.[32] As noted with the Cambridge Analytica scandal at the beginning of this chapter, the public and governments are now aware that surveillance capitalism is the way that information brokerage firms succeed in business.

Looking forward, social scientists predict that data-rich markets will continue to evolve and impact the mechanisms by which consumers do business.[33] Viktor Mayer-Schönberger and Thomas Ramge (2018) hypothesize that the exponential power of the internet to facilitate communication will likely alter the value of money through an effect upon market coordination.[34] They argue that data-rich markets will disproportionately benefit big-data intermediaries (including data brokers Amazon or Google), who will transmit the latent wealth in data to the markets that need it most. If the banking industry and traditionally organized firms do not adapt to the commodification of big data, and adjust their business practices accordingly,

[29] Mayer-Schönberger and Cukier 2015; Zuboff 2015
[30] Jorgensen 2017
[31] Upcoming: F. Cheneval 2017; Jorgensen and Desai 2017
[32] Powers 2015
[33] Burton-Jones 1999; Mayer-Schönberger and Cukier 2013; Mayer-Schönberger and Ramge 2018; Powers 2015.
[34] Mayer-Schönberger and Ramge 2018

their ability to profit from data-rich markets will be minimized at best and non-existent at worse. This literature would support the argument of a regime based on data commodification made earlier.

1.5 Freedom of Access/The Internet as a Public Good

Further literature treats the internet and general data available on it as more of a civil society mechanism.[35] According to this line of thought, similar to television, radio, and the newspaper, internet sites, social media, and the information on the internet serve as a way for individuals to hold their governments and larger society accountable to the political expectations of their particular culture.[36] As a result, individuals and groups are able to practice an extended form of civil action uses data as a tool of activism.[37] In fact, political participation in the modern world is handicapped if a population cannot access internet information or use information communicated via mobile methods to voice concerns about government misbehavior.[38] Lack of internet access, or having government restrictions upon how individuals access the global offerings of the internet and communicate with each other is identified as limiting political human rights, similar to restrictions on public protests, or secret ballot voting.[39] In addition, internet diffusion and cyber information access has opened political opportunities to communities previously politically disenfranchised.[40] Online activism has occurred around many issue areas, including contentious multilateral investment agreements,[41] NGOs pushing

[35] Margetts, et al. 2016; Powers 2015
[36] Deibert, et al. 2010; Karpf 2016)
[37] Margetts, et al. 2016
[38] Godberg 2011
[39] Joyce 2015; Wicker and Santosa 2013)
[40] Norris 2001
[41] Deibert 2000

for the international mine ban treaty,[42] and the Arab Spring protests.[43] Research shows that the internet has become an informational tool and a new public space for the exchange of political debate.[44]

One additional group of literature has addressed the internet as political tool used by states rather than non-state actors.[45] For instance, China and Russia created the International Code of Conduct for Information Security inside their Shanghai Cooperation Organization in 2011, primarily as a challenge to US hegemony in international cyber structure policy. Alongside trying to determine how the international community treats cyberspace, China has set the most aggressive protection against global internet exposure, by setting protocols programmed into routers or software at key choke points designed to block content for citizens.[46] Needless to say, the lists of prohibited content include anything critical of state practices or the Communist party, in addition to any Western entertainment content deemed a threat to Chinese culture. China is not alone, as Russian authorities have blocked access to Skype and Facebook, among other online locations, with access to such sights deemed "politically disruptive".[47] While Western states identify internet access as a space insuring political participation, non-Western states fear the threat to control of citizens. Notably this entire section of literature discusses access to information, some of which is online, but leaves out the implications of internet governance that involves collection and dissemination of personal data.

---

[42] Beier 2003
[43] Eltantawy and Wiest 2011; Wolfsfeld, Segev and Sheafer 2013
[44] Papacharissi 2010; Tolbert and McNeal 2003
[45] Choucri 2012
[46] Deibert and Rohonzinski - Chapter 1, *Access Controlled*, volume edited by Deibert, Palfrey, Rohonzinski, and Zittrain, 2010
[47] Nocetti 2015

1.6 Data Securitization

The last body of literature indirectly discusses data governance, with the main focus upon state-driven security policy. States utilize the internet as a form of cyber and informational warfare, and rely upon it for data surveillance. The underlying assumption in this literature is the ever-present threats between states which drives states to get creative and look for new ways to utilize information and develop "virtual weapons" as strategies for national defense or offense.[48] Cyber attacks can be perpetrated by other states or private actors who use "deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks."[49] Cyber defense strategy that utilizes personal or cyber information includes surveillance mechanisms, deployment of espionage software to spy on other states communications, and denial of service attacks on critical infrastructure like government or banking websites (purportedly used by Russia against Georgia and Estonia).[50] "Confidentially attacks" (illegally obtaining intellectual property) have contributed to sticky relations between the U.S. and China.[51] Lastly, harnessing social media for "fake news" or release of previously secret files or data is another way states can seek to influence geopolitics.[52] Deibert (2013) notes states' focus on protection of military or economic interests, making data utilization a byproduct of the end goal of national security.[53] In another example of the impact of information surveillance on average citizens, the Snowden leaks revealed how states used data surveillance as a mechanism of anti-terrorism. States have vastly expanded surveillance tolerance laws resulting in mass invasions of personal and cyber data

[48] Kello 2017
[49] Owens, Dam and Lin 2009, pg. 1; National Research Council 2010, p. viii.
[50] Osnos, Remnick and Yaffa 2017; R. J. Deibert 2013
[51] Singer and Friedman 2014, p. 70
[52] Booking and Singer 2016
[53] R. J. Deibert 2013

privacy.[54] Snowden's revelations also inspired research looking at how individuals and other states respond to the invasive use of data surveillance inside and outside state lines.[55]

1.7 Prior Internet and Data Governance Research

A small group of literature has begun to address personal and cyber data policy as its own category of research. Since the 1990s when internet diffusion occurred in academia and governments, policy convergence models expected policy convergence due to the widespread invasion of privacy potential within networked databanks and internet use.[56] Milton Mueller (2010) provided an extensive look at how states respond to threats to general sovereignty due to transnational interconnectivity and increased communication between private actors.[57] Like Mueller, Abraham Newman (2008) expected global policy convergence favoring consumer data privacy given the pressure the EU has placed upon MNCs to protect individuals' identity when using EU citizens' data.[58] Yet since Mueller and Newman have conducted the above research, policy convergence has not occurred outside Europe. For instance, the US/Asian model relies upon corporate self-regulation of data privacy, while the EU has codified a more top-down regulatory model.[59]

In general, the data privacy literature has tried to explain legalization of the privacy aspect of data and how these laws effect states' behavior in terms of surveillance.[60] Internet policies could continue to address behavior-based protections, cover general functions of the internet, and/or allow for some "virtual forgetting" of digitized data when demanded by

---

[54] Edgar 2017
[55] Lyon 2014; *Surveillance, Privacy and Security*, edited volume by Michael Friedewald, J. Peter Burgess, Johann Čas**,** Rocco Bellanova, and Walter Peissl 2017;
[56] C. J. Bennett 1992; Dunleavy, et al. 2006
[57] Mueller 2010
[58] Newman 2008
[59] Newman 2008
[60] Bamburger and Mulligan 2013; Bennett 1992; Flaherty 1989; Fuster 2016; Newman 2008.

consumers.[61] There is worry that increased privacy protection could increase information costs to internet users, who will have to choose between free online services, or increased data protections.[62] Problematically, governments can and do collect data on individuals, and do not classify that practice as surveillance, but classify the collected data as a neutral commodity disconnected from the individual on the other side of a screen somewhere.[63] In other words, if a computer program collects the data and sifts it for dangerous activity, governments may not define this activity as an invasion of personal privacy. Despite these practices by the U.S. and other states, some of the public are willing to forego freedom of control over their data if it ensures protection against terrorists, or others seeking to harm the public.[64] Again, these expectations are driven by the convergence model.

1.8 Gaps this Project Will Fill

Little to no work has looked at the reasons behind differences in national policy outcomes. Why did high levels of protection first occur in Sweden and Germany, and not in the U.K.? Why did the U.K. finally acquiesce to EU data protections in the 1980s? The coordination of data policy during EU legislation has important implications not only for data policy research, but also as it exposes the compromises necessary when states have existing national legislation that conflicts with each other but must agree on shared policy to meet EU needs. How these differences were accommodated in the 1980s and 1990s when setting EU-level data policy is of crucial importance in an era of increasing political fracturization in several issue areas.

Divergences in states preferences continue to matter in the long-run, even after EU policy is set. For instance, increased economic woes in several EU states led to conflicts over EU fiscal

[61] H. Z. Margetts 2009
[62] Lenard and Rubin 2010
[63] Gros, de Goede and Isleyen 2017; Schneier 2015, p. 152
[64] Schneier 2015, p. 268

policy following the 2008 financial crisis. Member States such as Hungary or Poland have sought to regress on matters of judicial independence since 2015. The Brexit drama was largely motivated by disagreements over shared EU immigration and trade policies obligations. Given the fact that a convergence toward digital human rights has emerged in the *Europe Union,* and *nowhere else*, explaining this case of policy compromise can add understanding of EU policymaking. This study also generates important discoveries for the human rights and data governance literature, by seeking to explain further about which actors matter most during policy coordination and why some human rights-regimes emerge in a regional or global system.[65]

There are many factors that shaped the development of digital human rights legislation in the EU. The European Union was founded to ensure economic integration first and foremost, and the protection of the Single Market remains a priority. In the 1970s and 1980s, the EU Commission started multiple EU programmes to increase growth in various industries of the Information, Communications, and Technology (ICT) sectors. Even as late as 2014, the EU Commission added a strategy for a Single Digital Market to the Single Market programme, bringing data governance to center stage once again .[66] The interaction between economic interests intersected with human rights issues has gone virtually unexplored. Furthermore, the change to data policy following the September 11, London, and Madrid bombings has yet to be explained by prior literature on EU data governance. **Key questions that remain unaddressed include:**

> *Why did the national laws created by EU states follow three particular pathways (data profiteering, data as a surveillance tool, data protection)?*
>
> *Why did the EU settle upon the digital human rights model, rather than continue to pursue data commodification (the first EU data policy)?*

[65] Archarya 2011; Keck and Sikkink 1998; Moravscik 2000; Risse-Kappen, Ropp, Sikkink 1999; Weiss 2013
[66] European Union 2014

What role did key elites play in the adoption of or blocking of a comprehensive EU digital rights policy?

This dissertation will address these gaps in the literature with the following chapters.

Chapter 2 discusses the theoretical argument. Here I explain two phases of the causal path toward EU digital human right development. Structural factors contributed to national policy preferences. These factors included domestic security threats, contribution to the economy by ICT firms, and the input by legal and human rights scholars during initial national data legislation. National policies were created between 1970-1999, which I call "Phase 1." During "Phase 2" (the mid 1990s-present), the European Union created EU Directives and Regulations resulting in the emergence of digital human rights as the primary mechanism of policy for personal and cyber data. During this phase, states had to decide which national preferences would prevail at the EU level, and which compromises would be accepted when national policies were at conflict with one other.

Chapter 3 outlines the mixed methodology used to test the argument developed in Chapter 2. Phase 1 includes case studies of Sweden, Germany and the UK, where I trace the evolution of data policy outcomes (dependent variable) that occurred in the early days of data proliferation. I support these findings with descriptive statistics showing how key structural factors (independent variables), such as domestic terror incidents, economic dependence upon ICT sector growth, and the consultation of legal experts shaped national laws. I then evaluate policy-making during Phase 2, by looking at EU data policy (dependent variable) reached when key states (pushed their preferences independent variables and key experts served on advisory committees for the Commission and Council of Ministers. Testing of the Phase 2 hypotheses

includes analysis of communications by EU Commission and Council members, along with the placement and advocacy activities of relevant epistemic elites and professional experts.

Chapter 4 provides the details and findings for testing of Phase 1, during which the national policy preferences develop. This chapter argues that the United Kingdom and Germany developed quite different policy stances regarding data; the UK protected economic growth for ICT firms, and Germany federalized the regional policies of data protection. To trace the national policy process, I used qualitative analysis of legislative debates and committee reports for each national legislature during the law-making process. I also examined the professional background and types of consultants used to offer "expert advice" to parliamentarians when data laws were created or changed.

In Chapter 5 I explain the EU policy-making of Phase 2, during which supranational policies emerged for all EU Member States. This chapter introduces the role played by EU elites, including EU Commission Presidents and epistemic experts. Each states' preferences along the three main factors of security, economic commodification, and digital human rights provide predictions for the data policies France, Germany, and the UK will seek for wider EU law. To support the argument that key national elites influenced EU policies, I reveal how the policy agenda pursued by EU Commission presidents from 1990-2015 contributed to the opening of political opportunities for setting data policies at the EU level. I then look at how national epistemic communities expanded the scope of data protection into becoming digital human rights, with particular impact made by the Article 29 Working Party.

Chapter 6 will summarize the findings, and the expected impact to scholarship. During Phase 1, individual states made national data policies clearly influenced by structural factors of importance to each particular state. For Sweden, the emergence of tech-industries occurred late

in the 20th century, making the ICT impact upon data policy less of a factor than the impact of open records access to all government files. The Swedish population was so motivated to protect computerized data, the country developed the first national law for data protection in the world in 1973. Germany's history of personal rights violations that occurred during the Holocaust continued to shape national political discourse and preferences, both of which led to strong and ground-breaking data protection law of 1977. The United Kingdom's history of civil turbulence in Northern Ireland combined with a significant dependence on ICT industries drove national laws protecting data to preserve business activity, while preserving data access for security officials. The European Union policies during Phase 2 revealed the impact of policy preferences by the particular states. When French representatives served as President of the EU Commission, they were quite influential in opening the door for new data policies. However, the individuals serving on the Article 29 Working Party committee held disproportionate impact above that of EU Commission. Their ability to shape EU policy to the highest level confirmed the arguments of past IR theorists about the role that epistemic experts play in human rights diffusion.

In conclusion, this dissertation serves many beneficial purposes for broader social science scholarship. First, it applies relevant international relations paradigms to data governance, something not done in previous literature. Secondly, it uses qualitative research with extensive case studies and content analysis of national laws to show that certain interests *really* matter when it comes to national and international political outcomes. Next, it will help fill the gaps in our understanding of how EU Member States work within a contested and competitive regime environment to influence EU level legislation toward their preferred policy outcome. Lastly, this project will contribute to our understanding of how states respond to their organizational

membership requirements, especially when policies set by the organization conflict with national preferences.

2 THEORY IN-DEPTH: REGIME COMPLEXITY AND DATA PROTETION IN THE EUROPEAN UNION

Chapter 1 introduced three important questions:

Why did the national laws created by EU states follow three particular pathways (data profiteering, data as a surveillance tool, data protection)?

Why did the EU settle upon the digital human rights model, rather than continue to pursue data commodification (the first EU data policy)?

What role did key elites play in the adoption of or blocking of a comprehensive EU digital rights policy?

This dissertation answers these questions by theoretically arguing that **data protection policies in the EU occurred along two-levels, national and regional (EU). At the national level: key structural interests drove each state toward particular types of data policies that would preserve the concerns raised by those interests. At the EU-level, powerful states influenced the policy model to align with their national preferences. At both levels, strategically placed legal and human rights protecting elites expanded data protection to create a digital human rights regime for the European Union.** The process of interaction between domestic and international interests seen in EU data policy outcomes has the potential to inform policy-making around other issues, specifically as regards policy coordination more broadly. As policy coordination occurs at the regional level in multiple areas of the world, this dissertation contributes to the larger international relations and comparative politics literature about the process of policy negotiations.

European Union member states (MS) make technology policies following Putnam's two-level games argument: at the national level, domestic institutions have emerged to address data treatment, and at the international level, states were and are pressured by multiple international

governmental organizations (IGOs) in which they are members to set policies that agree with the mission of the IGOs.[67] In the early years (1970s) of computer use and computer network expansion, state policy-makers relied upon domestic structural components such as security concerns, the contribution of the ICT sector to the national economy, and legal rights activism around data protection as the primary variables driving national preferences on policies about data creation, processing, storage, and re-use. By the 1980s, the second level of coordination began inside the Council of Europe and the Organisation for Cooperation and Economic Development (OECD), where each IGO created a list of suggested policies for member states to adopt concerning data treatment. The presence of outside pressure from IGOs and inside pressure from key actors in the Union eventually caused the EU Commission to open the doors for a Union-wide policy for data governance. As a result of this 'policy opening' promoted by EU Commissioners throughout the 1980s and early 1990s, the EU passed multiple mandates that would impact member states' domestic policies, most importantly, Directive 46 (effective 1995-2018). EU policy on personal data and now cyber data has evolved to include digital human rights protections for data, in many ways above any security or economic concerns for the use of data.[68]

This chapter explains these claims. First, I outline the theoretical background of institutional theory, also known as regime theory, and how policy formation is conditioned by institutional creation, both domestically and internationally. I then develop the empirical argument that traces the causal claims between domestic structural factors and national data

[67] Putnam 1988.
[68] Directive 95/46/EC https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN
GDPR https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

policy preferences. Next, I discuss how regime theory explains the creation of EU data policies. Specifically, how the structural components of powerful states within the Union try to leverage their preferences for data treatment laws that will align with their own security, economic, or human rights concerns. Concerning EU legislation, I trace how EU policy-making is purportedly intergovernmental, but in the case of data policy it has increasingly leaned toward supranationalism.[69] I conclude with the argument the United Kingdom and Germany have shaped policy mandates for the entire Union. My argument is built on the foundation of institutional theory at the domestic level and regime theory at the international level.

2.1 National Level Policy-Making and Institutional Creation: Phase 1 (1970s-late 1980s)

Institutions, or the "rules of the game" serve as tools to protect the interests of various domestic actors who wish to see to particular policy outcomes that will benefit them.[70] There are numerous arguments by comparative political scientists and and sociologists that have shown how domestic institutions are created to protect a variety of key interests: economic, power base, or cultural.[71] [72] Douglass North (1990) maintained that institutions were created to improve upon the economic status quo, especially as regards economic efficiency and coordination.[73] To North, a rule/institution would be created and stay in place as long as it promoted wealth maximization and economic growth. Migdal (1988) showed that once government institutions or policies are in place, middle-level government agents will work to keep the institutions in place

[69] Within this dissertation, "intergovernmental" refers to joint coordination of policies by two or more states with shared interests. "Supranational" refers to policy that is imposed from above, superseding national policy, in some cases resulting in conflict occurs between the national and supranational policies.
[70] I use Douglass North's definition of institutions: "the rules of the game in a society." p. 3, North 1990.
[71] Migdal 1988, North 1990, Putnam 1993, Skocpol 1979, Tilly 1990
[72] The discussion in this dissertation is limited to formal institutions, and their contribution to regime creation.
[73] North 1990

as long as they served the interests of these individuals.[74] Tilly (1990) agreed with Migdal's proposal; the bourgeoisie will initiate the creation of policy-making agencies, whose ongoing function is to protect state bureaucratic interests, particularly in capitalist states. To Milner (1997), institutional creation is a rational way to coordinate policy outcomes and increase the likelihood of Pareto-optimal outcomes for states, by promoting distribution of goods better than during past arrangements.[75] In agreement with each of these scholars, I propose that domestic data laws are a form of institutional creation to serve the needs of domestic interests.

Policy development involves a few vital steps. The first stage is for policy-makers to decide what is defined as an important issue, thereby making it onto the national policy agenda.[76] Once the issue has been added to the agenda, policy decisions hinge on the need for cooperation on the distribution of various resources or goods, influenced by the nature and structures of domestic political power. [77] Wide institutional variance exists among EU states, in terms of parliamentary structures, political party participation, executive power distribution, and judicial oversight. The purpose of this dissertation is not to explain the variance in political institutions that exist among EU states. However, structurally speaking, all legislation at the national level of EU states operates according to basic rules of democracy – with parliamentary offices held by elected officials.[78] Political parties will thus seek public support for election and re-election using party issue platforms designed to ensure long-term political careers.[79] In the case of data policy in the European Union, what particular characteristics or interests at the domestic level pushed policy-makers into setting data policy and in what direction? I propose that European

[74] Migdal 1988
[75] Milner 1997
[76] Majone 1989, Stone 2012
[77] Birkland 2016, Schattschneider 2013, Stone 2012, Riker 1996
[78] Hix and Lord 1997
[79] Aldrich 1995, Downs 1957, Riker 1982

governments who seek voters' support will introduce and/or pass national policies (dependent variable) involving data regulation to meet the desires of interest groups in three structural areas (independent variables): economic interests, security concerns, and/or human rights protections for personal data. I now examine how each of these factors are important to the domestic interests of EU states.

2.2 Economic Interests

The literature evaluating the intersection of the economic interests of voters, corporate actors, and the state is quite complex. Economic voting research has uncovered mixed findings about the role of sector-based employment and voting support. Voters will punish incumbent governments, holding the government responsible for economic downturns.[80] Attribution of responsibility for periods of economic growth is less proven, however; voters seem to hold governments accountability for reversal of economic gains, rather than a lack of growth.[81] We do know that political and corporate interests can interact in ways that favor particular firms or sectors. Industries will most likely enjoy political influence when broad public-private coalitions exist allowing firms to lobby on behalf of industry concerns.[82] If low levels of conflict exist between the desires of political decision-makers, or if the interests of an economic actors and politicians align, governments will pass public policies that are favorable for these firms.

Technology-related sectors are known contributors to the economic growth of OECD states participating in the global marketplace during Phase 1 (1970s-80s).[83] The economic contributions by technology firms to economic growth was quite consistent, and EU states

[80] Lewis-Beck and Paldam 2000
[81] Lewis-Beck and Paldam 2000
[82] Michalowitz 2007
[83] OECD 2003, World Bank 2006

experienced similar linear patterns to that of U.S. firms.[84] In the 1990s, technology sector growth primarily came from manufacturing of computers and communications equipment, and software development.[85] Economic gains made by ICT investment and diffusion varied among EU states during Phase 2 (after late 1980s), and this growth lagged behind US performance. Despite the lag, EU states backed the potential by continued ICT investment through the 1990s-early 2000s using a combination of investments in technology infrastructure. Investments matched increased demands for telecommunications and internet services.[86] Between 1995-2000, share of ICT value added to the economy of OECD states averaged 9.5%, with some EU states seeing growth from ICT at 16.5%.[87] By 2011, growth had cooled somewhat to a European Union wide mean of 6.0%, but again, averages for some states persisted above 11%.[88] The substantial contribution by ICT firms to economic growth helped Member States to experience growth in technology-based industries while manufacturing in other sectors has declined. In addition, the demand for persons with ICT skills remained steady or increased slightly since the mid 1990s, even in the aftermath of the 2008 financial crisis. Eurostat reports cite that:

> "*More than two fifths (42 %) of large enterprises recruited or tried to recruit personnel for jobs requiring specialist ICT skills in 2016, while more than one fifth (22 %) of large enterprises reported that they had hard-to-fill vacancies for jobs requiring specialist ICT skills. By contrast, the corresponding shares for medium-sized enterprises were 17 % and 8 % respectively, and for small enterprises they were 6 % and 3 % respectively."- Eurostat*[89]

---

[84] van Ark et. al 2002
[85] OECD 2001
[86] Röller & Waverman 1996
[87] OECD 2002
[88] OECD 2018
[89] http://ec.europa.eu/eurostat/statistics-explained/index.php/Digital_economy_and_society_statistics_-_enterprises

2.3 Security Issues of the State Involving Data

In addition to the role that ICT dependence played in the national debate, the provision of national security has become a largely data-driven endeavor. Since the 1970s, states utilized data as a surveillance tool within their larger defense arsenal to reduce security risks from both individuals and state-level actors. Following the advent of the 9/11 attacks in the United States, countries worldwide realized the need for improving border patrol and security screening procedures over individuals entering and living within their territory.[90] Nowhere has this become more relevant that among member states of the European Union, where the U.K., Spain, and France have experienced a comparatively disproportionate numbers of deaths related to terrorism compared to other states in Europe, according to the Global Terrorism Database.[91] The increased numbers and visibility of attacks against the public can reduce trust and support for governments in power.[92] States have responded to public fears and the increased attacks with a variety of measures. These include more bilateral, collaborative border management, increased funding for law enforcement, and additional legislation designed to facilitate and widen surveillance of potential perpetrators of violent attacks.[93] This last measure is significantly reliant upon access to "Big Data",[94] sometimes generated by government, at other times co-opted or coerced out of private sector data brokers such as Google or mobile phone service providers.[95]

---

[90] Longo 2018
[91] Alcantara 2017 and Global Terrorism Database. Terrorism related deaths, 1970-2016: UK = 2519, Spain = 1141, and France (1972-2016) = 492.
[92] Chanley 2002
[93] Deibert 2013, Longo 2018.
[94] Big Data: "An approach to data analysis that aims to capture data comprehensively about a particular phenomenon, looking for patterns in the data." Mayer-Schönberger and Ramge, 2018, p. 77. Big Data is generated by data brokers or data profilers who correlate large quantities of seemingly unrelated data together in order to profile individuals based on larger patterns of behavior, online and offline.
[95] Deibert 2013, Longo 2018

Use of Big-Data for states' security purposes has significantly affected data use by governments. As noted by Matt Longo (2018), states now utilize public and private sector data for multiple security-related purposes, much of which is tied to counter-terrorism efforts after 9/11.[96] First and foremost, data can be used to assess the security risks associated with people or goods entering the state at airports or ports of entry. Border security personnel increasingly utilize biometric and biographic data profiles to improve accuracy and speed of processing human movement across borders. Lest one think this surveillance trend is solely for tracking non-citizens' activity, surveillance officers in many countries rely on face recognition software tied to CCTV camera feeds watching the mass public for the purposes of law enforcement.[97] Lastly, Big Data is a resource used for speeding up the movement of legal citizens re-entering the country, such as through the FAST Entry or TSA-Pre-check program in the United States, Registered Traveler in the U.K. for U.S. or Commonwealth citizens, or the Schengen Visa freedom of movement provided for EU citizens. All of these measures are used by states and state representatives to ensure that border flows are both safe and expeditious, all whilst simultaneously preserving state sovereignty and security. Though this may seem counterintuitive to the data privacy wishes of citizens in democracies such as the U.S. and Europe, research shows that perceptions of threat by terrorism may increase public willingness to forego civil liberties related to privacy. [98]Data researchers predict only increases in the application of Big Data collection, use, and brokering by states performing security-based activities.[99]

---

[96] Longo 2018
[97] Schneier 2015
[98] Huddy et. al 2002
[99] Deibert 2013, Flaherty 2010, Schneier 2015

In addition to the use of large-scale data to monitor people inside or entering their borders, states are increasingly reliant upon data and meta-data[100] to surveil other states, and a variety of non-state actors, such as politicians, diplomats, and high profile economic actors. With the diffusion of internet use and the propagation of data that occurs around its use, states see the cyber realm as another space in which to spread and exert power.[101] Thanks to the low barriers for entry, both big and small states can enter into this space and perform both defensive and offensive actions against other states or national interest targets.[102] Unfortunately, the very nature of internet infrastructure means that vulnerabilities in cyber-linked assets are often only exposed after an attack is perpetrated, giving offensive actors a seeming advantage over those seeking to deter cyber attacks.[103] Private data loss is a potential casualty during attacks which result in data breaches. Thousands of individuals have experienced data privacy losses during the data breaches associated with the Estonian government and banking industries in 2007, the US Office of Personal Management in 2015, and the German Reichstag attack in 2015.

Often the best way to accomplish cybersecurity is to use data for proactive surveillance of state and non-state targets seen as potential threats to the states. Covert surveillance can be accomplished without attrition of accountability by the states, especially when contracted actors perform the surveillance on behalf of the state, at least until the perpetrating state is caught and "shamed."[104] Even if the actors performing the surveillance espionage are publicly identified, the state actor behind the action will try to distance itself from the exposé. For example, U.S. embarrassment when caught spying on German Chancellor Angela Merkel's mobile phone

[100] Meta-data: "categories of data, about data" - Mayer-Schönberger and Ramge, 2018, p. 66.
[101] Rosecrance 2010
[102] Clark 2016, Rosecrance 2010
[103] Kello 2018
[104] Deibert 2013

conversations resulted in public efforts by U.S. officials to throw the focus on Edward Snowden, framed as an individual who acted in opposition to his own state.[105]

Currently, states primarily use digital surveillance with data as a tool of espionage, less so than as an offensive weapon. Unwilling to react in kind to cyber attacks with cyber retaliation, or by use of conventional weaponry, states result to living in a condition of "unpeace" with each other, broken by occasional outbreaks of open attacks if the target is seen to be vulnerable, or cyber-attacking another states if it is economically useful to the aggressor state or its interests.[106] China in particular has been known to practice significant amounts of economic espionage to acquire intellectual property advantages for state-backed industries.[107]

Due to the nature of increased cyber vulnerability, the public and state concern over terrorism, and the desire of states to protect vital civilian and military assets, I propose that that conventional security threats, cyber threats, or the perception of risks of such threats now drives states toward seeing data as a security tool. As a result, legislation or institutional creation can occur around giving law enforcement, criminal investigative, and security officials easy access to data. States justify the loss of privacy or data control as being tied to the greater good, protecting national interests such as crucial infrastructure, and as part of the state's overall sovereignty and security mandate. Given the increased number of attacks by terrorists and extremist groups in European states, I propose that data access is now being framed as a useful mechanism for state security provision, providing another example of a how a domestic institution was created around the issue of data.[108]

---

[105] Johnson et. al 2014
[106] Kello 2018
[107] Lee 2013, Skinner 2014
[108] Lynn 2010

2.4 Data as a Privacy Concern, i.e. Digital Human Rights

The final structural variable that shapes EU states' national data policies is that of the key legal and human rights advocates who encourage rights-based data protections. According to the ideational literature, members of civil society play a large role in getting states to adopt particular human rights policies. Civil society includes, but is not limited to "… human rights organizations, religious groups, political parties, and student organizations…".[109] This scholarship has shown that human rights policies can be adopted as a result of both internal and external pressures, in a 'two-level' spatial environment.[110] Depending on the issue being debated, researchers have looked at both levels to explain how policy success occurs. Thomas Risse-Kappen (1995) outlined the necessity of researching domestic and international actors and structures, as it is neither all state nor all society that fully explains human rights movements. As data policy emerged at the domestic level first in Europe, I argue that the causal pathway begins at the national level.

Policy change cannot happen without an opening in the legislative agenda, thus making it conditional upon a window of political opportunity being opened in the agenda space of legislators.[111] Reimann (2006) found that advocacy is more successful when new openness meets advocacy action.[112] Tsutsui and Wotipka (2004) agree with Reimann; during the early stages of advocacy around an issue, domestic political opportunities are especially crucial to increase numbers of citizens participating in a cause.[113] We know several key facts about how non-state actors can push for new openings regarding human rights policies. Activists rely upon measures

[109] Cardenas 2004, p. 215.
[110] Cardenas 2004
[111] Tarrow 1998
[112] Reimann 2006
[113] Tsutsui and Wotipka 2004

such as information politics, leverage-building campaigns with high-profile actors, or rationalist arguments to pressure governments to develop human rights policies. Domestic activists will also resort to linking with outside networks if the state is resistant to outside change.[114]

Placing the pattern of behavior for activism regarding human rights within the context of data policy, there is emerging scholarship to show that civil society has embraced activism related to technology and its impact to individuals' rights. Recent interviews of multiple ICT (information, communications, and technology) activists in Europe revealed that privacy and data protection were high among missions undertaken by various groups and individuals in activism. For instance, Irish activists worked to monopolize newspaper headlines in order to increase public support and pressure governments into policy protections for data (this in response to the growing use of data as a commodity by telecommunications firms).[115] Other activists have utilized traditional social movement mechanisms, such as protests.[116] In the late 1990s and early 2000s, still other groups brought court cases against states or the private sector, with the goal of pushing policy-makers into acknowledging data rights within the realm of fundamental human rights. Lastly, Löblich and Wendelin (2011) have shown that ICT policy activism has created coalitions of multiple stakeholders, including individuals from industry alongside civil society actors.[117] This "networking" of rights-motivated activists (human rights insiders) and private sector industry representatives (outsiders) concerned with the impact of technology use upon human rights aligns with past networking of other human rights groups, such as those opposing land mine use, or weapons bans.[118]

---

[114] Benford and Snow 2000
[115] McIntyre 2008
[116] Kolb 2005
[117] Löblich and Wendelin 2011
[118] Finnemore and Sikkink 1998, "International Norm Dynamics and Political Change"; Sikkink 2005; Hintz and Milan 2009

On additional factor exists that may elevate issue activism to be taken seriously by government policy-makers: involvement by epistemic experts. An epistemic community is "a network of professionals with recognized expertise and competence in a particular domain and an authoritative claim to policy-relevant knowledge within that domain or issue area."[119] Epistemic experts provide professional, substantive expertise for governments who seek specialized expertise in an environment of imperfect information. This is particularly true during policymaking for laws that intersect new technology and legal rights, as most politicians do not come from technology-based fields prior to serving in government. Haas (1992) pointed out that epistemic experts share normative beliefs along with technical knowledge. Several scholars found that the normative preferences on policy shared amongst members of the professional community can diffuse throughout the international system, as these individuals consult with multiple governments and international organizations.[120]

In their landmark work on transnational advocacy networks, Keck and Sikkink (1998) described networks of liked-minded individuals from NGOs, social movements, foundations, media, trade unions, IGOs, or even sections of government.[121] These individuals create influence by designing issue agendas, helping to set institutional procedures, and ultimately, influencing state behavior, through the crucial elements of "issue resonance, network density, and target vulnerability."[122] I propose that legal and human rights professionals in the European Union created linkages between government policymakers, the legal rights community, and ultimately, the oversight bodies of data protection at the national and EU level. They used the consulting space they were given as a platform to frame and promote fundamental human rights for

[119] Haas 1992
[120] Keck 1993; Keck and Sikkink 1998; Meyer, Boli et al 1997.
[121] Keck and Sikkink 1998
[122] Keck and Sikkink 1998, p. 26.

personal and cyber data. As Haas stated, "To the extent to which an epistemic community consolidates bureaucratic power within national administrations and international secretariats, it stands to institutionalize its influence and insinuate its views into broader international politics."[123]

To summarize this section, regime/institutionalist theory applied to EU Member States will show domestic institutions being created to protect and preserve policy that matters to particular interest groups. There are three key groups to whom policy on data treatment is crucial. Government security ministries, law enforcement, and criminal prosecutors see data as a tool for protecting state sovereignty and national security. The ICT sector identifies data as a powerful economic commodity and would like to keep control over how data is collected, processed, stored, and moved. Lastly, legal professionals and human rights advocates increasingly identify data use and abuse as a component of fundamental human rights and will use their consultative power to promote digital human rights. Given the three main interests which are focused on data as a policy concern, I expect to see the following in my national cases:

> *In EU states with large-scale economic dependence on ICT firms, states will pass economic commodification polices **(i.e., national institutional regime)** protecting the use of personal and/or cyber data for profit.*
>
> *In EU states with a history of numerous domestic terrorist attacks, the state will promote securitized policies for cyber data **(i.e. a national institutional regime),** resulting in state and law-enforcement gaining access to the databanks of both public and private sectors.*
>
> *In EU states where legal experts or academics based in human rights disciplines are used as legislative consultants during the law-making process, these states will extend human rights protections over data legislation **(i.e., a national digital human rights regime).***

[123] Haas 1992, p. 4.

Now that I've explained the national characteristics that lead to policy-making around data, I turn to EU-level policymaking.

2.5 International Regimes and Regime Complexity: Putting Pressure on States from Outside

The prior section established the main domestic interests that should shape national data laws. I now turn to examine the regional or EU-level causal pathway for data legislation. Recall that my theoretical argument states that **data protection policies in the EU occur along two-levels, national and regional (EU), in a complex regime environment.** I have two expectations for this time period and level of policymaking.

> *At the EU-level, powerful states will attempt to influence EU policy to align with their own national preferences.*[124]
>
> *The presence of strategically placed legal and human rights experts will lead to expanded human rights protections over data, creating a digital human rights regime.*[125]

In the 1980s, some IGOs began to push their member states to adopt policies to converge upon a specific type of data management policy - primarily that of data commodification. These recommendations aligned with the domestic interests of some EU states, making policy adoption simple. As pressure from these IGOs grew and diffused throughout the international system, the European Union Commission added data governance to the list of issues it wanted to decide according to an intergovernmental fashion. Coordinating data policy could facilitate ongoing economic integration and peace in the Union. During the EU policy formation process, key EU member pushed against some Community policy recommendations in the 1990s and 2000s. Despite the conflict, today, EU policy has generated a "digital bill of human rights."

---

[124] This is based upon Hegemonic Stability Theory, explanation in the subsequent paragraphs.
[125] This follows the logic of the epistemic networking established by Haas, Keck, Sikkink, and others.

To explain how EU policy reached this convergence point, I now discuss the international regimes and policy mandates that have led to these outcomes. The relevance of how EU states' coordinated efforts to make a Union-wide digital human rights policy has implications for EU-policymaking on other issues, and could inform scholarly debate in other regions of the world that work to coordinate policy on shared issue agendas. In short, to understand the end policies such as Directive 95/46/EC and the GDPR, I build upon past IR scholarship regarding regime creation and function. I utilize the conceptualization provided by Stephen Krasner, who defined regimes as, "principles, norms, rules, and decision-making procedures around which actor expectations converge in a given issue-area."[126] Each of the main IR theories of realism, liberal institutionalism, and constructivism contribute to my argument.

2.6 Realism, Liberal Institutionalism, and Constructivism: Three Approaches to International Regimes

At the systemic level, Keohane and Nye (1989) predicted that as utility of force declined, and economic interdependence grew during the 20th century, states would find greater advantage in participating in international regimes which would give them more control over shared issues.[127] Despite the fact that international regime creation has exploded since WWII, international relations theories attribute different reasons for the creation and maintenance of regimes. Each of the main IR paradigms explains an aspect of regime structure and functioning that underpins this dissertation. Realist regime theory explains the role of "hegemonic" or powerful states[128] in creating regimes, which I apply to some members of the EU. Liberal

[126] Krasner 1983. Note: within this dissertation, I use the terms regime, institution, and organisation to indicate the presence of organised rules for a shared issue area.
[127] Keohane & Nye, 1989
[128] I use Robert Keohane's definition of a hegemonic state, where "one state is powerful enough to maintain the essential rules governing interstate relations, and willing to do so." (Keohane 1984, 2005, p. 35)

institutional theory explains how and why a hegemon is not necessary for regime stability or continuity, helping to show why EU states have continued to follow data policies set out years ago. Constructivism clarifies the contribution made by social factors such elite networks, by allowing regimes to be adaptive and receptive to the influence of epistemic experts working with the Commission. I now examine each theory for its contribution to the digital human rights regime.

2.7 Realism

At the heart of realist theory, there is no expectation that states would desire to create a regime at all, given that it will likely impinge on the most sacred norm of states: sovereignty. Realist scholars overcome this constraint by utilizing systemic structure and states' goals to explain the propensity of states to create regimes.[129] Krasner (1983) noted that self-interested states will allow spontaneous regime creation, will negotiate regime creation via agreements, or will impose regimes upon less powerful states when it is their interest to do so. Realists also expect that most regime initiation will be done by the predominantly powerful, or "hegemonic" states.[130] After all, these states have more resources to provide the public goods needed by the community and have the capability to punish free-riders.[131] As a trade-off for providing some public goods to all states within the regime, the hegemon expects to control the issue agenda.[132]

Several things challenge the rigidity of regimes. Internal contradictions can become apparent over time during application of the regime rules, or power shifts can occur within the international system that alter who fills the hegemonic space. Pure realism cannot explain why

[129] *International Regimes*, 1983, Chapter 1: "Structural Causes and Regime Consequences: Regimes as Intervening Variables", by Stephen Krasner.
[130] Keohane and Nye 1989
[131] Nye 2014; Gilpin 1987, p. 100
[132] Keohane and Nye 1989

regimes persist, if the original purpose no longer exists, or if the hegemonic state which first created the regime begins to decline. Hegemonic Stability Theory proposes that when the hegemon declines, the regime it created and maintained should decay.[133] Scholars such as Ruggie (1982) counter this claim. [134] To Ruggie, if other states continue to benefit from the framework of the regime, then regime instruments will be reshaped to adapt to shocks to the regime such as loss of the regime leader, but the regime may not die altogether. Realism expects hegemons to create a regime in order to control an agenda and achieve a goal. Reaching the goal is possible because less-powerful states will join the regime to free-ride in the provision of public goods of some kind, or to avoid sanctions by hegemonic states who get to control the issue agenda.

2.8 Liberal Institutionalism

Omission within the realist argument can be addressed using the ideational framework of liberal institutionalism, and by applying this to the formation of data protection in the EU. First, realism assumes that shared states' interests provide the motivation for states to forego forego sovereignty in particular areas. [135] A liberal institutional counter argument was made by Keohane (1984), who noted that regimes can be self-perpetuating, given the rules that lock states into ongoing participation. These rules can persist long after the original conditions ted have changed, ensuring regime longevity long after the initial utility function has decayed. When we understand the nature of regimes to be long-term, membership in the regime signals a credible commitments and long-term accountability to other states during multiple iterations of interaction around the issue. In addition to improving accountability, regimes reduce transaction costs, increase

[133] Keohane 1984/2005
[134] Ruggie 1982
[135] Keohane 1984/2005

economies of scale, and increase goods provisions. Finally, international regimes give voice to small and mid-sized states; they will work to preserve regimes as a leveling agent over shared issue arenas.[136] The data regimes created by the OECD and Council of Europe, and later by the European Union exemplify Keohane's proposed long-standing regimes. EU Member States that have joined these organizations have made commitments to various regimes built into the mission of the IGOs.

Returning to the power state argument, regime membership binds member states to the preferences of the states which achieved agenda control for the regime.[137] Early regime literature examined security regimes but expanded in the 1980s to include economic regimes.[138] Since the focus of this paper is not on security-based regimes, I will forego discussing the security literature. Economically-speaking, national governments want to take successful domestic economic policies and scale them up to the international level if seen as beneficial to the national economy.[139] However, regimes that were created on the basis of one shared concern can experience "mission creep" as members add new dimensions to the original institutional agenda. European Union competences present an instance of mission creep. What began with the goal of economic integration in the European Steel and Coal Community of 1951, led to exponential policy spread into multiple issue pillars involving economic, security, and justice affairs by the Maastricht Treaty of 1992.[140] Today, the EU *aquis communitaire* has incorporated all types of issues into the scope of governance under EU control, including trade, financial systems

[136] Chapter 5, "The Governance Problem in International Relations" by Peter Alexis Gourevitch, in *Strategic Choice and International Relations***,** edited by David A. Lake and Robert Powell, 1999.
[137] Keohane 1984/2005
[138] Jervis 1982; Keohane 1984; Keohane and Nye 1989; Krasner 1983.
[139] Moravscik 1998
[140] Bache et al, 2015

regulation, genetically-modified agriculture restrictions, climate change policies, intellectual property protections, and of interest to this dissertation, internet and data policies.[141]

Liberal institutionalism adds the element of domestic economic concerns to the variety explanations for why states create, join, and cooperate with international regimes, including those that include data governance. Yet this paradigm lacks an explanation for how states determine which interests should be carried into the international space. Wendt (1992) points out that both realist and institutionalist arguments rely upon the presence of social threats, but neither approach explains how social threats emerge or change.[142] Both realism and liberal institutionalism simply assume that diverse threats exist, secondary to the primary interest of protecting state sovereignty. Wendt proposes that the main motive of states – protecting sovereignty – is actually a socially constructed and accepted norm, implying that the development of interests is a learned process, constantly evolving across time, and impacted by an interactive process with the domestic environment.[143] The constructive approach provides the final missing piece to explain the emergence of a data protection regime in the EU.

2.9 Constructivism

Constructivists contend that the structure of the international system is interactive. Social actors build the structure of states that constrains their own Behaviour, which then leads to international constraints upon Behaviour.[144] These constraints can be institutional organizations, or regimes. Identifying the intersubjective nature of the international order and by implication the intersubjectivity of regimes gives scholars the ability to explain that regimes are based in the

[141] Drezner 2007
[142] Wendt 1992
[143] Wendt 1992
[144] Ruggie 1998

identity of states, and that this identity often has normative factors. Crucially, constructivism points out that individuals, including professional or epistemic actors, contribute to the evolution of domestic norms that can then be diffused throughout the international system.[145] By allowing for cross-interactions between the domestic and international spheres, the constructive approach acknowledges that identities and interests are constantly being reassessed for value and for instrumentality.[146]

Constructivism also provides explanation on how sociopolitical factors impact regime adaptation across time.[147] Frieden (1999) suggests looking at domestic actors' features in the context of the political environment when trying to understand national preferences, which in turn shape strategies the state will pursue when negotiating internationally.[148] The preferences of domestic actors, particularly elites and firms, in addition to the aggregate population will influence a state's foreign policy .[149] Without the contribution of constructivism, the role played by non-state actors in determining policy changes in the EU would be completely overlooked. Constructivism thus provides important tools to explain the transformation of data regimes across time and space, making a necessary contribution to this dissertation when explaining the emergence of these regimes.

To reiterate: regime theory explains the framework for developing institutions to coordinate policy in shared issue areas, which could include personal and cyber data governance. Realist regime theory attributes the origination of regimes to hegemonic, or powerful states,

---

[145] Haas 1992, Keck and Sikkink 1998
[146] Wendt 1992
[147] Moravcsik 1997; Wendt 1992
[148] Chapter 2, "Actors' Preferences in International Relations," in *Strategic Choice and International Relations*, edited by David A. Lake and Robert Powell, 1999
[149] Chapter 2, "Actors and Preferences in International Relations", by Jeffry A. Frieden, in *Strategic Choice and International Relations*, edited by David A. Lake and Robert Powell, 1999.

seeking to internationalize their domestic goals and interests. Liberal institutionalism explains regime continuity and the credible commitments that bind states to ongoing compliance even after hegemonic decline. Constructivism fills in the gaps of the other two approaches, by explaining that the *a priori* power of domestic norms and the international activities of norm-entrepreneurs can diffuse these values via international networks, as they act to advice and shape policymaking within IGOs. Together, these international relations paradigms explain why and EU regime for digital human rights could emerge and persist. I now apply regime theory to EU data governance.

2.10 The Context of Regimes Applied to Data Policy in the European Union

International regimes have huge potential to impact the policies and preferences of governments of EU states seeking to insure a particular outcome around important issues. When states create (or join) international regimes, the goal is to design formal institutions and organizations to set constraints and expectations around states' behavior on a particular issue or set of issues. Examples of formal international regimes joined by EU Member States include the United Nations (UN), the World Trade Organization (WTO), and the North Atlantic Treaty Organization (NATO). Without regimes, states suffer from the coordination problems: conflicting interests, incomplete information, and a lack of overarching enforcement bodies.[150] The presence of regimes to govern a particular issue area should promote less friction and provide more certainty for states regarding how other states are going to act around an issue. Because regimes are expensive (involving foregone areas of freedom or cost to certain actors) states must determine if the reward for creating regimes or participating in regimes is more

[150] North 1990

valuable than the price paid.[151] In addition to passing laws and creating domestic agencies to address data treatment at the national level, EU Member States are willing members of multiple international regimes, as seen in Table 1.

Table 1: EU Member States' International Regime Membership

Country	European Union	OECD	Council of Europe	United Nations	NATO
Austria	1995	1961	1956	1955	*
Belgium	1958	1961	1949	1945	1949
Bulgaria	2007	*	1992	1955	2004
Croatia	2013	*	1996		2009
Republic of Cyprus	2004	*	1961	1960	*
Czech Republic	2004	1995	1993	1993	1999
Denmark	1973	1961	1949	1945	1949
Estonia	2004	2010	1993	1991	2004
Finland	1995	1969	1989	1955	*
France	1958	1961	1949	1945	1949
Germany	1958	1961	1950	1973	1955
Greece	1981	1961	1949	1945	1952
Hungary	2004	1996	1990	1955	1999
Ireland	1973	1961	1949	1955	*
Italy	1958	1962	1949	1955	1949
Latvia	2004	2016	1995	1991	2004
Lithuania	2004	*	1993	1991	2004
Luxembourg	1958	1961	1949	1945	1949
Malta	2004	*	1965	1964	*
Netherlands	1958	1961	1949	1945	194
Poland	2004	1996	1991	1945	1999
Portugal	1986	1961	1976	1955	1949
Romania	2007	*	1993	1955	2004
Slovak Republic	2004	2000	1993	1993	2004
Slovenia	2004	2010	1993	1992	2004
Spain	1986	1961	1977	1955	1982
Sweden	1995	1961	1949	1946	*
United Kingdom	1973	1961	1949	1945	1949

[151] Abbott & Snidal, 1998; Keohane 2005.

2.11 Regime complexity – The General Environmental Context

Regimes can have overlapping, and sometimes competing goal; the presence of multiple, overlapping regimes or in produces a "regime complex." Regime complexes involve, "a network of three or more international regimes that relate to a common subject matter; exhibit overlapping membership, and generate substantive, normative, or operative interactions recognized as potentially problematic whether or not they are managed effectively."[152] Alter and Meunier (2009) rightfully state that regime complexes can be parallel (having no formal overlap), overlapping (multiple institutions exist that each have authority over an issue), or nested (competence over issues located in concentric circles of regimes).[153] In other words, new institutions can mirror the functions of old ones, or new and old institutions can cover the same issue area but conflict in behavioral requirements, or new and old institutions can overlap in certain aspects of an issue. I argue in this dissertation that data governance in the EU occupies a space of regime complexity.

EU states have created domestic regimes for data governance (national laws) and they are members of multiple international organizations that also have data policy recommendations. As seen in Table 1, EU member states are members of the European Union, the Organization for Economic Cooperation and Development (OECD), the Council of Europe (CoE), the North Atlantic Treaty Organization (NATO), and the United Nations (UN). All of these regimes have suggested policies associated with personal and cyber data governance. The most significant data regimes regimes include Convention 108 of the Council of Europe, ETS 185/the Budapest Convention on Cybercrime of the Council of Europe, Article 8 of the European Convention of Human Rights, and the OECD Guidelines on the Protection of Privacy and Transborder Flows of

[152] Orsini, Morin, Young, 1981, p. 6
[153] Alter and Meunier 2009

Personal Data.[154] As members of the Council of Europe and OECD, EU states are held to voluntary compliance regarding these mandates. National legislation is expected to reflect the norms and practices agreed upon by the consensus within the community of states that have joined these organizations. This can be problematic for states.

When the policy recommendations made by IGOs do not agree with each other, or do not agree with domestic laws, states that are members of multiple organizations face competing policy demands. The policy recommendations of the Council of Europe, OECD, and UN are voluntary, however those of the European Union, if violated, could endanger membership in the Union itself. Multiple domestic data laws have been in place since the 1970s. From the 1980s, multiple IGOs promoted data law convergence toward protections during automatic processing and transborder data movement. A data regime complex can be said to have emerged due to the "overlapping institutions from both an issue-area, and a regional perspective."[155] Literature in the last ten years has acknowledged the regime of internet governance, but has not discussed the ways that this and other regimes overlap to affect cyber data governance in particular.[156] Figure 1 offers a visual representation of this overlap in interests which compete for policy influence for EU states making data policies. (See Figure 1, next page).

[154] Council of Europe 2001, Fuster 2016, Mayer-Schönberger 2015
[155] Aggarwal 2005, p. 4
[156] Drezner 2007, Franda, 2001, Nye 2014.

Figure 1: Data Regime Complex

2.12 International Level Policy Coordination – Setting EU Data Policy

In this section, I address the critical components for policy coordination in the EU, particularly when a new issue is added to the policy agenda. There are two primary steps involved during EU policy evolution: opening an opportunity for policy introduction, and the cooperation and compromise necessary to decide what policy will be adopted Union-wide. Thus, the work in this dissertation that traces the evolution of policy introduction and coordination for data policy has wider applications for policy scholarship across many issue areas, both inside and outside the European Union.

2.13 New EU Policy Agenda Power: The Commission

I propose that a new issue will be added to the policy agenda at the EU level when a tipping point of interest is reached among two or more hegemonic states regarding an issue deemed of shared importance.[157] This is a novel and innovate idea being introduced to the

[157] Scholars disagree as to whether policy-making takes place motivated by neofunctionalist integration efforts, due to the intergovernmental designs by national governments, or as a part of "new

understanding of EU policy-making. The legislative structure of the European Union requires that new policy be initiated by the European Commission or the European Parliament (although the Parliament can only initiate a call for action if it feels the Commission has neglected to respond to suggestions by the Parliament).[158] Parliament's ability to suggest new legislation is a more recent addition to the legislative process, added with the 1992 Treaty of the European Union/Maastricht.[159] In reality, Parliament uses its increased "co-decision" power to pass/veto new legislation; the power to initiate legislation still stands with the Commission.[160] Therefore, the crucial and necessary element for an issue to be considered for community-wide governance is that it is introduced by the Commission. Furthermore, this introduction is conditional upon interest being taken by whichever state serves as the presidency of the EU Commission, who chooses to place the topic onto the issue agenda during its term as president of the Commission. Once the Commission adds an issue to the agenda, it will ask the Council of Ministers to research the topic and consider the need for community-wide governance. The Council could issue a recommendation (not legally-binding for Member States), suggest a Directive, or work with the EU Parliament to pass a Regulation, the latter of which requires states to implement the policy into national law. Thus, the Council can act as a filter for new policy opportunities within the Union, as it decides whether to move forward with the Commission's request.[161]

Unlike past scholars, I am not arguing that the Commission possesses sole power over initiating policy for the larger Union. I do suggest that the Commission can at times serve the role of principal to initiate legislation on behalf of the agents (states). At other times, the

---

institutionalism" which combines rational interests with constructivism's emphasis on path-dependent constructs. Pollack 2010.

[158] Garrett and Tsebelis 1996, Nugent 2002

[159] http://www.europarl.europa.eu/about-parliament/en/powers-and-procedures/legislative-powers

[160] Wallace, Pollack and Young 2015

[161] Kassim et. al 2001

Commission will act as agent for the Council during the policy-making process, by facilitating the will of the Council (agent).[162] In the former scenario (principal role), the Commission serves as an initiator for opening political opportunities for policy-making in the Union. Research has shown that the Commission designs the wording of policy to match what it believes will elicit the most support from Member States.[163]

When the Commission issues a new proposal, it has opened a new political opportunity for those on the Council and in Parliament.[164] In other words, the call for a new Directive or Regulations opens the door for new influence to be exerted by national representatives on issues of importance to their state, i.e. creating political opportunities that did not heretofore exist. After a new law is suggested by the Commission, national representatives serving in the Council and any advisory committees walk into the new opportunity determined to shape EU legislation in the direction of their state's interests. While Council or even Parliamentary members may have wished to alter EU-level policy on that particular issue in the past, their ability to do so was limited until the Commission opened the door by making a new proposal. Those serving in the Commission therefore have a significant level of agenda power by controlling the opening (or not) for new policy.

Members of the issue-relevant Council of Ministers also hold a significant level of power, as the Council researches and plans the particulars of the proposed regulation. EU Council members and those serving on Commission and/or Council research committees are charged with the responsibility of research, giving these entities the power over information given to the Commission, the Council, and Parliament. Information can reduce or erect barriers to

---

[162] Nugent 2002; Nugent discusses the wider debate between other scholars as to the role of the EU Commission. See Nugent's reference to works by Sandholtz 1993, Fuchs 1995, and Mazy 1995.
[163] Kassim et. al 2001
[164] Tarrow 1994

institutional agreement, or regime creation.[165] Researchers shape new legislation via information seeking and provision, and via the policies suggested to the Commission, Council, and Parliament. Epistemic experts on these bodies may have considerable latitude as policy-shapers to incorporate normative elements into new policies, such as identifying data as a privacy concern, and therefore within the fundamental human rights protections of Union law. In this way, research committees can influence the outcome of new norms that may have been unleashed by new policy opportunity opened by domestically interested representatives serving on the Commission when it delivered a proposal.[166]

Since the Commission and the Council of Ministers members hold the highest amount of agenda-power during the initial stages of policy creation, they can act as crucial "nodes" or gatekeepers who control the policy-making process at the supranational level, potentially working to ensure that their states' preferences are preserved in EU law.[167] Thus, while the Commission opens the door, the causal map that began at the national level (during Phase 1) continues to the EU-level (Phase 2) during which the Commission and any advisory bodies present their suggestions for EU law. Given these powers, I expect:

> *The EU Commission president will act as the primary actor opening doors for new data legislation policy for the EU Community.*

2.14 The Power of Hegemonic States

My next argument concerns *which particular* member states ultimately hold the greatest chance of success in seeing their preferences emerge within the final EU policy.

---

[165] North 1990
[166] Finnemore and Sikkink 1998
[167] Hafner-Burton, Kahler, and Montgomery 2009.

To insure their preferences are prioritized, powerful states may serve as norm entrepreneurs during the policy-shaping phase of the legislative process, pushing other states toward the "rightness of their views."[168] For example, the U.S. as the primary hegemon of the post-Cold War era was disproportionately influential in matters of setting global internet policies on the maintenance of internet infrastructure, largely due first mover advantages in developing the internet technology. The U.S. also worked to achieve data commodification protection for mobile data within the OECD data privacy recommendations, to the benefit of U.S. multinational data brokers.[169] Whether powerful states and their representatives hold disproportionate power over personal cyber data governance in the European Union is a point on which the literature remains less established, but one that I intend to address.

In the past, the policy wishes of great power states in the EU such as Germany or the UK have often been successful in becoming Community-wide law. In his work on EU policy coordination, Hussein Kassim (2001) points out that there are two views by scholars on how policy cooperation is likely to occur.[170] The "convergence" approach, combines rational theory with sociological ideas to expect convergence based on efficiency and shared values. The "continuing divergency" approach contends that strategic, issue specific legislating is more likely as states will fight for protections over domestic policy idiosyncrasies. While Hussein proposes that in reality a bit of both occurs, to Hussein the importance of state governance style, interests, and state structures is significant. For instance, federal-style Germany was a "locomotive" when promoting European integration, following the two world wars. In "brake states" like the United Kingdom, there is a propensity to oppose any policy that encroaches on intergovernmentalism.

---

[168] Florini 1996
[169] Bennett 1992, Fuster 2016, Powers and Jablonski 2015
[170] Kassim, Co-ordinating Action in Brussels 2001.

The U.K. prefers mandates that allow equal amounts of national controls, or at least the ability of each state to insert exclusionary clauses into the EU legislation. More "passive" states only get involved when the legislation is of keen interest to them

I return to the debate on how states are able to diffuse domestic policy into the international system. Two key works of literature have shown that it is the interaction between domestic and international interests that can alter states' participation in international agreements.[171] In his classic "Diplomacy and domestic politics: the logic of two-level games" Robert Putnam (1988) proposed that national governments will work during diplomatic negotiations to preserve domestic interests, whilst simultaneously trying to avoid international losses. [172] The larger the "win-set" or the wider the number of domestic actors who are satisfied with an internationally-proposed policy, the greater likelihood that the diplomat can agree to terms dictated by her diplomatic colleagues, or by a membership organization.[173] Milner (1997) concurred, in that international cooperation will be filtered through the policy preferences of domestic actors.[174] This speaks directly to the expected behavior of powerful states in the EU during data policymaking. I suggest that France, Germany, and the U.K. meet the criteria for more powerful states of the EU, given their population sizes, military power, capital access, and market sizes. This model predicts that when they hold the Commission presidency, they will seek data policies that benefit their own domestic interests. In my final hypothesis, I summarily propose the following due to the power held by hegemonic states, and their ability to control "carrots" and "sticks":

> *As a result of their hegemonic power, the domestic preferences of powerful EU states will more likely be the convergence point for EU data policy.*

[171] Milner 1997, p. 40-45.
[172] Putnam 1988
[173] Putnam 1988, p. 435-450.
[174] Milner 1997, p. 9-15.

2.15 Epistemic Advocacy Power

Lastly, similar to the argument made for national data laws, the EU Commission routinely relies upon epistemic professionals to provide expertise on technical and legal matters. As Pollack (1997) pointed out, the informal agenda setting power built into many EU institutions allows considerable power to those not formally appointed directly by the Member States, nor by directly elected by EU citizens.[175] In other words, the process of policymaking in the European Union has built in informal power for those without direct ties to governments in so far as they were not elected into office or perhaps do not serve as permanent appointees. I propose that epistemic professionals (agents) that give advice during the policy consideration phase can leverage their professional knowledge and the normative consensus of their network to promote a particular policy agenda to the principle actor (the EU Commission, Council of Ministers, or Parliament). Building on the work of Kingdon (1984), Pollack also argued that successful policy entrepreneurs exhibit three crucial characteristics. The person must be seen as an expert, be known for network connections, and be persistent in waiting or a new policy window to open.[176] Members of epistemic networks possess all of these attributes.[177]

Therefore, my last expectation is that:

> *Legal and human rights experts serving in advisory capacity to the EU institutions will advocate for fundamental human rights protections for personal and/or cyber date in the EU, creating an EU digital human rights regime.*

In the next section of this dissertation, I explain the methodology used to test these arguments.

---

[175] Pollack 1997
[176] Kingdom 1984
[177] Haas 1992; Keck and Sikkink 1998.

3 RESEARCH DESIGN AND METHODOLOGY

This dissertation utilizes a variety of methods to test the theoretical argument introduced in Chapter 2. For reasons I outline below, the primary testing was done with qualitative methods. To explain the creation of national data laws during Phase 1, I used case studies combined with historical process-tracing to map the evolution of national data regimes in a sample of EU Member States. Descriptive statistics support the structural arguments made at the national level for the three independent variables (economic commodification of data, domestic security incidents, the presence of legal rights experts during the national legislative process). The types of data laws to emerge at the national and EU level serve as the dependent variable at both levels. All laws are manually coded with an original coding scheme and extensive content analysis explained below. During Phase 2, I created a new composite measure to predict the preferences for data commodification sought by the most powerful states of France, Germany, and the UK at the EU level. The data used to predict the states' preferences for the other two structural variables (security incidents, role of legal experts) remain the same as at the national level.

The logic of combining case studies and process-tracing in Phase 1 follows the methodology suggested by Bennett and Checkel (2015), George and Bennett (2005), and Herb (2017).[178] Bennett and Checkel (2015) argue that process-tracing allows researchers to perform deductive testing upon hypothesized relationships between causal mechanisms. Links can be uncovered between the independent variable(s) and the outcome of interest during the causal

[178] Bennett and Checkel 2015, George and Bennett 2005, Herb 2017.

process, based upon the inferences made about the causality.[179] George and Bennett (2015) propose that,

> *"The method and logic of structured, focused comparison is simple and straightforward. The method is 'structured' in that the researcher writes general questions that reflect the research objective and that these questions are asked of each case under study to guide and standardize data collection, thereby making systematic comparison and cumulation of the findings of the cases possible. The method is 'focused' in that it deals only with certain aspects of the historical cases examined."- p. 11*

When process-tracing of individual cases is combined with case comparisons, this creates a powerful, synergistic tool for comparative historical analysis.[180] Past comparative literature incorporating this combination of methods includes Skocpol's *States and Social Revolutions* (1994) and Wood's *Forging Democracy from Below* (2007).[181]

3.1 Case Selection

I have chosen to test the national level of data policy development in the countries of Germany, the United Kingdom, and Sweden. While case studies of all EU Member States' data policies would expand data governance scholarship, time will not permit studies on all the EU states during this dissertation. My cases reflect both a "most similar" and "least similar" selection approach. All case states are developed economies with democratic regimes, as well as being EU, OECD, Council of Europe, and UN Member States (i.e., an overlap of regime memberships). Similarity in organizational membership allows for the regime complexity argument to be controlled in the respect that the IGO memberships are all the same. Economic indicators reflect additional similarities; each of these countries have high levels of international

[179] Bennett and Checkel 2015, p. 11; George and Bennett 2015, p. 214.
[180] Prof. Michael Herb seminar, 3 April 2017.
[181] Skocpol 1994, Wood 2007

trade in GDP (Germany 46%, UK 30%, Sweden 44%), and high average incomes in GDP per capita (Germany $42, 161, UK $40,412, Sweden $51,844, all in USD).[182]

Dissimilarities include population sizes (Germany 82.5 million, the UK 65.6 million, Sweden 9.9 million)[183], dates of accession to the EU (West Germany 1958, UK 1973, Sweden 1995)[184], and participation in the Eurozone (Germany participates, the UK and Sweden do not). A final dissimilarity is location: Germany is in central Europe, the UK in western Europe (non-continental), and Sweden is in northern Europe. Dissimilar factors allowed me to rigorously test the argument that policy convergence should occur across multiple states (recall that the 1980s literature expected technology policy convergence among democracies). Finally, the independent variables of epistemic expert involvement (highly prominent in Germany and Sweden), economic dependence on ICT firms (lower in Germany and Sweden), and frequent security/terrorist attacks (highest in UK) show variance in the independent variables as recommended by King, Keohane, and Verba (2012) during qualitative social science research.[185]

3.2 Time

Data times measure from 1970-2015/2016 dependent upon data availability. I began in 1970 as this was the approximate time point during which state agencies and private sector firms began to utilize computerized data management and storage. By the 1990s, internet use was diffused throughout government offices and academic research facilities, and internet use began to spread to public and business sectors. National policies matched this pattern diffusion, with national data laws enacted early in the 1970s in some European states. When computer

[182] https://data.oecd.org/trade/trade-in-goods-and-services.htm
[183] World Bank World Development Indicators, Population 2016 figures.
[184] European Parliament website: http://www.europarl.europa.eu/external/html/euenlargement/default_en.htm
[185] King, Keohane, and Verba 2012

networking expanded internet use and data transmission, states incorporated cyber data policies into their larger data legislation from the 1990s forward.

3.3 Predicted Outcomes: National Laws on Data Governance (1970-1999)

Recall my expectations at the national level:

> *In EU states with large-scale economic dependence on ICT firms, states will pass economic commodification polices **(i.e., national institutional regime)** protecting the use of personal and/or cyber data for profit.*
>
> *In EU states with a history of numerous domestic terrorist attacks, the state will promote securitized policies for cyber data **(i.e. a national institutional regime),** resulting in state and law-enforcement gaining access to the databanks of both public and private sectors.*
>
> *In EU states where legal experts or academics based in human rights disciples are used for legislative consultants during the law-making process, these states extend human rights protections over data legislation **(i.e., a national digital human rights regime).***

The outcome of interest (Y) during Phase 1 was the type of national data laws created by EU Member States. During the early years of this phase, data was computerized due to technological breakthroughs and adoption by public sector bureaucracies and private sector firms. In additional to manual data transfers to computer databanks, data could now be processed automatically, with no type of human oversight in processing. States had to determine how these activities would be legislated, in terms of data treatment during databank creation, and data processing and storage. States also had to decide if the new laws would apply to both state and non-state actors. The wording or content of laws could indicate:

- use of data as an economic commodity, and/or
- use of data for security purposes of the state, and/or
- protection of digital human rights for individuals' data.

I do not assume that three main preferences would generate mutually exclusively types of laws. However, when these interests came into conflict, lawmakers would have to prioritize

which of the three preferences will be granted the most leverage. To measure this outcome, I analyzed national laws that were introduced or passed in the case states during from 1970-1999 as regarding general personal data (pre-internet data).

Information on the national data laws was obtained from multiple research sites and official state sources. German data laws were obtained from two online repositories. English copies of some German data laws were sourced from the German Law Archive, a repository of over 2000 German legal documents translated into English by researchers at the University of Oxford, UK.[186] For laws unavailable at the aforementioned site, I retrieved the original laws in German from the *Bundesministerium der Justiz und für Verbraucherschutz* website, a law repository site maintained by the Germany Ministry of Justice.[187] The two most important laws originally unavailable in English were the 1977 and 1990 data protection laws. I located the 1990 law on the Bundesministerium website in html format, and subsequently translated the law into English using Google translate. The 1977 law was unavailable in a copiable format; I hired a graduate student majoring in German language acquisition from the University of Alabama to translate the law into English.[188] The Government of Sweden maintains a website for Swedish statutes in translation, provided by the Ministry of Justice; this was used as the source for Swedish data protection laws.[189] Laws unavailable in English were retrieved from the same website and were translated into English using Google translate. British data protection laws were retrieved from the government website legislation.gov.uk.

---

[186] Many thanks to the researchers involved in establishing this archive: Gerhard Dannemann, Christopher König, and Lorenz Böttcher. https://germanlawarchive.iuscomp.org

[187] https://www.gesetze-im-internet.de/index.html

[188] William Thomas, student at the University of Alabama, provided the English translation of the 1977 BDSG German Data Protection Law.

[189] https://www.government.se/government-policy/judicial-system/swedish-statutes-in-translation---judicial-system/

To assess each data law and categorize it as either protecting the data economy, giving access capability to law enforcement, intelligence agencies, or other governmental actors, or assign it as digital human rights, I performed manual content analysis. Chong and Druckman (2011) note that no standardized method exists for assessing the framing built into textual content and political communications material.[190] However, Chong and Druckman, and Rubin and Rubin (2012) all identify commonly used practices for researchers wishing to identify thematic patterns in qualitative data.[191] These steps include identifying the issue/person/event of interest, isolating the attitude of interest based on the research question, inductively creating original frames using past literature, and then choosing the material to analyze.[192] Prior to coding the actual documents, clear specification must be written to identify the frames that will subsequently be coded in the current material under investigation. Counting the frequency of frames, and whether they use positive/negative connotations can determine salience of a topic. Volume of mention or use of a particular frame can also indicate valence of an issue to the individual or organization issuing the communication. While the intent of this dissertation is not to measure the effectiveness of particular types of communications used by those writing the laws in each country or in the EU, I do argue that mentioning an issue in either a positive or negative light indicates intent to either support or remove support in a particular area. Lastly, using documents from the timeframe of key debates on policy change will ensure that a useful sample of material is evaluated for policy change.

For this dissertation, I therefore developed the following coding scheme in each case state:

---

[190] Chong and Druckman 2011, "Standardized guidelines on how to identify (or even how to define more precisely) a frame in communication do not exist.", p. 240.
[191] Rubin and Rubin 2005
[192] Chong and Druckman 2011, p. 240; Rubin and Rubin p. 207-211.

Table 2: National Law Coding Scheme (using Sweden's 1998 law as example)

	Positive mentions per sentence	Negative mentions per sentence	Net Score
Economic use of data	0, 1	0, 1	0
Security/law enforcement access	0, 1	0, 1	0
Protect data/privacy rights	0, 1	0, 1	1
TOTAL			0 = economic use of data 0 = security/law access 1 = protect data

Example: Sweden's 1998 Personal Data Act, Section 1 Reads, "Be it enacted as follows. General Provisions, Purpose of this Act, Section 1: The purpose of this Act is to protect people against the violation of their personal integrity by processing of personal data."

The above example from Sweden was coded 1 for one sentence with multiple words in favor of protecting data (protect, violation, integrity).

Thus, laws could be coded accounting for the possibility of multiple goals for data treatment. For example, if the the law included positive or negative mention or word associations when discussing any of the three frames (data commodification, security use of data, protecting data). The net score created during coding of laws indicates the overall hierarchy among the policy preferences for data treatment. For laws that treat data as an economic commodity will have words and phrases that discuss keeping data open for economic use, giving permission for data movement, and/or granting data controllers the ability to destroy or keep data indefinitely, according to their preference or need in doing business. Laws that securitize data will have words that give more access to government actors for security purposes such as permitting law enforcement or criminal investigators permission to collect or retrieve data from either public or private sources. These include court orders for surveillance, requirements for data processors ("controllers") to submit data when requested by state officials, or asking data controllers to retain data for certain periods of time if needed by government for criminal investigation or prosecution. In some cases, the laws even provide for data mobility during international criminal investigations or prosecution, whereby state officials could transmit data on a state's own

citizens across state borders to assist partner states with security processes. Finally, laws that legalize digital human rights will provide protection for personal data, such as limiting how processors collect, store, maintain, or re-use data (including selling or moving data to third parties). If the net score was equal for all three preference areas, it will be noted.

3.4 Measuring: Data Economy, Security Threats, Epistemic Expert Presence

The independent variables for Phase 1 included economic contributions of the data generated by business and personal use, domestic security/terrorism incidents, and legal or human rights experts used as consultants during law-making. I now explain the operationalization of these variables.

3.5 Economic Impact of Data

> *In EU states with large-scale economic dependence on ICT firms, states will pass economic commodification polices **(i.e., national institutional regime)** protecting the use of personal and/or cyber data for profit.*

Deciding how to measure the economic impact of data involved choices on how to operationalize the impact. The economic commodification of data is conceptualized in this project as any attempt by public or private actors to receive monetary gains from data, be it personal data collected and held on individual computers or computer networks, or cyber data created by individuals' participation in online websites and during use of smart and mobile phones. Data in these forms can be attached to personal identity, or anonymized, but it is being used for the purposes of generating profit for many types of industries, including firms that operate as "data brokers." Data brokers include public and private collectors, users, processors, and storers (i.e., "controllers") of personal or cyber data.

The digital and data markets are recent phenomena within the global economy. In Phase 1 (1970-1999), profits were made firms using data in many ways, such as firms that

computerized data, processed it, and/or created greater storage and movement technology. Economic gain from the ICT sector has been attributed to many industries by the OECD and World Bank, including manufacturing, telecommunications, retail, insurance, and financial services firms.[193] Unfortunately, as the technology sector developed unevenly across the EU, the resulting available variables to measure profits from data was inconsistent across EU states in the early years of computer automation of data. The most reliable measures collected across multiple EU states include ICT services exports (1961-2016), investment in ICT supply (1985-2016), high technology exports (1988-2016), and insurance and financial services (1985-present).

In order to best capture the impact of data upon the domestic economy of my case states, I chose to use variables used by the EU Commission in the 2017 Policies on the Data Economy Report as well as variables used by the IMF when measuring the digital economy.[194]

These include ICT services exports (% of service exports), investment in ICT supplies (% of total non-residential gross fixed capital formation), [195] high tech exports (% of manufactured exports), and insurance and financial services (% of services). The variables of ICT services exports, high tech exports, and insurance and financial services exports are all collected from the World Bank World Development Indicators database, when used during this dissertation.[196] Investment in ICT supplies was collected from the OECD database. Descriptive statistics of the four variables were compared in each case state.

---

[193] See OECD Digital Economic papers series, or World Bank annual reports on Information and Communications for Development.
[194] European Commission 2017, IMF 2018
[195] https://data.oecd.org/ict/ict-investment.htm
[196] World Development Indicators Database, Science and Technology indicators at http://www.worldbank.org

During Phase 2, the profit model shifted toward the production and utilization of big or meta data, in addition to the previously mentioned activities.[197] Big data brokers and generators of big data include "pure players", or firms whose core products create data-based products and services, alongside "mixed players" who combine traditional business practices with data-driven components.[198] Each of these industries generate massive quantities of data either directly as a result of their business model or as a by-product of their regular activities. The data created by these companies therefore has potential to serve as an economic commodity either to the producing firm or to other firms to which the data is sold in the global marketplace. After 2000, much more data became available, in terms of annual, country-level figures, and in terms of an increasing variety of measures for ICT sector impact. From 2000-2016, I utilize a comprehensive, composite measure I have created to test the impact of ICT and data generation on the domestic economy. These measures will be discussed in the separate section of this chapter that explains Phase 2 methodology. I also used the single variable, Value Added as percent of GDP; this data was retrieved from the OECD database.

3.6 Security Incidents

> *In EU states with a history of numerous domestic terrorist attacks, the state will promote securitized policies for cyber data* ***(i.e. a national institutional regime),*** *resulting in state and law-enforcement gaining access to the databanks of both public and private sectors.*

Security incidents are measures of threat perception of domestic security risk. "Incidents" are conceptualized as any domestic attack against state or non-state targets that could be perceived as a breach of state sovereignty, including attacks on territorial spaces, and physical infrastructure, whether military or civilian targets. I measured incidences of threats to security by

[197] Recall from the theory chapter that meta data is simply "data about data." Mayer-Schönberger and Ramge, 2018, p. 66.
[198] Carraneo et. al 2016

counting the frequency of such attacks (bombings, personal attacks, etc.) during Phase 1 in each case state. Data on security was sourced from the Global Terrorism Database (GTD) project which is organized and maintained by the University of Maryland.[199] The GTD is "an open-source database including information on terrorist events around the world from 1970-2016", containing over 170,000 data points. I provide descriptive statistics for Germany, Sweden, and the UK for Phase 1. For Phase 2, I add statistics for France as I discuss the predictions for the hegemonic states' preferences on data policy for the EU. While I had originally intended to also measure cyber attacks occurring in the 2000s, there is no single, reliable source for such attacks at present. The Council of Foreign Relations has an online list of reported attacks, but the accuracy of this list is conditional upon self-reporting by the attack targets. Given the questionable validity of this data, I made the decision not to include cyber attacks within the security incidents calculations.

3.7 Digital Human Rights

> *In EU states where legal experts or academics based in human rights disciplines are used as legislative consultants during the law-making process, these states will extend human rights protections over data legislation* ***(i.e., a national digital human rights regime).***

Digital human rights is the term I developed in the introduction chapter to describe rights-based legal protections of personal data, and later, for cyber data. I argue that states which extend human rights protections over data may do so through the influence of legal and human rests experts who come from judicial or academic backgrounds. This argument follows the logic in the human rights and social movements literature, which has shown links between the pressure of non-governmental actors who seek changes to current law or additional human rights

[199] https://www.start.umd.edu/gtd/about/

protections and positive government responses.[200] Pressure can be applied by "strategic use of information to garner attention...[201] Based on this literature, I originally intended to evaluate human rights activism for data protection by following the example of following the example of Ron, Ramos, and Rogers (2005), who tallied the number of privacy-based NGOs involved in data protection activism.[202] Unfortunately, identifying these groups proved highly unsuccessful, as groups dedicated to this mission did not emerge until the mid to late 2000s.[203]I was therefore unable to create my own comprehensive list of organizations that worked at the national level on this topic in each of my case countries.

I then attempted to assess information campaigns waged promoting data protection at the national level. Media coverage is assumed to contribute to the larger movement success, as it promotes public awareness of topics, builds urgency into calls for action, and facilitates increased membership in social movements, all of which impact funding sources and further movement potential.[204] I had intended to measure information warfare campaigns about data protection and digital human rights for both phases by looking at news coverage and news advertisements from 1970-2016. Unfortunately locating news stories covering information campaigns about data protection proved equally difficult. Major news outlets did not digitize newspaper content in the Lexis-Nexis system until at least the mid to late 1990s. They also did not backdate the digitized content, so all content present in Lexis-Nexis is only from

[200] Keck and Sikkink 1998, Tarrow 1998, Tsutsui and Wotipka 2004.
[201] Stroup and Murdie 2012
[202] Ron, Ramos and Rodgers 2005
[203] For example, the European Digital Rights association (EDRi) was formed in 2002 to advocate for data protection and other types of protections for digital content across Europe.[203] In addition, the creation of a list stakeholders who file regular reports to the UN High Commissioner regarding the right to data privacy is a new phenomenon from the 2010s.
[204] Benford and Snow 2000, Kolb 2004.

approximately 1995-forward. This left no way to access the news coverage of such campaigns during Phase 1.[205]

I developed a proxy measure for human rights advocacy around data. As outlined in the theory chapter, epistemic experts can and do alter policy outcomes by drawing on community norms within their profession. To measure the influence of epistemic experts I looked at legislative investigatory committees and consultants sought during the research phase of new data legislation in each case during Phase 1. Each national database listed in the prior section on data legislation coding was also queried for committees, consultations, public hearings, and other support meetings held prior to each major piece of data legislation, using the terms "data, protect, rights, personal, integrity, privacy, and computer." I also outline the personal professional training and background for each national supervisor placed as the head over each country's data protection authority agency. I assume that those coming from legal, jurist, and judicial backgrounds are more likely to promote data protection rights, than those from business, ICT, or non-legal, non-academic professional histories. The shortcoming of this method is that one cannot establish directly the motives for individuals outside their personal statements, but when available, personal quotes and official text released by these persons were used to support each case.

3.8 Supranational Data Policies in the EU (mid 1990s-2016)

> *The presence of strategically placed legal and human rights experts will lead to expanded human rights protections over data, creating a digital human rights regime.*

To test the expectations for Phase 2, I used several mechanisms to trace the influential components and outcomes from the mid 1990s-2016. First, I confirmed the preferences of the

[205] Top news consumption rates are reported by the Council for European Studies at Columbia University and the Reuters Institute reports on an annual basis.

powerful states along the three causal factors from Phase 1 (data commodification, national economic dependence upon the ICT sector, and digital human rights). I use these preferences to predict what each state will promote during their tenure as EU Commission President, during which the country has greater capacity to drive the legislative agenda for the Union.

Regarding economic dependence upon the ICT sector, I created a composite mechanism to measure the impact specifically for this dissertation, which I will explain below. Domestic terror attacks recorded by the Global Terrorism database were compared across three powerful states to predict propensity to support data securitization. The professional background of national agency heads for data protection were utilized to measure legal epistemic influence, since these agency heads often serve as the points of contact between the EU Commission and Council of Ministers and the various national authorities responsible for implementing EU data law.

Next, I performed content analysis of media communications and official documents released by the EU Commission to identify any framing used by the Commission presidents when attempting to call for new EU data legislation, or when asking for amended legislation that reflected their states' preferences during Phase 1. Finally, I compared the expected national preferences to the calls by EU Commission presidents for legislation against the types of actual EU laws passed to determine if the hegemonic states' preferences prevailed. To summarize, the national preferences serve as causal factors, while the types of data laws are the outcomes. Regarding the influence of epistemic experts, their presence in key research bodies is a causal factor and I expect to see them make calls for expanded high levels of data protection as attempts to influence policy toward digital human rights.

3.8.1 Phase 2: 1990 to 2015

At the EU-level, powerful states will attempt to influence EU policy to align with their own national preferences.[206]

The case states identified as "hegemonic" or powerful states follow the parameters established by Morgenthau (1947), Keohane and Nye (1989), and Krasner (1983), in their respective works on balance of power theory, Hegemonic Stability Theory, and regime theory.[207] Hegemonic, or great power states, are those possessing more military and economic power than that of the near neighbors in their region, or even globally. In the European Union, I apply this definition and find that the United Kingdom, France, and Germany are the predominant hegemonic states in the EU. Thus, these states could have more power to push their policy preferences at the EU level.

During Phase 2, technology diffusion occurred simultaneous to technological advancement. More extensive data on the economic impact of data became available from 1991 forward. To measure the increased dependence upon economic growth in ICT , I created a composite measure I call the Data Technology Exports Contribution (DTEC). This covers the additive effect of economic gains from exports made by technology-based firms from 1990-2016 in each country. The DTEC contributes greater understanding to our knowledge of the economic power of these industries by highlighting growth in *exports* of data. Recall that data mobility was one of the first motivations for data protection promoted by the OECD and Council of Europe. Measuring separate variables is helpful to understand which firms within ICT may be growing faster than others, but use of individual variables does not answer the cumulative effect of sector-

[206] This is based upon Hegemonic Stability Theory, explanation in the subsequent paragraphs.
[207] Keohane 1985; Keohane and Nye 1989; Krasner 1983; Morgenthau 1947.

wide growth. The DTEC offers an expansive look at the varieties of ways in which data-driven industries will contribute via exports within the global digital economy. See Figure 2.

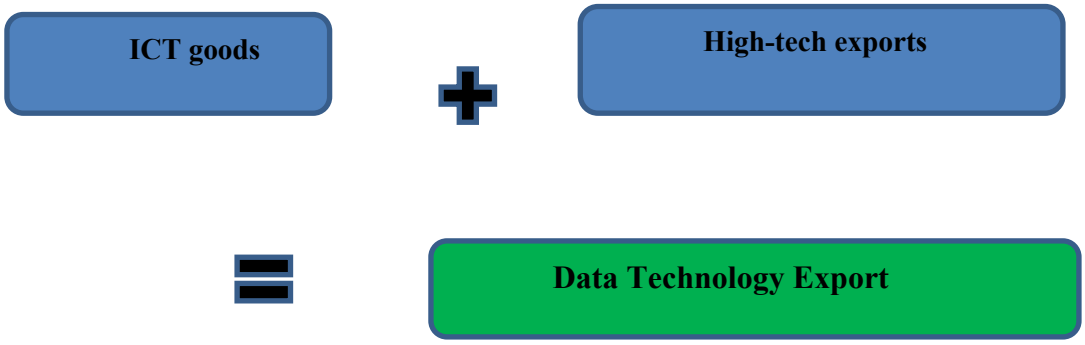


Figure 2: Demand: Export Value of ICT Firms

To create the composite measure, Data Technology Contribution, I take the raw data for the variables indicated in Figure 1 for each of the three case states (explanation on choice of states to follow), standardize all variables, and calculate the mean value in five-year periods for each indicator.[208] The DTEC composite identifies case country trends in digital technology impact, which I use to predict propensity to support data commodification within EU data legislation. Secondary to the first prediction:

> *National representatives serving on the Commission will promote calls for new legislation for EU legislation that align with the national interests during Phase 2 (data commodification, data securitization, digital human rights).*

The independent variable for this hypothesis was calls for legislative action taken by national representatives to introduce EU legislation that align with national policy preferences. As established in the theory chapter, agenda-setting on EU legislation is primarily done by the

[208] This will create composite predictions for 1990-95, 1996-2000, 2000-2005, 2006-2010, and 2011-2015.

EU Commission. The starting point was to look at communiques from those serving on the Commission, with a focus on Commission presidents, and officials within the Directorate-General for Justice and Consumers who hold responsibility over justice, consumer rights, and gender equality issues. I also studied the communiques of representatives serving on the Council of Ministers within the Justice and Home Affairs Council (responsible for supervising this issue area for the Council).

Finally, I added key investigatory committees, such as the EU Commission Working Party 29, which began in 1995. The Working Party was "established by Article 29 of Directive 95/46/EC…. [and] provides the European Commission with independent advice on data protection matters and helps in the development of harmonised policies for data protection in the EU Member States."[209] Working Party 29 began research in 1995 and continued until 2018 when the GDPR went into effect. The party included representatives of the national supervisory bodies in the Member States, a representative of the European Data Protection Supervisor's office, and an EU Commission representative. The group contributed significant amounts of research and policy recommendations to the Commission, in the form of press releases, official documents and opinions on policy suggestions, and issued annual reports with suggested policy directions for data governance. After identifying the crucial actors involved in opening opportunities for new legislation, I could collect the documents that spoke to their intentions for EU data policy.

Any official press releases, calls for a proposal, presidency mission statements, or other communications that were generated from the Commission, Council of Ministers, or Working Party 29 during Phase 2 (1990-2016) were studied for intent to legislative data along any of the

[209] https://edps.europa.eu/data-protection/data-protection/glossary/a_en

three preference alignments. If the elites called for legislation, but the framing of the text within the proposed EU legislation included concerns not addressed by my hypotheses, OR if the wording was in opposition to my predictive patterns this would confirm that intergovernmentalism was ***not*** at play.[210] In other words, through communications or activities to push national preferences rather than reach a coordinated compromise during times of policy conflict, EU Commission Presidents, Council representatives, or those on the WP 29 committee could show attempts at supranational agenda controls. Evidence of promoting nationally preferred policies at the expense of coordinated intergovernmentalism would challenge some scholarship that has argued for intergovernmental policymaking. Contrarily, if these leaders and/or WP 29 By suggest alternatives to my three proposed policies or suggest "middle ground" compromises, these individuals would indicate they were considering the community-wide interests in conjunction with national interests on the issue of data governance. In other words, community concerns would overshadow states' interests if the null were true.

> *The presence of strategically placed legal and human rights experts will lead to expanded human rights protections over data, creating a digital human rights regime.*

Epistemic experts at the EU level are expected to play a similar, but expanded role, to that of the national level argument. Similar to during the investigatory phase of national policy-making, the EU uses experts as consultants to many EU institutions and oversight bodies. I looked for how these individuals were utilized as information providers and the positions of influence they held as relates to the most powerful bodies of EU lawmaking: the Commission and Council of Ministers. WP 29 formally released three types of documents to the Commission on a regular basis: Opinions, Recommendations, and Annual Reports. Each of these contained

[210] Recall from the theory (section 2), that intergovernmentalism, as proposed by Moravscik and others, argues that states will promote their national preferences rather than think in a community mindset, when setting EU-level policy.

assessment of current conditions, validity and effectiveness of current laws, and examination of the current social, economic, and political conditions that may warrant changes to EU data laws. Suggested changes were also provided in these communiques. If EU laws expand human rights protections when WP 29 suggested protection expansion, or in spite of opposition by security or economic interests, the argument for the importance of epistemic experts in changing EU policy can be supported. The coding scheme for evaluating the documents from WP 29 is explained in the following paragraph.

Next, the EU laws are examined as outcome variables for the increased pressure placed on EU lawmakers. The presence of increased laws for data protection as a fundamental human right further supports the argument that a digital human rights regime has been created in the European Union. The process of passing the following list of laws as relates to EU data legislation was examined at length. Given the lengthy content of these laws, they were not manually coded as were the national data laws. Batch coding was automatically applied using MaxQDA Software. Using an a priori coding scheme of the frequently used descriptions for the main three variables (data commodification, data securitization, or data protection rights), each law received a lexical search for the key terms. Each law was then auto-coded for word frequency of each term. This provides a blunt instrument to measure the content of each law. The search term scheme is indicated in Table 3.

Table 3:Auto-code Search Terms

Data Protection Search Terms	**Security Search Terms**	**Economic Commodification Search Terms**
Processing of personal data	Security	Economic
Protection of personal data	Police	Business
Right to privacy	Judicial	Marketing
Fundamental rights and freedoms	Court	Free movement of data
Fundamental right	Defence	
Consent		

While it does not allow for sentiment analysis as with the national laws, the code frequencies are capable of establishing the main focus of each law along the three preference areas. See Table 4.

Table 4: EU Personal Data Policies

Year	Directive/Regulation	Source/Description
1993	Maastricht Treaty	Includes brief mention of secrecy responsibilities for data accessible by some EU staff
1995	Directive 95/46/EC , Article 1 *	EU Commission: Establishes fundamental rights of natural persons as regarding processing of personal data; forbids restriction of free flow of personal data between Member States
1997	Directive 97/66/EC	EU Commission: Proposal for Council Directive on personal data/privacy as relates to public digital telecommunications and mobile networks
1997	Amsterdam Treaty	Incorporates protection for personal data during automatic processing alongside facilitation of free movement of data
2000	Treaty of Nice	NO mention of data protection at all
2000	Charter of Fundamental Rights	Included the right to protection of personal data; UK opposed this, stating Convention did not have this competency
2001	Regulation No. 45/2001	EU Commission: Provisions for processing personal data by Community; created European Data Protection Supervisor (EDPS)
2002	Directive 2002/58/EC	EU Commission: Regulates protection of data and privacy during use by electronics and telecommunications firms
2006	Directive 2006/24/EC	EU Commission: Requires traffic data retention for 6 mos-2 yrs. for prosecution of serious crimes
2007	Lisbon Treaty	EU: Modified legal structure by abolishing pillar structure, including past Treaty Provisions for protection of personal data; establishes data protection as a fundamental right by this moving of the issue into a first pillar area of competency
2008	Directive 2008/977/JHA	Justice and Home Affairs Council framework for data protection during police cooperation
2012	Code of EU Online Rights, Chapter 4	EU Commission: Establishes basic rights for EU citizens when using online networks and services.
2016	General Data Protection Regulation 2016/679	EU: Extends the protection of processing of personal data as a fundamental right; preserves free flow of data; mandates third country compliance
2016	EU-US Privacy Shield	EU Commission: Establishes minimal standards of processing protection for EU citizens' personal data transferred to US during use of digital marketplace or social media

Finally, the theoretical basis for this dissertation proposes that EU states occupy international spaces that include overlapping, nesting, or duplicative regimes at the international

level that may compete with their domestic regimes on data legislation. I evaluate the regime memberships in which EU states are members as relates to the calls for data governance by each regime. This allows me to test the impact of pressure by these regimes upon EU states to pass laws the align with the treaty commitments of the regime.

Now that I've described the various methods used to collect data and test the expectations for the national and EU-level of data policymaking, I turn in Chapters 4 and 5 to explaining the outcomes found.

4 THE DEVELOPMENTOF NATIONAL PREFERENCES ON DATA PROTECTION POLICIES, 1970-1999

4.1 Findings - Sweden

I began with the state of Sweden, which was the earliest adopter among my case countries to create any type of data-specific law or statute. The first law passed was the Data Act of 1973 (*Datalagen*), and was designed to prevent "undue encroachment" on individual privacy of personal data. Aspects of data protection addressed in the law included data collection, treatment, and storage, descriptions about the properties of the data subject,[211] and the level of permission required from the data subject. Most importantly, it served as a template for subsequent legislation adopted in many western European states.[212]

The 1973 law also set the pattern for future data laws in Sweden, taking the stance that personal data should be protected by the state. The justification written into the laws and given in statements by the data protection authorities stated that using data represented a risk of loss to the data subject. The Swedish language does not have a word that directly translates into "privacy"

[211] "Data subject" is a frequently used term among data laws and data policy suggestions by various international organizations. It refers to the individual(s) about whom the data is collected.
[212] Flaherty 1989, Fuster 2016.

in English, but the references to data protection in the 1973 law and following laws repeatedly refer to the protection of the data subject's "integrity". Data controllers[213] are obliged to prevent such a breach from happening, or suffer a variety of penalties, such as fines, prosecution, or even imprisonment. In other words, Sweden took a very hardline stance toward personal data protection as a human right almost as soon as data collections were amassed in large-scale data banks in the 1960s and 1970s. The 1973 was the first of thirteen laws passed during Phase 1 that affected personal data in any way. Two laws concerned only the agency staffing and regulatory authority, without mention of the data treatment itself.[214] All laws that directly impact personal data treatment are listed, along with their net scores, in Table 2, next page.

Table 5: Swedish Data Laws, Phase 1 (1970-1999)

Year	Name of Law	Description	Total Coded Sentences	Text Analysis Scores	Net Score
1973	Data Act (*Datalagen*)	Prevention of loss of personal privacy through data use	37	+ 2 Econ Pos -8 Data Protect +27 Data Protect	+2 Econ +19 Data Protect
1973	Credit Information Act (*Kreditupplysningslagen*)	Regulate licensing for credit and debt collection firms that collect data; Created the Data Inspection Board (DIB)	36	-5 Data Protect +31 Data Protect	+31 Data Protect
1974	Debt Collection Act (*Inkassolagen*)	Regulate use of automated personal data files; no collection of religious, political, or race data to be kept.	8	-4 Data Protect +4 Data Protect	0
1978	Act on Names and Pictures in Advertising (*Om Namn Och Bild I Reklam*)	Regulate personal data use in advertising.	7	-3 Data Protect +4 Data Protect	+1 Data Protect

[213] "Data controllers" is defined as individuals, businesses, or public actors who are responsible for data collection and management of data regarding data subjects in any form.

[214] The 1982 Data Fee Ordinance (*Förordning om avgiter för Datainspektionens verksamhet*), and the 1987 Ordinance for Authorization for the DIB to Execute on Automatic Data Processing in Tax Audit (*Förordning med bemyndigande för datainspektionen att databehandling vid taxeringsrevision*) did not directly impact data protection or treatment.

1980	Secrecy Act (*Sekretesslag*)	Allows for data movement between governmental authorities.	50	+8 Security Pos -1 Econ Neg +6 Econ Pos -14 Data Protect +21 Data Protect	+8 Security Pos +5 Econ Pos +7 Data Protect
1981	Credit Information Act, amended	Changes to credit record-keeping; data banks have to update DIB if credit info services are ended.	3	+3 Data Protect	+3 Data Protect
1981	Debt Collection Act, amended	Changes to debt collection practices, but no significant data changes	2	+2 Data Protect	+2 Data Protect
1982	Data act, amended	Reduced licensure requirements for data processors, except for sensitive data banks. Raised fees to help recover costs of DIB.	6	-2 Data Protect +4 Data Protect	+2 Data Protect
1987	Ordinance with Instructions for the Data Inspectorate (*Förordning med instruktion för datainspektionen*)	Instructions for DIB officials on conducting inspections for data controlling registries.	2	+2 Data Protect	+2 Data Protect
1998	Personal Data Act (*Personuppgiftslag*)	Regulate identity data among "data controller" firms in Sweden. Align Swedish national laws with EU Directive 95/46/EC	86	+2 Security Pos -1 Econ Neg +4 Econ Pos -30 Data Protect +49 Data Protect	+1 Security Pos +3 Econ Pos +19 Data Protect

Source: Swedish Law Repositories located at http://www.riksdagen.se/sv/ and https://www.regeringen.se/

Conditions prior to the establishment of new laws play into the theoretical argument on why laws were created and which interest groups the law may serve. The years prior to the 1973 law saw a high level public anxiety over a proposed public census and responses by the government to involve academics and jurists in particular, as expert witnesses to the Riksdag (parliament) regarding the need and types of laws that should be considered for data.

In the early and mid 1960s, mechanized record and data management expanded in Sweden. Yet expanded technology adoption alone did not create public concern over personal data use until the late 1960s. To explain this, one must understand two factors: the proactive nature of Swedish governance, and the structural conditions present at the time.[215] Scholars have

[215] Bennett 1992

shown that the Swedish government has taken a proactive stance toward policy-making, rather than wait until conditions become negative and need correction.[216] In addition, existing laws in Sweden in the late 1960s and 1970s allowed access to governmental document archives for members of the press and the public.[217] The government proposed a population wide census for 1970; this proposal led to public concerns over the ways that census data would be managed and who would have access to the data collected.[218]

One additional condition that facilitated public fears over the information that could be released as a result of the updated census in the era of computer-based data was that universal adoption of national identification numbers (PINs) for all members of Swedish society. PIN data includes birthdate and sex, and have been used by all private sector and governmental agencies when providing services to people, similar to social security numbers in the U.S. census data were collected, and individuals were identified and listed by PINs, given the public access of all governmentally-collected data, then anyone in society would have access to whatever information was collected by the Census enumerators. Finally, heightening public concerns also radiated around the potential for computer linkages of the census data using PINs to other databanks not authorized to possess the information collected by the government during the census enumeration.

Responding to public fears, the Riksdag delayed the census, and instead fell back on a structural practice of creating an advisement committee to investigate the issue further before moving forward. Parliament established a Royal Commission on Publicity and Secrecy of

---

[216] Elmore et. al 1986, p. 221.
[217] Freedom of Press Act (*Tryckfrihetsförordning*, 1949:105) and multiple versions of the Secrecy Act, dating back to 1937.
[218] Bennett 1992, p. 62-63; Newman 2008, p. 42-50.

Official Documents in 1969.[219] While the commission was completing its report, the Supreme Administrative Court, the highest civil court in the state, issued a ruling in 1971 ruling that magnetic tapes used for storing information were de facto documents, making them subject to public access similar to other documents under the Freedom of the Press Act. This raised the question on what types of limits should be set for the access to documents, and automatic data processing (ADP) under the Freedom of Information Act.

The 1972 report, "Computers and Privacy" concluded that new ways of collecting and storing data did indeed present "… new threats to threats to personal privacy. Compared with information kept in documents it is principally a matter of degree, but the difference is such that the situation has changed in a decisive way."[220] Following this report, the Riksdag passed the Data Law in April of 1973, which set the initial restraints on data treatment by public and private actors. Importantly, the law institutionalized the protection of personal data by forming a Data Inspectorate Board (DIB), which would be permanently responsible for oversight on the implementation and monitoring of compliance with the law. The creation of this investigatory commission by the Riksdag and the passing of the 1973 law set the foundation for personal data rights as a normative practice in Swedish data policy. All data laws that were passed after the 1973 law throughout the Phase 1 period until 1999 followed the precedent set by this law in protecting personal data, and later cyber data, as a right to privacy, or "integrity" of the individual person.

After looking at the coded laws for the Phase 1 period, and the initial law creation, it is clear that the overwhelming outcome for the case of Sweden was the establishment of data

[219] Flaherty 1989.
[220] Sweden, Commission on Publicity and Secrecy of Official Documents, *Computers and Privacy*, p. 6 (Sweden 1972)

protection as a digital human right. I now turn to test the three hypotheses to see if the contributing factors confirm the outcome as being tied to elite activity around data protection. The first hypotheses proposed that dependence upon ICT firms will predispose a state to allow for data commodification.

4.1.1 Economy

The Swedish economic model is one with foundations in the 1930s.[221] Similar to many states during the worldwide depression of the 1920s and 1930s, Swedish politicians and economists developed state policies designed to ameliorate the effects of the depression. First efforts at social welfare were motivated by the desire to reduce industrial conflict, as strikes and wage-based disagreements were frequent occurrences in the early 20th century. In 1928, the Saltsjöbaden agreement was reached between the Swedish Employers Association (SAF), the Swedish Trade Union Confederation (LO), and the government. The Social Democrat party maintained control over the government for over 40 years, from 1932-1976. The Saltsjöbaden agreement and having the same government in power provided the foundation for corporatist negotiations and policy agreements between management, labour, and the state for the remainder of the 20th century. In the 1940s, the ministry of finance attempted modified Keynesian demand policies to fuel growth; tax rates rose and restrictions were placed on planned investments and reserve fund withdrawals. From the 1950s and 1960s, additional taxation, and reduced currency movement were implemented at the suggestion of economists Rehgn and Meidner. The Rehgn-Meidner plan of structural rationalization was aimed at offsetting the overheated economy. The plan promoted a wage plateau and elimination of unprofitable firms, whist retraining and

[221] Magnussun 2000 was the data source for the industrial and economic history of Sweden during the 20th century, references in this section of the dissertation.

relocating the unemployed. By the end of the 1960s, labour market policies were the most popular economic tool used by the government.

Sweden experienced a severe recession in 1971. The 1973 election created a balance between socialist and non-socialist blocs; economic policies during this period such as "tax reductions, industrial stockpiling, releasing of investment reserves…" did lead to wage increases of 4%, but exports fell considerably due to the overpriced currency (krona). These factors in turn created severe unemployment, stagnant industrial growth, and large deficits in the balance of payments resulting in a severe depression by 1976. Stagflation took hold. In 1976, the Social Democrats experience losses during the election and their power bloc in parliament. The new non-socialist government had different ideas on how to manage the economic crisis. They introduced tax reductions and releasing of investment reserves. Most importantly, the government devalued the krona three times; values fell 14% between 1976-77, and an additional 11% by 1981. Traditional mechanical production sectors suffered the worst damage during this era. Shipbuilding, iron, steel, and mining all had production fall by between 30-50% from 1974-1982. The government spent considerable amounts to support benefits to employees in these industries, much of which was borrowed from overseas. Despite the eventual economic plateau and then recover, these industries did not resume their pre-depression production rates. By 1982, competitiveness had returned to the Swedish economy, exports began to rise, and unemployment started to fall again.

The 1980s and 1990s saw a crack in the strength of the compromise model that had been established since the 1930s. In 1982, the Social Democrats were turned to power, and party leader Olof Palme and his minister of finance Kjell-Olof Feldt mimicked Margaret Thatcher's "first way" policy with a "third way" for Swedes. In addition to keeping the krona value in the

competitive range, wage solidarity policies and trade union loyalties were firmed in order to cap wage increases. The Ministry of Finance released money and financial market restrictions, releasing capital flows, which then prompted speculative property investing. The prior imbalance of payments was corrected by the mid 1980s, but the third way policies had set in motion other outcomes that were less favourable. Inflation grew. Unfortunately, the manufacturing and export-oriented engineering sectors experienced a labour shortage that subsequently reduced productivity in the areas of the economy that had grown most substantially during this period. Despite the currency devaluations, resource transfers were not able to compensate for these deficiencies in the export sector of tech-based industries, which had begun to flourish as traditional manufacturing exports shrank. The overheated economy of created a series of "crisis policies" on the part of the Social Democrats in 1990: strikes would be banned, and wages frozen again. The Social Democrats resigned after an uproar in parliament over the suggested policies. Sweden felt the slowdown of the global economy in late 1990, and deflation resulted as the Moderate government had to break its campaign promise to prop up the value of the krona. By the mid 1990s, Sweden had undergone a series of banking crisis, requiring government bailouts in 1990, 1991, 1992, and 1993.

To summarise: the picture of economic contribution in Sweden during Phase 1 follows the pattern of many industrial states in the West. Immediately following World War II, Sweden relied upon a corporatist bargaining model and industrial manufacturing of consumable goods such as iron, steel, and less so, but still including some agricultural components for economic stability. A recession/depression in the 1970s led to increased mixed economic policies whereby the government began to experiment with the core "Swedish economic model" in order to offset increased oil prices, inflation, and an overvalued currency. While the corrections were successful

in the short-term, they were accompanied by changes in the global market that reduced demand for traditional manufactured goods, plus increased wage competition from overseas. Swedish businesses began to adapt by growing into mechanical engineering and technology based production more broadly, and technology and service sectors more specifically at the middle of the 1980s until today. As a result, the percentage of persons employed in tech sectors increased, and the resulting dependency of economic growth upon ICT sectors increased as well.

The theoretical argument set the expectation that in EU states with significant economic dependence upon ICT firms, these countries will be likely to pass national regimes protecting data commodification. The data available in the early years of Phase 1 to measure the contribution of the ICT (information, communications, and technology sector), involves two subsectors of ICT services: ICT services exports, and the insurance and financial services exports. Both variables were measured by the World Bank as a percentage of overall commercial services exports, and were found in the World Development Indicators database.[222] Looking at the latter part of Phase 1, the data on investment in ICT supplies and high tech exports becomes available, giving a more in-depth picture of the role that ICT sector firms played in the Swedish economy during this period.

[222] The World Bank 2018

Table 6: ICT Services Sector Contribution, Sweden, 1970-1990

Year	ICT Services Exports, % of services exports	Investment in ICT Supplies, % of total non-residential gross fixed capital formation	High Tech Exports, % of manufactured exports	Insurance & Financial Services, % of commercial services exports
1970	9.35	*	*	6.70
1971	8.70	*	*	7.03
1972	9.96	*	*	**7.48**
1973	9.70	*	*	5.89
1974	10.10	*	*	4.84
1975	14.07	*	*	5.20
1976	13.29	*	*	6.49
1977	14.15	*	*	5.32
1978	**15.53**	*	*	4.69
1979	13.53	*	*	3.73
1980	11.36	*	*	4.02
1981	10.49	*	*	3.14
1982	**31.53**	*	*	**6.74**
1983	31.14	*	*	5.57
1984	**34.27**	*	*	5.40
1985	17.55	15.04	*	5.43
1986	17.47	15.43	*	7.24
1987	13.71	15.80	*	7.70
1988	12.42	16.48	12.34	8.70
1989	13.41	15.48	12.71	9.69
1990	14.20	15.21	12.90	9.26
1991	14.67	16.80	13.29	12.64
1992	14.76	19.83	**13.31**	**12.71**
1993	15.58	**26.45**	12.97	3.53
1994	16.56	25.46	12.83	2.97
1995	18.32	24.84	16.41	2.47
1996	19.45	24.08	17.94	2.48
1997	22.38	25.59	19.44	2.72
1998	35.33	27.76	19.82	3.05
1999	**36.40**	**28.80**	**21.54**	3.24

Source: World Bank, World Development Indicators Database; OECD

* Indicates no data available for these years

Table 6 reveals the upward growth in the ICT sector in general, with services exports, high-tech exports, and ICT investments experiencing several peak periods in Phase 1, and a peak in Fin-services exports in 1992. ICT services exports in the 1970s contributed 9.35% of all service exports, but had nearly doubled by 1978 to 15.53% of service exports. ICT services exports struggled in the late 70s and early 80s, but had doubled again to 34.27% of services exports by 1984. Oddly the sector contribution halved in 1985, and didn't recover to previous highs until 1998 and 1999, with rates of 35.33% and 36.40% respectively. Unlike ICT services exports, Investment in ICT Supplies (as a percentage of total non-residential gross fixed capital formation) experienced steady growth in the years 1985-1993, rising from 15.04% to 26.45%. Here the levels essentially plateaued, rising slightly to 28.8% by 1999. High tech exports as a percentage of manufactured exports experienced a similar pattern to ICT investments, by rising steadily between 1988-1999, from 12.34% to 21.54%. Finally, Insurance and Financial Service exports (as a percentage of commercial services exports) were quite volatile from 1970-1982; figures began at 6.70%, dropped to 3.14%, then bounced up 6.74% of commercial services exports. From 1982-1992, the general trend was upward, reaching 12.71% in 1992. After this point, figures dropped dramatically, never rising about 3.53%, thus contributing much less to the economy.

We know that the environment for tech and ICT firms between 1955-1980 was somewhat positive; there was a positive market for entrepreneurship of these firms. According research by MIT and the Swedish Board for Technical Development, the fastest growing firms in Sweden by 1980 were those whose product or services were primarily in technological fields.[223] Out of 250,000 persons employed in manufacturing, 85,000 people worked in technical engineering

[223] Utterback et. al 1988

firms, or approximately 34% of those working in manufacturing altogether. Interviews of 77 firms revealed that 25% of these firms formed after 1955 had revenues above $1 million USD by 1980. In addition, surveys of engineering-based firms employing at least 20 people between 1955-1980 were independently owned in Sweden, making tech-based entrepreneurship a significant portion of the start-up businesses of the time.[224] Compared to the other two cases, Sweden falls in the middle of the three countries in terms of employment in technology industries. As the data in Table 3 shows, three of the four variables of available data on the ICT sector for this period indicate a significant contribution by these firms to the Swedish economy. It is less clear why the ICT insurance and financial services did not experience the growth of the other ICT products and services industries. It is beyond the scope of this dissertation to address this deviation from the other variables, but it is certainly worth investigation in research for the future.

Unfortunately, as I have shown, the overall economy of Sweden was not experiencing steady growth from 1970 to 1990. Sweden's annual GDP per capita of growth of 1.99%, which was below the OECD average of 2.71%. Overall, in the case of Sweden, while ICT firms experienced generally positive growth, and provided an increasing contribution toward the Swedish economy, these contributions do not seem to have impacted the protection policies chose for data by the Riskdag. Data commodification was *not* codified into a majority of the laws, and minimally codified into the Secrecy Act of 1980 and the Personal Data Act of 1998. I conclude that Hypothesis 1a is ***not*** supported in the case of Sweden.

[224] Utterback et. al 1988; approximately 85,000 out of 250,000 firms.

4.1.2 Security

As indicated in the methodological chapter, **security incidents** include "any attack against state or non-state targets that could be perceived as a breach of state sovereignty, including attacks on territorial spaces, and physical infrastructure, either military or civilian targets." The more frequent and numerous are security incidents in the state, data access for security, police, and law enforcement personnel will become more important. To test this expectation, I looked at data for these types of attacks during Phase 1; this data was acquired from the Global Terror Database (GTD).[225] Table 4.3 provides an overview of the frequency of conventional security incidents in Sweden during Phase 1 (see next page for full table).

Table 4.3: Security Incidents, Sweden, 1970-1999

Year	Fatalities	Injuries
1971	1	2
1972	1	0
1973	0	0
1974	0	0
1975	**3**	**13**
1976	0	0
1977	0	0
1978	0	0
1979	1	0
1980	0	0
1981	0	0
1982	0	0
1983	1	0
1984	0	0
1985	0	0
1986	1	1
1987	0	0
1988	0	0

[225] Note: There were no cyber attack incidents during this period, due to the nascent condition of the computer industry as a whole. Data reveals that states and non-state actors had not begun to use cyber offensive attacks among the case states until after 2005.

1989	0	0
1990	**1**	**11**
1991	1	1
1992	**2**	**5**
1993	0	0
1994	0	1
1995	0	0
1996	0	0
1997	1	1
1998	0	0
1999	**0**	**4**
Total	**13**	**39**

Source: Global Terrorism Database

Recall I expected states with numerous domestic terror incidents to be more likely to pass national regimes of data securitization, yet Sweden did not experience a significant number of such incidents. Looking at Sweden's data on security incidents, statistics reveal the most activity in 1975, 1990, 1992, and 1999. These figures confirm that among the case states, Sweden experienced the least numbers of terror attacks. Looking at the four years of heightened activity, we see that each of these occurrences were unusual events in some way, and disconnected from any larger, organized and long-term security threat to the state. The 1975 attack involved a stand-off between five guerilla members from the German Baader-Meinhof, or "Red Army Faction" militia group stormed the Swedish Embassy in Stockholm. The extreme Marxist and anti-Semitic group was active in Germany from approximately 1970-1998, and used violent means such as bombings, kidnappings, and gun battles with police as a part of their wider goals to generate a revolution against the disproportionate power of the industrialized states against the rest of the world.[226] During the 1975 attack perpetrated against the Germany Embassy in

[226] Moghadam 2012

Sweden, five RAF members held embassy staff hostage, whilst making demands for the release of 26 RAF group members imprisoned in Germany. Swedish security and German authorities refused to negotiate with the militants, and after approximately 12 hours, two people were dead (two embassy staff persons, one militant).[227] During the melee, the militants set off an explosion that blew up the embassy, and caused burns and injuries to members of the group and remaining hostages in the building. This event represents the single-most loss of life connected with a security attack in Sweden during Phase 1, however, the overall effect was intended to target not Sweden, but the German government and its policy.

All of the subsequent security attacks during Phase 1 involved isolated individuals or groups as the targets. The highest profile, politicized attack took place with the 1986 assassination of Social Democrat Prime Minister Olof Palme. Investigators blamed a then-unknown gunman, who appeared off the streets of Stockholm to shoot Palme as he was leaving a theatre with his wife one evening. A petty criminal was convicted in 1989, but this ruling was later overturned in 2004.[228] Multiple theories abound as to the root cause of Palme's death, including accusations against arms dealers from India, Kurdish rebels from Turkey, or a former witness interviewed by police after the killing, Stig Engstrom. To this day, no concrete proof has been offered as to the motivation nor has the real killer been identified, causing the attack on the prime minister to be categorized as an isolated incident.

Following the prime minister's death, the next national security challenges arose in the early 1990s. A far-right Swedish extremist by the name of John Ausonius ("the laser killer") shot members of various Stockholm communities in 1991-1992.[229] He was convicted in 1995

[227] BBC News 2005
[228] Anderson and Cowel 2018
[229] BBC News 2017

for a total of 11 attacks, resulting in one death, all against immigrants or persons of non-Swedish appearance. On 5 April 1992, the Iranian embassies in nine countries were simultaneously invaded by rebel group members in opposition to the government of Iran. The Swedish embassy was one of the multiple sites attacked. Approximately 50 protesters set fire to two buildings and six cars in Stockholm associated with the Iranian diplomatic core. The ambassador's wife and children were treated for shock, but no one was killed. Swedish security officials arrested 21 persons connected to the event. 1999 ended with a peak of activity in the summer, with two incidents purportedly involving neo-Nazi groups. Peter Karlsson, an investigative journalist, and his son, were injured during a bombing of their car on 28 June in Nacka. Karlsson had been researching the activity of the neo-Nazi group, the Ariska Bordraskapet ("Aryan Brotherhood").[230] Less than a week later, two policemen suffered several injuries when investigating a stolen car that exploded when they approached it.[231] This crime were attributed alternately to either another neo-Nazi group, the Nationalsocialistick Front (NSF), or the Hells Angels.

Altogether, while these events were certainly disturbing and disruptive, **they did not represent a larger pattern of security risks endemic to the entirely of Swedish society, there was little need for increased law enforcement access to data.** There were a total of 39 persons injured, and 13 deaths from terror-related attacks between 1970-1999. The mean casualties were 1.79 per year. As the total population of Sweden during this period was a mean of 8.4 million persons, one can conclude that security fears were not a high risk factor taken under consideration by Swedish policy-makers when addressing data governance.

[230] Nordic Business Report 1999
[231] Younge 1999

4.1.3 Digital Human Rights

In states with a more active legal and academic elite pushing for more codification of human rights, we should see an increased attempt at identifying and protecting data within the human rights policy umbrella. To evaluate this, I looked at the roots of Swedish data law and the roles given to various jurists, judges, and academic faculty, during consultation with the Riksdag in the years prior to and during Phase 1. In the case of Sweden, record-keeping practices by the government were particularly impactful.

Swedish society has a precedent of over two hundred years of open access to information collected by the government, or what Anderson calls the "principal of public access to official documents."[232] This practice dates back to a change of party in power when the the "Caps" (*mössorna*) party won control of Parliament in the 18th century. Following the takeover by the Cap party, their government pass the Act of 1766 to reverse censorship practices by the prior party in power, the "Hats" (*hattarna*). Importantly, freedom of access was coupled with norms of avoiding secrecy by government actors. Since that point in time, the press (and thereby the public) have enjoyed legal access to government files.[233] This purposive reversal of censorship opened the door for the population to expect the Swedish government to be transparent on how it was doing business. No core changes were made to this policy during the 19th or 20th centuries, though minor revisions were made to access and secrecy laws in 1810, 1812, and 1949.[234] The revisions continued to support public access, expanding it to local government files in 1937, although granting local officials the right to appeal given particular grounds.

[232] S. V. Anderson 1973, p. 420.
[233] S. V. Anderson 1973
[234] S. V. Anderson 1973, p. 422.

The Swedish population continued to grant freedom of collection to the government regarding private information in the late 20th and early 21st century, as long as was held in check by public access to whatever records were obtained. This included supportive attitudes to the addition of a personal identity number system, which was given in 1946 to every resident. Similar to, but more comprehensively utilized than the U.S. social security number, this number was assigned to Swedes from birth to death, and was an identifying tool attached to all documents, legal and commercial, regarding all individuals. As an example of the ongoing expansion of Swedish governmental record-keeping, in 1968, the tax-payers' registry was given permission to computerize record-keeping on all taxpayers. The taxpayer's registry accumulated data on 6.5 million people, using local manual sources of records on the population, and computerizing all data collected for tax purposes.[235]

The government kept monitoring application of the access laws as time progressed, creating a Publicity Committee (*Offentlighetskommitté*) in 1960, that issued a report in 1966 to the Ministry of Justice on recommended practices for the future. The formation of the research committees designed is crucial to how the Riksdag approaches revision of past laws or formulation new laws, and this practice is integral to the argument of this dissertation. Committees typically include civil servants, legal officials or jurists, members of the press, and academics.[236] The specific composite mix of advisors on the 1960 Publicity Committee used their legal professional perspectives to inform the types of recommendations made for multiple laws that impact information policies, including the 1937 Secrecy Act, the 1973 Credit Act, and the 1972 Data Act which was to come. Member of the Riksdag and the civil service were heavily slanted toward a background as lawyers, judges, and/or academics.

---

[235] Flaherty 1989
[236] S.V. Anderson 1973, Flaherty 1989, Fuster 2016, Ilshammar 2007.

The general feeling amongst the members of the Swedish Parliament (Riksdag) was positive and supportive of expanding the use of computers and data management for government purposes.[237] The public sector's role as "early adopter" cannot be overstated. Colin Bennett (1992) notes that as early as 1963, the Swedish government was collating databanks for population registration, land records & automobile records, and social services, all under the management of the Central Bureau of Statistics, or *Statistiska Centralbyran* (SCB).[238] In addition to government attempts at collecting data and harnessing data banks for bureaucratic purposes, the private sector saw adoption of computerization to be part of wider goals to rationalize trade and industries in order to improve the economic bottom line. [239] A few officials within the bureaucracy did express some reservations. Minister of Justice Kurt Hugossen worried that local housing authorities' records were increasingly being tapped for commercial purposes, as businesses used the records for marketing and advertisement canvasing.[240] Despite this, use of computers to collect, organize and store data moved forward, as it was largely seen as a part of improving oversight into government actions, an attitude which has been firmly entrenched in Swedish society for centuries. Only in the very late 1960s, did a debate emerge around data collection and treatment, centered on several factors related to computerization of data.

The public was largely unconcerned about data collection by the government until the census records were scheduled to be updated in 1970.[241] The proposed 1970 Housing and Population Census became the trigger for a larger debate on data treatment. People expressed concern over the exponential effect of data appropriation that would be possible with centralized

[237] Ilshammar 2007
[238] Bennett 1992
[239] Johansson 1993, p. 63-80.
[240] Ilshammar 2007
[241] Census data was collected in Sweden every five years. Prior censuses had occurred in 1960 and 1965.

and computerized data banks.[242] Particular fears swirled around the potential for personal records from the Census being linked and matched to other types of governmental records, reversing the anonymity related to non-Census record collections. Additional fears related to the difficulty in correcting false information once data was logged into a large, government computer network. Lastly, public apprehension about the Census was matched by increased hesitancy on the part of parliamentary officials to adopt a computerized census model without further debate. The Riksdag responded to the public concerns by delaying the collection of the 1970 Census, and instead created another advisory board to investigate the potential for data breaches to privacy and anonymity that might occur as a result of adopting computer-based data management, rather than traditional paper records for the Census. As referenced in the economic hypothesis section for Sweden, the late 1960s and early 1970s were a turning point for increased demands in accountability by voters toward policymakers; this included the desire for more responsive turns to fears about governmental record-keeping.[243]

In January of 1969, two members of the RIksdag (Kaj Björjk and Kurt Hugosson) introduced bills that concerned citizens' rights to privacy. Both MPs wanted parliament to address the potential for violations in privacy regarding already existing legislation, such as the Secrecy Act. The government established the Committee on Publicity and Secrecy Legislation (*Betänkande av Offentlighets- och sekretesslagstiftningskommittén,* or OSK) in April 1969.[244] The findings and suggestions made by the OSK would have a huge impact upon Swedish data legislation, laying the foundation for the types of laws and oversight the state and the public would expect.

---

[242] Bennett 1992, Ilshammar 2007.
[243] Magnusson 2000, p. 255; Ilshammar 2007, p. 23
[244] Ilshammar 2007, p. 23.

First, the OSK committee was comprised of intellectuals with a combined background of expertise in legislation, statistics, public administration, ministry of justice bureaucracy, and legal academic faculty. The committee consisted of Erick Adamsson (parliamentary council chairman), Allan Eriksson (philosophy academic), Jan Freese (court of appeals lawyer, Assistant Secretary of the committee), Hans-Olaf Hansson (actuary), Kurt Hugosson (parliamentarian), Sven-Erik Larsson (former farmer, now career parliamentarian), Karl-Olof Lidin (assessor), Åke Polstam (parliamentarian), Edmund Rapaport (statistician), Kent Skoog (consultant), Hans-Olov Stark (ministry of justice), Erik Svedberg (parliamentarian), and Per Svenonius (public management expert). According to Dr. Lars Ilshammar[245], academic and national archivist who conducted extensive interviews with many of the OSK members, the committee had a two-fold mandate. They were charged with making proposals for how individuals' privacy could be protected whilst simultaneously allowing for the Swedish norm of public access to records. The task was challenging to say the least. The public concerns were represented in the committee by several parliamentarians, who together came from four of the five parties holding seats in the Riksdag at the time. The Chairman was Rune Hermansson, a Social Democrat, with prior experience as a judge of appeals, and a minister with the Department of Justice between 1960-1966. Under Hermansson's leadership, the OSK was able to present an initial report to the Minister of Justice Lennart Geiger by June 1972. The OSK recommended revisions to the current Freedom of the Press Act, but the core of their suggestion was the creation of an entirely new data act, and importantly, a new governmental agency which could serve as the supervisor of records management for computerized data. I argue that this report served as a critical juncture for Swedish data policy, laying the foundation for digital human rights in Sweden.

[245] Ilshammar 2007 p. 34.

The Data Inspection Board (DIB, XXX in Swedish) was a novel approach to computerized personal data for several reasons.[246] First, the law set government, not the computer users, or private citizens, with the bulk of the responsibility for fair data treatment. Multiple scholars note the precedent set by Sweden for data legislation, which was followed by numerous European states[247]. By registering all databanks collecting personal data, the law would allow manual record-keepers to continue their current practices unchanged. The data aw regarding computer-based personal data would apply to both public and private databanks, making oversight the norm across all segments of professional computer use. Lastly, it was a first-point of use law, meaning that the government would be informed as to every existing and new databank holding personal data, and would be able to inspect practices on site, ensuring compliance once a databank was registered.[248] The OSK was suggesting a data law that would formally institutionalize personal data protection. The bill was presented to the Riksdag in February of 1973, and adopted on April 12, 1973.

The next step taken by the Riksdag truly solidified Sweden's pathway toward a policy of digital human rights. The Data Act of 1973 (*Datalagen*), was the first national law regarding data treatment in Sweden, and stated that its main purpose was "to prevent undue encroachment on individual privacy." [249] [250]Board members would serve four year terms, with a Director-General, as the head of the agency, chosen from candidates with judicial experience. Director-Generals and eight Deputy-Directors could serve indefinite terms. The DIB board would four legislators, someone form the major trade unions, one representative from major industries, a member from

[246] Bennett 1992, p. 161-170.
[247] Bennett 1992, Flaherty 1989, Fuster 2016.
[248] Bennett 1992, p. 161.
[249] Flaherty 1989, p. 93.
[250] There is no equivalent to the English word for "privacy" in Swedish. The law uses the word "integritet" – translated similar to the English "integrity."

the public administration, and researchers. All together this would include ten other board members outside of the Director-General, and all chosen by the Cabinet of the Riksdag. All databanks in Sweden holding personal data would be required to obtain a license upon registration with the DIB. Only the Riksdag itself was exempted from this requirement. The initial duties given the DIB through the 1973 Data Act were to license data banks, supervise compliance, and administrate. The new Data Inspection Board (DIB) was to be an autonomous agency given responsibility over how data was collected, from whom it could be collected, and concerned with the permission of the data subjects about whom the information was taken. As a result of this responsibility, the activities of the DIB encroached upon additional law compliance, such as that of the Credit Reporting Act, and the Debt Collection Acts.

The final aspect of the impact of particular actors upon the development of data protection as a human right in Sweden can be seen in the leadership styles of the DIB Director-Generals (DGs).

Table 7: Directors-General of the Swedish Data Inspection Board

Years Served in DIB	Name of Director General
1973-1977	Claes-Göran Källner
1977-1987	Jan Freese
1986-1989	Mats Börjesson
1989-1992	Stina Wahlström
1992-1998	Anitha Bondestam
1998-2004	Ulf Widebäck

From 1973-1983, the DIB largely focused on licensing databanks. After the law was revised in 1982, the scope of responsibilities expanded into supervision and on-site inspections. Källner brought his experiences as a legal expert to the DIB, having served as a court lawyer since 1955, as a minister of the Interior from 1963, and the Head of the Department of Civil Affairs just prior to his taking on the DG role at the DIB. Without doubt, however, Jan Freese,

who was the second DG in Sweden, led the country and much of Europe toward a digital human right framework for data protection since the 1960s. Prior to working at the DIB, Freese had been a court of appeals lawyer and judge from 1964-1973. At the DIB, he took a proactive role, often advocating for the importance of data protection and the agency with the media. In fact, Freese saw himself as a policy-maker, not just a policy implementer. Noting the lack of a word in Swedish equivalent to the English word "privacy", Freese argued that the spirit of the 1973 law essentially promoted, "individual's right to be left alone."[251] In 1978, Freese actually opposed a tighter reconceptualization of the word "integritet" in the proposed revision of the law, preferring to give the DIB more leverage on interpreting the levels of encroachment being perpetrated against data protection by registered data banks. He also actively opposed linking databanks from multiple agencies, stating, "The road to 1984 is paved with good intentions. Besides that, you can't compare apples and pears – two data banks could have different rules for collection, and then can affect the quality of information."[252] Freese advocated for data protection throughout Europe and globally during the 1970s and 80s, writing multiple documents and working papers regarding the topic, and appearing at data policy conferences.[253] Among Data Inspection Board Directors in Europe, Freese served the second lengthiest term of service in management capacity, second only to Spiritos Simitis in Germany.[254]

In 1986, Freese accepted a role as the Deputy Managing Director and Head of the Social Policy Department of the Swedish Industrial Federation, and the management of the DIB switched to Mats Börjesson. Börjesson served only three years from 1986-1989, focusing mainly on "guiding" the DIB through implementation of the 1982 Data Law revisions, rather than acting

[251] Flaherty 1989, p. 105.
[252] Wicklein 1981, p. 205
[253] Flaherty 1974, 1989; Ilshammar 2007
[254] Flaherty 1989; Fuster 2016.

as a policy innovator as had Freese.[255] In 1978, the Riksdag revisited the Data Law, wishing to address concerns on burdens of protection as relates to ”sensitive data” such as health problems, criminal history, etc., that may have inadvertently been exposed to public access as a result of the ambiguous wording of the 1973 law. A new advisory commission, the *Datalagskommittén*, or Data Act Committee (DALK)[256] looked at the exemption of government databanks from the general protection requirements of non-government facilities, and found that it was necessary to update the 1973 law to address sensitive data protections. DALK issued policy revision reports on a regular basis between 1976-1984. Suggested revisions in 1978 included protections for sensitive data, but the core areas of restrictions in the 1973 law remained the same. The most significant changes that occurred to the DIB in Phase 1 included 1982 changes to the licensure paperwork, making it more of a registration than a permission-seeking framework, and 1997 revisions to the Data Law, in order to comply with the 1995 Directive passed by the EU Commission (Directive 95/46/EC). None of the directors following Freese aggressively sought media exposure for the agency to the degree of Freese, however they did work with the Riksdag to influence proposed legislation that would impact their work with data protection. While many if not all had legal expertise similar to Freese (Wahlström and Widebäck were both court attorneys or legal consultants for the Riksdag), subsequent DGs kept the” status quo” of the DIB functionality, following the pattern of professionalization and civil service created by Källner, and sustained by Freese before then.

In the case of Sweden, there is substantial support for the idea that the legal exports chosen for regulatory committee research and as managers for the DIB have moved forward the agenda of digital human rights for Sweden.

---

[255] Flaherty 1989, p. 128.
[256] DALK Report on the Revision of the Data Act, *Statens offentliga utredningar* 1978: 54, pp. 340, 341.

4.2 Findings: The United Kingdom

Table 8: UK Data Laws (Phase 1:1970-1999)

Year	Name of law	Description	Total Coded Sentences	Text Analysis Scores	Net Score
1974	Consumer Credit Act	Individuals granted right of access to credit source information for correction purposes.	32	+4 Security -2 Security +1 Econ + 17 Data Protect - 8 Data Protect	+9 Data Protect + 2 Security + 1 Econ
1984	Data Protection Act	Regulates use of automatically processed personal data regarding individuals; designed to ensure compliance with CoEurope Convention 1981	191	+13 Security -4 Security +5 Econ +125 Data Protect -76 Data Protect	+49 Data Protect +9 Security +5 Econ
1998	Data Protection Act	Created new provisions for regulation of processing personal information; designed to ensure compliance with EU Directive 95/46/EC	464	+18 Econ -7 Econ +44 Security -19 Security +218 Data Protect -151 Data Protect	+67 Data Protect +25 Security +18 Econ

Source: www.legislation.gov/uk

The United Kingdom was the last of my case states to adopt data protection legislation (Sweden 1973, Germany 1977, UK 1984). A core barrier to developing data protection legislation in the U.K. lay in the lack of constitutional structure for human rights protections. More than any of the other case states, Britain also experienced a somewhat politicized approach to the topic, with political will regarding data legislation waxing and waning across time based upon whether the Conservative or Labour party held the majority in Parliament. Security fears involved both data security and the need for access to data by government security actors. Finally, data protection legislation was pushed through by a combination of private actors in the

legal sector, and the ICT business community, the latter motivated by its primary fear of market losses without such protections, the former by the need to protect the public from data privacy losses.

As noted by Bennett, one of the main hurdles for data protection legislation in Britain was the lack of a formal, written constitution.[257] Unlike the countries of Sweden, and Germany, both of whom had constitutional precedent that established a base set of human rights, the United Kingdom did not have such a document. In addition, the norms of privacy protection that exist in the German case due its history of oppressive Nazi surveillance simply did not exist in Britain.[258] Unlike Sweden, there was no established history of public expectations for government transparency about information collected on the population. Public access to data collected about the British public did not exist until an incident involving a Labour MP in 1982, an incident I will discuss in the next paragraphs.

I note in brief, that when computer technology advanced in the whereby personal privacy could be affected by actions taken during government overt or covert surveillance of the public, the U.K. had no foundation on which to build legislation for data protection or treatment as a whole. As a result, the process toward legislating data management was much more piecemeal, and driven by an odd combination of the legal community, academics, and the ICT sector itself. Politicians and law-makers were the last to arrive at the conclusion that such laws were necessary. As in the case of Sweden, it is crucial to trace the structural factors that contributed to the willingness by the Thatcher administration to finally submit a data protection law to Parliament.

---

[257] Bennett 1992, p. 82.
[258] Flaherty 1984

Prior to Phase 1, there had been a few scattered attempts at introducing legislation that would protect against information abuse by media and the government during investigation of the private lives of citizens. In the House of Lords, Lord Mancroft introduced an unsuccessful bill in 1961 to prohibit "… any unjustifiable publication relating to his private affairs and to give him rights at law in the vent of such publication."[259] On the House of Commons side, several individual attempts were made to introduce legislation. MP Alex Lyon attempted to be a catalyst for privacy protections by introducing a "Right of Privacy Bill" in 1967, but it failed to receive general support. Mr. Brian Walden initiated the "Privacy Bill" in 1969, which also died. The "Control of Personal Information Act" sponsored by Huckfield and Coombs in 1972 asked for the creation of a data bank tribunal to regulate and monitor personal information management. The bill did receive a second reading in April of 1972, but was defeated in 1973.[260]

While individual MPs were interested, broad political will to actually pass legislation on the part of the Labour government was non-existent. Though Britain did not have a plan to develop centralized databanks as in the case of Sweden, individual MPs were increasingly worried about the potential for abuse as computerized record-keeping grew in practice, and these MPs kept pressuring the Home Office to do something. Government responded to their concerns with the Justice Report *Privacy and the Law*, released in 1970, which did offer a draft Bill based upon Walden's Privacy Bill. The recommendations in the report were met with press opposition due to fears of serious restrictions to freedom of the press and speech.[261] The continued pressure by parliamentarians upon the Home Office to be proactive regarding information privacy

---

[259] Lord Mancroft, HL Debs., 5s., 13 march 1961, col. 607.
[260] HC Deb 21 April 1972 vol 835 cc967-1012, comments by Mr. Leslie Huckfield. HC Deb 21 April 1972 vol 835 cc967-1012. See also Price 1984.

[261] Dworkin 1973

legislation let them to call for an investigative body to research the issue further. The hope was that a compromise could be reached which did not impinge upon press freedom to perform investigative journalism on members of the public.

The Younger Commission, headed by Sir Kenneth Younger, first met in May of 1970, and initially looked only at the issue of privacy as relates to the public sector. (The Committee did include private sector concerns as well, after receiving feedback from various industries to expand the breadth of the evaluation). The committee was told to "consider whether legislation is needed to give further protection to the individual citizen and to commercial and industrial interests against intrusions into privacy by private persons and organizations, or by companies, and to make recommendations."[262] As a part of the investigation, a series of public opinion polls were conducted to measure the level of public support for privacy legislation. 38% of Britons considered privacy as important, 29% as very important, and 16% extremely important.[263] The Younger Committee Report on Privacy responded with a series of suggested measures, but disagreed in a 14:2 vote among committee members that the government should go so far as to propose a law codifying the "right to privacy." The majority in the committee did not want a prosecutable law that would require civil court officials to choose between an individual's right to privacy and "public interest."[264] The committee also feared that a bill to protect information privacy would unfairly restrain the press, a sector which had strongly opposed the idea of a privacy bill from the very start. Rather, the Younger Committee asked that the Press Council institute a voluntary code of ethics, and it called for a new Complaints Commission to accept and

[262] Younger Committee 1972, p. 1.
[263] *Report of the Committee on Privacy*, Cmnd. 5012.
[264] HL Debate June 1973, vol. 343 cc104-78, see also HC Debate 13 July 1973, Vol. 859, cc1955-2058.

examine public complaints regarding invasions of privacy during press investigations. Both instruments were subsequently rejected by the press.

The Younger Report offered ten principles for data treatment, primarily focused on the finance industry and data processing involving computers.[265] Personal information should be collected only for specified reasons, data access given only to those duly authorized, and data stored for a prescribed period of time. In addition, computer systems designed to manage statistics should anonymize data.[266] Credit agencies and banks received particular attention; credit reference information should not be released by financial institutions without the consent of the credit subject. In all of these sectors, monitoring security should be designed into the information systems to make "precautions against the deliberate abuse or misuse of information."[267] Data accuracy should be maintained. Lastly, they recommended a Standing Commission be appointed to "examine the use of computers, particularly for handling personal information." Heath's Conservative government agreed to establish the standing committee, but had no plans to legislate data protection as a result of the initial report. Much of the Younger Committee's suggestions were virtually ignored. The only suggestions that did become law from the initial report were those regarding credit information protections, enacted in the Consumer Credit Act of 1974.

During the early 1970s, the public continued to raise concerns over the intent of British officials to record and store personal information during a series of data collection events, some of which caused enough angst on the part of the population that the government did react. The format of the 1971 census in Britain resulted in the "biggest outpouring of public concern about

---

[265] Bennett 1984, p. 86.
[266] HC Debate 13 July 1973, vol. 859, cc1955-2015, comments by Secretary of State for the Home Department, Mr. Robert Carr.
[267] Bourn and Benyon 1983, p. 12, 13.

privacy ever witnessed in that country."[268] As the over 100,000 census-takers went throughout the country collecting data, people opposed participation by complaining of the invasive nature of questions regarding personal details such ethnicity, and the number of persons living per household. Some residents refused to participate altogether, a few lawsuits were filed, and an official investigation was launched to address census procedures.[269] Further public outcry arose from the formation of the Driver and Vehicle Licensing Centre in 1973; the Centre centralized over 33 million records on drivers in Britain.[270] Mr. Leslie Huckfield complained during the House of Lords debate over the Control of Personal Information Bill that the licensing center was just the beginning of public sector computerization of personal information record-keeping.[271] The Department of Health and Social Security were preparing to digitize social work paperwork, the National Police Computer kept criminal history records in databanks, and other databanks were housed by the Departments of Defence, Trade and Industry, and the Civil Service Department. Most troubling to members of the public and therefore to some MPs was the discussion over linking many of these databases, which would risk the further exposure of private information to individuals not authorized to see types of information from other state agencies. (MPs regularly mentioned fears of Nixon-like Watergate scandal, should data protection not be addressed by Her Majesty's government.[272] It would be left to the Labour government that came into office in 1974 to act upon the findings and recommendations of the 1972 Report.

---

[268] Bennett 1982, p. 52.
[269] Magwick and Smythe 1974.
[270] Bennett 1984, p. 48; Warner and Stone, p. 105.
[271] C Deb 21 April 1972 vol 835 cc967-1012, Order for Second Reading.

[272] Comments by Mr. Robert Carr, HC Deb 13 July 1973 vol 859 cc1955-2058

As mentioned, the only distinct action taken by the government was to establish a standing research committee on the topic. The Lindop Committee, led by Sir Norman Lindop, met beginning in July of 1976, and met over 50 times in the next two years. Much of what the committee addressed concerned how to define many terms which had not been addressed in the Younger report, as well as to outline the scope of protections needed by the government. Data privacy was identified as, "the individual's claim to control the circulation of data about himself."[273] Their first report, released in 1978, called for legislation that would create a Data Protection Authority, which would then implement codes of behavior for data treatment, including "collecting, processing, and storing personal data on computers" based on "fair information principles."[274] Unfortunately, the issue was politicized again, as the Labour government asked for additional input by the IT industry; the Lindop Committee generated a list of 250 organizations and asked them for feedback. When Labour lost control of the government through a no-confidence vote in 1979, and Thatcher's Conservatives were elected in 1979, they delayed action again, finding the Lindop suggestions suspect, being instigated by a Labour initiative.

As several scholars point out, civil liberties groups continued to apply the pressure to the Home Office to write a data protection law throughout the 1970s.[275] The Home Office Secretary responded in 1981, indicating the government had no intentions of acting on legislation, arguably caught between its dual mandates to act as protectors of justice (Ministry of Justice) yet also serving to protect national security (Department of Interior).[276] Only links between the concerns of the private sector, and U.K. membership in the Council of Europe combined together

[273] Bourn and Benyon 1983, p.14?
[274] Bennett 1992, p. 90.
[275] Bennett 1992; Bourn and Benyon 1983; Fuster 2016
[276] Bennett 1992; Bourne and Benyon, p. 25; Cornford 1981

provided enough of an incentive to change the collective mind of the Thatcher government. In 1981, the Council of Europe held a meeting specifically to address data policy: the Convention for the Protection of Individuals with regard to Automatic Processing of Data ("Convention 108"), which concluded in a treaty open for signatures by all member states.[277] The treaty outlined several recommendations for member states that would set data protection for automatically processed personal data, and codify this within legal systems that would protect storage and use of such data. This protection should simultaneously allow for data transport across state lines during business transactions, a matter of concern for the rapidly developing ICT sector of several Council of Europe and OECD member states.

In fact, the U.S. had pushed the initiative throughout the Convention in order to benefit the growing ICT sector in the country. Britain had signed the treaty. When 1982 was declared by the Thatcher government to be the "Technology Year" as an effort to play catch up with U.S. gains in the ICT sector, British ICT firms joined human rights activists in pushing the government to finally act on the issue. In fact, they feared profit losses if they were unable to reassure other European firms and governments that the minimal requirement set by Convention 108 were being met and monitored by the British government. Finally, the issue was framed in a way that the economic policy and trade-focused Thatcher government could embrace. Timothy Raison, Secretary for the Home Office, announced a forthcoming White Paper which would explain the government's intended legislation.

The White Paper of 1982 did address data protections, but in reality, followed none of the core suggestions made by either the Younger or Lindop Committees. Instead of a permanent agency to act as a Data Protection Authority (DPA), the paper suggested a registry be created for

[277] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108

personal data banks, to oversee the cataloguing of computers processing personal, non-anonymized data.[278] A bill was formally introduced in the House of Lords in December of 1982, and received a second reading in January of 1983, but was unable to pass through both sides of Parliament before the May break. It was again introduced and passed in the Lords in June/July of 1983, and taken up by the Commons in January of 1984. The bill passed with a vote of 226 to 104 at that time, securing according to Gerald Kaufman, "... the absolute minimum the government can get away with."[279] The wording angered civil liberties groups, as it provided no protections for manual (paper-based) data, and it allowed for cross-border data transfers. Despite these weaknesses, it was the first data protection law of the United Kingdom, and its success was due to a mixed alliance among the "… business community, the trades unions, the consumers' associations, the computer industry, the medical and other professions, and the civil liberties and human rights interests…"[280]

I now turn to explain how each of the three major factors (economic commodification, security, and human rights activism) contributed toward the 1984 law and the subsequent 1998 revision.

4.2.1 Economy

Britain's economic history is first understood by the evolution of industrialization and technological change in the state. First-mover advantage took place during the age of industrialization in the 18th and early 19th centuries, and Britain adopted textile processing for cotton and British inventors created steam engine power and other mechanized improvements that increased labor efficiency. By 1851, the country was one of the world's largest exporters of

[278] Bennett 192, p. 92.
[279] Gerald Kaufman, HCDebs, 6s, 30 January 1984, col. 43.
[280] Bourn and Benyon p. 32.

manufactured and commodified goods, including textiles, engineering products, steam engines, coal and iron.[281] Unfortunately for Britain, it was unable to maintain this advantage, and by the 20th century was obtaining much of its advanced technology from other states, as the Fordist mechanisms adopted in the early 1900s were not adaptable to ICT product and service diffusion in the latter part of the century.

Regarding economic policy prior to Phase 1, during the interwar years, the country functioned as "managed economy" whereby free trade policies gradually shifted toward protection policies, including general tariffs on manufacturing in the 1930s, cartels and foreign investment controls in the 1930s, which also led to abandonment of the gold standard in 1931. Following the end World War in 1945, during the "Golden Age of European economic growth", the U.K. went its own way, as the government chose not to adopting the corporatist strategies used in the Scandinavian states or Germany. Instead of using collective bargaining to facilitate wage restraints, British leaders chose to subsidize failing industries, incentive technology invention, not diffusion, and keep owners and industrial controls separate. By the 1980s, the U.K. was experiencing unemployment levels similar to the depression years of the 1930s, matched with decreased in production from 9.3% in 1963, to 1.2% by 1986. The Thatcher government had to significantly reform fiscal, economic, and trade policy to privatize key industries, and reduce the "propping up" of outdated sectors to improve competitiveness sin the global market.

To assess the contribution of the ICT sector upon the economy, it was necessary to compare this sector to the contributions to GDP growth made by more traditional sectors. Primary sector indices reveal slow growth or contraction from 1964-1979 (agriculture in

[281] Cambridge Economic History of Modern Britain, 2014

constant prices grew from 55 to 71.93; mining contracted from 187-109.2).[282] In the secondary industries, manufacturing grew (72.6 to 90.6) faster than did construction (65.9 to 69.4). Only the tertiary industries saw significant positive changes; post and telecommunications more than doubled from 30.6 to 59.7, and financial and intermediate industries grew from 27.6 to 59.6 during the same period. GDP during this period grew from 58.7 to 76.5 by 1979. Production as a whole gained from 62.6 to 87.6.

Adding complexity to the environment of mixed output growth, the exogenous shocks created by the OPEC output restrictions of 1973 and 1979 led to reductions in demand on car-related products. This motivated the U.K. to develop and expand its oil extraction capabilities in the North Sea. A "petrocurrency" environment emerged, whereby the value of the pound was correlated with oil prices. This was both good and bad, as rising oil prices added the value of the pound for investors, but falling pound prices encouraged more exports by UK manufacturing products. Keeble (1989) notes that even during economic decline years such as the early 1980s, aggregate decline in technology employment fell much less than did traditional manufacturing (-7.7% compared to -27.7%, between 1979-1986.[283]

As growth in technology industries cooled in the U.S., U.K. firms stood ready to fill some of the worldwide demand for ICT goods and services. Between 1977-1984, high-tech manufacturing grew 46%.[284] Computer services grew 48%, and electronic data and computer processing equipment grew 23%. [285] This in turn created significant demand for high-skilled staff; high-skill workers expanded 24% to make up 55% of the work force between 1978- 1984,

[282] Source: ONS *Annual Abstract of Statistics,* 2010, "UK Growth Across Time," Chapter 1, p.4.
[283] Keeble 1989, p. 153-155.
[284] Buchart 1987 (Butchart 1987)
[285] Keeble 1989, p. 155.

while unskilled labor shrank 19% to comprise 22% of the work force in 1984.[286] Furthermore, exponential employment opportunities occurred among startup firms in ICT; 99% of net growth in employment between 1980-84 occurred in companies with fewer than 50 employees, formed after 1975.

Looking at the data on contribution by ICT to the British economy, using the four variables of measurement also used for Sweden, we see confirmation that ICT goods and services were increasingly an important portion of the U.K. economy.[287] ICT services exports comprised anywhere from 23-32% of exports, investment in ICT supplies few from 13.95 to 27.18% of capital formation, high tech exports increased from 24.74 to 29.92%. Similar to the case of Sweden, insurance and financial services firms experienced the most volatility in growth; they contributed 20.88% in 1986, fell to 13.34% in 1991, then grew again to 24.65% by the end of the period. All four measures ended the period at levels higher than when data first became available in 1985. (See next page for table.)

[286] Kelly and Keeble 1988

[287] Note, unlike Sweden, data availability for these variables for the U.K. economy begins in 1985, which does limit the ability to track long-term trends. After an exhaustive search for alternative measures for this country, these variables were again the most consistent measure of ICT contribution, also allowing for comparison to the other case countries.

Table 9: ICT Services Sector Contribution, United Kingdom, 1970-1999

Year	ICT Services Exports, % of services exports	Investment in ICT Supplies, % of total non-residential gross fixed capital formation	High Tech Exports, % of manufactured exports	Insurance & Financial Services, % of commercial services exports
1985	*	13.95	*	*
1986	23.47	15.60	*	**20.88**
1987	*	15.80	*	17.56
1988	*	15.93	24.74	16.91
1989	*	**16.18**	**25.20**	14.75
1990	*	15.93	23.61	**16.43**
1991	25.08	18.21	24.65	15.34
1992	**26.31**	18.51	23.59	15.78
1993	24.85	19.06	**25.97**	16.74
1994	26.35	20.82	25.70	17.28
1995	25.12	22.98	27.03	17.53
1996	27.65	**25.12**	26.69	19.18
1997	27.83	23.85	27.09	**22.12**
1998	**32.56**	25.58	28.68	20.06
1999	30.26	**27.18**	**29.92**	**24.65**

I expected that states with large-scale economic dependence on ICT firms will likely pass economic commodification polices (i.e., national institutional regime) protecting the use of personal and/or cyber data for profit. There is **considerable support for this prediction in the case of Britain.** While the primary and secondary sectors continued to contract and/or plateau, ICT goods and services followed an overall growth pattern during Phase 1.

4.2.2 Security

To test the impact of national security threats in the U.K., I again measured the frequency of domestic terror attacks during Phase 1, using data from the Global Terror Database (GTD). Table 10 provides an overview of the frequency of conventional security incidents in Sweden during Phase 1.

Table 10: Security Incidents, United Kingdom, 1970-1999

Year	Fatalities	Injuries	Casualties
1970	20	1	21
1971	110	1	111
1972	368	223	**591**
1973	210	275	485
1974	235	329	564
1975	245	129	374
1976	264	19	283
1977	103	17	120
1978	81	113	194
1979	133	146	279
1980	78	92	170
1981	86	118	204
1982	95	152	247
1983	77	186	263
1984	69	249	**318**
1985	64	175	239
1986	63	80	143
1987	104	120	224
1988	372	276	**648**
1989	66	174	240
1990	76	123	199
1991	88	235	323
1992	94	453	**547**
1993			0
1994	66	177	243
1995	11	5	16
1996	14	395	**409**
1997	23	35	58
1998	46	259	**305**
1999	7	161	168
Total	**3268**	**4718**	**7986**

Among my case countries in Phase 1, the U.K. experienced the most catastrophic and consistent attacks upon domestic security. The Troubles years (1968-1999) of internal conflict within Northern Ireland shaped the national debate on terrorism and national security not only during that time, but since that period. While it is beyond the scope of the dissertation to

perform a thorough explanation of the causes and implications of the conflict, general patterns that occurred during the Troubles can be used to test Hypothesis 1b.

Northern Ireland enjoyed home rule from 1922-1972, with the Unionist Party forming government outside of Belfast at Stormont, based upon the social power held by Protestant fraternal groups. Catholic disenfranchisement was assured via gerrymandering, and social subjection practiced through housing discrimination and denial of various cultural rights.[288] Scholars and journalists cite the protest by Catholic populations in 1969 over voting rights discrimination as the catalyst for political contention that subsequently occurred. The Irish Republican Army split from the Official IRA party in 1969 over strategies of enhanced violence to promote political concessions from Westminster.[289] When the local constabulary was unable to manage the violence that escalated by Catholics and Protestants, British troops were sent in to settle the unrest from that point.[290] While civilian deaths began at that point, the first British officer wasn't killed until February of 1971, when shot by the IRA.

Looking at the data in Table 10, peaks in violence and casualties occurred in the years of 1972, 1984, 1992, 1996, and 1998. Each of these peaks contributed to the perceived need of U.K. security and government officials to monitor the activities of the IRA through surveillance and information gathering. Data is needed for surveillance and prevention of attacks. During a civil rights march in Londonderry on "Bloody Sunday", 30 January 1972, 13 civilians were shot by the British Army, and dozens more injured (this was the single most violent event during the early 1970s). The U.K. government responded to the increased violence by dissolving the self-

[288] http://www.theirishstory.com/2015/02/09/the-northern-ireland-conflict-1968-1998-an-overview/#.W7vZbi2ZO1s
[289] Bamford 2005; Telegraph U.K.; Washington Post 1998.
[290] Bamford 2005

rule Stormont Government, and instituting direct rule from Westminster. This event served as a critical juncture for U.K. security policy in the region until the 1980s.

Between 1972 and 1984, civilians and military casualties occurred, with various incidents taking place during which government troops or high-ranking officials become targets of IRA violence. Christopher Ewart Biggs, the British Ambassador to Ireland, was murdered by a car bomb in Dublin, July of 1976. In 1979, Airey Neave, an advisor to Prime Minister Thatcher, was killed by a car bomb as his car leaves the Houses of Parliament in March. Prince Charles' godfather Lord Mountbatten was killed by a Provisional IRA bomb exploding in his boat in Sligo in August of 1979. Finally, the Grand Hotel in which PM Thatcher was staying was hit by a bomb in October of 1984. Each of these incidents involved a high-profile target associated with the government in Britain.

The explanation for the peak figures lay in several factors that explain surges of violence by actors on both sides. First, the British army instituted counter-insurgency tactics following Bloody Sunday. Meanwhile, opposition forces splintered into several IRA factions, with the most extreme "Provisionals" bent on achieving full island independence from Britain by forcing them into compliance by means of extreme violence. Additional violence took place between rival factions of IRA groups, which targeted one another. Loyalist paramilitaries killed over 300 Catholic civilians during the mid-70s, and expanded their bomb attacks to areas outside of Londonderry and the Northern Irish border. The British attempted to de-escalate tensions between the Northern Irish and the British army; an "Ulsterisation" policy returned control to the RUC (local) police. Secondly, the government created an internment without trial policy for paramilitary activists, as a way to by-pass traditional legal outlets for accused attackers, and to "speed up" the justice process, thereby raising the cost of violence against the U.K. government.

Imprisoned loyalists called hunger strikes resulting in the death of approximately 10 republic prisoners. Third, during the 1980s, IRA leadership changed hands, the IRA moved targeting to British soil in some cases, and the Crown aimed to target IRA fighters and avoid civilians. The overall casualty rate of the 1980s decade was lower than during the 1970s. Finally, a provisional ceasefire was declared unilaterally by the Provisional IRA in 1994, broken in 1996 with a mass bombing in London, but reinstated in 1997. Talks eventually resulted in the Good Friday, or "Belfast" Agreement of 1998. The terms have maintained an overall peace in Northern Ireland ever since.

Parliamentarians discussed security implications of the proposed data legislation during the Troubles, especially during the 1980s when the new data law was being debated in Parliament. In April of 1983, Mr. Whitelaw argued in the House of Commons that the Official Secrets Act cannot be skewed within the wording of the new data law to provide,

> *"…a data subject with access to his file, where the file relates to police suspicions about his criminal activities, would be nonsense…we all believe in the protection of national security."*[291]

Michael Meacher, who had suffered personal embarrassment when his medical records were obtained and printed in a news story carried by *The Sun*, countered the idea that information access even by law enforcement is innocuous, saying,

> *"We all know that police information—after all, the police are fallible, like us all—can often be irrelevant, out of date, incomplete or inaccurate and that the unchecked circulation of such material can often be extremely damaging."*

In other words, Meacher argued that individuals should have a measure of control over

[291] Whitelaw and Meacher comments, HC Deb 11 April 1983 vol 40 cc553-628.

data that police or law enforcement collect about them. In the House of Lords, Lord Gardiner protested the already free access to personal information by security personnel of information, indicating it was already a privacy invasion when this information was released to non-authorized parties. Gardiner stated during a July 1983 debate,

> *"... there was close contact with police officers at local stations and the practice of exchanging mutually useful information had developed on a quid pro quo basis. The police denied this statement categorically, and in a Home Office answer to a Parliamentary Question this denial was maintained: 'Any suggestion that the police give facilities to debt collectors and private investigators is quite without foundation.' We were assured by the police that the sources of information for private detectives were not police sources."*[292]

In the end, the 1984 law was subsequently passed to include some restrictions upon law enforcement's use of personal information, but still making much more provision than did Swedish laws for information access when pursuing matters of national security. Despite the reduction in Northern Irish violence during the mid 1980s, and the signing and keeping of the Good Friday Agreement in 1998, the 1998 updated version of the data law tripled the power given to security or law enforcement regarding access and use personal and cyber data. **As a result, there is support for data securitization in the case of the United Kingdom.**

4.2.3 Digital Human Rights

In the United Kingdom, the impact made by legal and human rights experts upon data legislation changed across time, but these individuals did not have the same level of influence upon data governance as their counterparts in either Sweden or Germany. Even with public complaints about information collection and digitization in the early 1970s, the British

[292] Lord Gardiner comments, HL Deb 06 June 1973 vol 343 cc104-78.

population was originally less concerned with data protection as a topic than were their Swedish counterparts.[293] This opinion did change across time; in 1972, only 16% of Brits felt that privacy issues were "extremely important", but by 1987, the figure had risen to 73% of the public which felt that privacy issues were "very important."[294] Unlike the German case to follow, British citizens had not suffered under a totalitarian regime, causing the public to be highly sensitive to information surveillance practices of the government. Each time the public did express reservations about increasing powers of data collection or data-sharing across agencies, the official government response was to establish investigative committees that would report to Parliament, who would then respond with a decision on the necessity and scope of any subsequent legislation. Therefore, testing the contribution of legal and academic elites involved a hard look at the power and activities of the Younger and Lindop Committees.

The first official British government efforts to address privacy in the computer age was through the release of the Justice Committee report *Privacy and Law* in 1970. This followed the failed efforts by various MPs to introduce and pass a bill protecting personal data privacy.[295] This initial report offered a draft bill based upon the previously failed bill introduced by Brian Walden in 1969. The draft argued that,

> *"each human being needs to able to limit the area of his intercourse with others… Above all we need to be able to keep to ourselves, if we want to, those thoughts and feelings, beliefs and doubts, hopes, plans, fears and fantasies, which we call 'private' precisely because we wish to be able to choose freely with whom, and to what extent, we are willing to share them."*[296]

---

[293] In 1976, Swedes ranked privacy of the people in the top 3 issues of concern. Source: Bennett 1992, p. 42, and "Public Attitudes to Data-Processing in the Information Society", English Summary of the Report from the Swedish Central Bureau of Statistics, Stockholm: Data inspektionen, January, 1985.
[294] 1972 statistics from Great Britain, Home Office, *Report of the Committee on Privacy,* Cmnd. 5012 (The Younger Committee); 1987 statistics from Data Protection Registrar, *Third Report*, London, HMSO, 1987, p. 40-45.
[295] Dworkin 1973
[296] *Privacy and Law*, 1970, p. 4.

The precise policy suggestions in *Privacy and Law* were not acted upon, however, at least the door was open for further discussion on data protection by Parliament and the government.

Next, the Younger Committee was created as a response to both Walden's rejected bill and the recommendations in the *Privacy and Law* paper. To pacify Walden for the blocking of the bill after by the Home Office after its second reading in the Commons, the Home Office had promised to establish the study group to evaluate the issue and report back to Parliament. Sir Kenneth Younger, who had previously practiced law from 1932-1939 was chair of the committee, and set the stage for future boards of inquiry established by future governments regarding the issue of privacy and data governance.[297] Younger had an extensive history in government service. He joined Parliament as the winning Labour candidate from Grimsby in 1945, and would later serve in the Foreign Office under PM Bevin in 1950-51. In the 1960s and 70s he was an advisor into legal and penal matters for the government. He acted as the chair of the privacy committee from 1970-76, during which he also a directorship of Chatham House – the Royal Institute of International Affairs research body. He died prematurely in 1976, just as he had been appointed to serve as chairman for the second research committee set up by Parliament regarding data privacy matters.

Under Younger's leadership, the Committee delved deeper intro privacy concerns than perhaps the Home Office had anticipated. The background of three of the Committee members undoubtedly shaped the approach by the committee to the issue. As stated, Younger had a legal background. So did Alex Lyon, the Labour MP from York, who joined Parliament in 1966. Lyon had supported British entry in the the European Economic Area in 1971, and was appointed by Wilson to serve as minister of state regarding race and immigration issues in 1974. Another

[297] Oxford Dictionary of National Biography, Sir Kenneth Gilmour Younger biography.

committee member, Lord Donald Ross, has been a legal advocate since 1964, and held positions such as Sheriff of Ayre and Bute in the 1970s, Chairman of the Judicial Studies committee in the 1990s, and retiring as Scotland's second most senior judge.[298] Voting with the minority in the committee which wished for a significant data privacy law, in a Parliamentary speech he argued that the major human rights conventions should inform British policy: "from the point of view of principle…" the UK law "should now be brought into line with these important declarations."[299] Both Lyon and Ross signed the dissenting, minority opinion that the Committee should have formally suggested a new law, and not only voluntary practices to protect personal data by the Press and others. Despite the fact that the majority opposed an actual law, the Younger Report released in 1974 laid the foundation for digital human rights protections through the suggestions of informational security, anonymity of statistical data collections, and the importance of data accuracy and monitoring by the government.[300]

The next body to undertake research toward the topic was the Justice committee, which fulfilled the promise made by the government to create an official White Paper in response to the 1974 Younger Report. The 1975 report *Computers and Privacy* (Cmnd). 6353) agreed with the Younger suggestion on legislation to restrain computer use of personal information, and the necessity of a permanent government agency responsible for database monitoring. The latter suggestion was another critical point in the path toward data protection; this new "Data Protection Authority" could ensure that safeguards over personal information were being followed by public and private sector computer users. Notably, MP Alex Lyon served on this

---

[298] *The Herald,* 12 February 1997, "Lord Ross warns that judges should stay out of politics; unease over crime speech" - https://www.heraldscotland.com/news/12077997.Lord_Ross_warns_that_judges__should_stay_out_of_politics_Unease_over_crime_speech/

[299] Kenyon 2016, p. 5.

[300] Bourn and Benyon 1983, p. 12, 13.

committee as well, as did Paul Sieghart, another influential jurist and human rights advocate that would shape British data policy in substantial ways during the 1980s and 1990s.

Finally, the government reached a place where in the early 1980s, it had received a tipping point of pressure by not only civil liberties groups, but also from the public, the computer industry, and persistent members of Parliament from various parties. A "Data Protection Committee" of ten persons, was established in July of 1976, under the leadership of Sir Norman Lindop. Lindop had previously worked as a Lecturer in Chemistry at Queen Mary University in London. Lindop's Committee was given stricter guidelines than were given to prior committees: address the concerns over computerized data privacy. Out of the ten committee members, the mix of professions included those with backgrounds in legal or academic professions, as well as the IT industry, the latter being a point of contention for civil liberties groups.[301] Professor James Durbin was a statistician who taught at London School of Economics between 1950-1988. John Hargreaves as an IBM executive. Dr. Charles Florey was the son of Lord Howard Florey, the discoverer of penicillin, and a public health expert in his own right.[302] Charles Read was the director of the Inter Bank Research Organization. Ken Potts held the Chief Executive post of the Leeds City Council. Professor F. M. Martin taught social administration at Glasgow University. Celia Good hart and Bridget Paton served in local government bodies. Sir David Pitblado was an auditor general. Hugo Young, a member of the press, wrote for the *Sunday Times.* Only Paul Sieghart had a background in privacy advocacy. Sieghart had a profound influence upon not only the Lindop Committee work, but subsequent Justice Committees, working tirelessly for various human rights initiatives throughout his career.

[301] New Scientist, "Protection for whose data?", July 1976.
[302] Interview with Professor Charles Florey, 17 February 1998.

Paul Sieghart, of Jewish ethnicity but Catholic religious heritage, fled Austria with his mother to live in England in 1939. After dropping out of a mathematics degree program at University College, London, he eventually chose to practice law until being rejected for a "silk" Queen's Counsel merit appointment by his fellow lawyers. He then switched careers to become a human rights author and advocate. As mentioned, Seighart served on the British section of the International Commission of Jurists, as well as the Justice and Lindop committees. He pushed the Home Office to appoint him to the permanent Data Protection Committee that was established after the 1984 Data Law was passed. A prolific author, he wrote titles covering international human rights, as well as issues discussing computers, technology, and personal privacy. Sieghart's perspective on digital human rights can be summed up with a statement made during an appearance at 1984 conference on data protection hosted by the University of Leicester.

> *"There are no harmless data. Or to put it another way, it is not the data that are harmless, it is what people do with them that is the problem."*[303]

The Lindop, or "Data Protection Committee" *Report on Data Protection* of 1978 had conducted surveys with over 300 organizations and individuals.[304] The report suggested several additions to the Younger Report of 1972, including needs to legislation that would be flexible enough to cover manual and digitised data which may evolve over time. It also suggested scope application to include public, and private sectors, with frustration expressed at the reticence of the police and secret services who "refused to answer any questions. After more police stonewalling the committee relied upon information uncovered by an investigative journalist to

[303] Bennett 1992, p. 35; Bourn and Benyon 1983.
[304] Warren and Dearnley 2005

explain applications over national security information-gathering. Seven broad principles were introduced, including:

- Data subjects should be informed on data collected about them, for how long it would be kept, and by whom it would be used.
- Personal data can only be used for reasons authorized by the data subject,
- Personal data accuracy should be maintained
- Users should only handle personal data in lawful interests
- The community should be protected from prejudice resulting from data access.

Though a new Conservative government delayed action when elected in April of 1979, as stated in the political history evolution of Great Britain, eventually the government acquiesced to pressure by the ICT industry itself, wishing the government to pass formal legislation to avoid risking loss of international business. The 1984 Data Protection Act was passed a full 170 months after the first government commission had been created regarding the issue of data protection.

The next successful data law passed in 1998, following a similar pattern: government reluctance, eventually submitting to international pressure by powerful organizations, and internal pressure from civil rights advocates and legal professionals. The 1998 Data Protection Act was largely in response to pressure from the European Commission. In 1995, the Commission adopted Directive 95/46/EC to signal regional compliance among EU Member States with the Council of Europe Convention 108, to which the member states had been signatories and many states had ratified.[305] The Commission had stipulated EU Member States were required to adapt their national data protection laws to the parameters of Directive 95/46/EC within three years of its passing. The U.K. balked at the demands of privacy being an actual "right" as this had not been codified into the 1984 law. The 1998 U.K. law did not add

[305] The UK ratified Convention 108 in 1987.

"privacy" as a protected right within the new law, but did agree in 1998 to have U.K. courts apply the rights within the ECHR, including Article 8 which indicated a right to respect for private life. The ramifications of the Commission demands will be discussed more in the next substantive chapter which examines the supranational policy process regarding data protection. Suffice it to say that the remainder of actions taken during Phase 1 provided little expanded scope of protection for data, other than those mandated by Directive 95/46/EC.

In the United Kingdom there is limited support for the idea that the legal exports chosen as consultants and parliamentary research committee members were able to successfully shape the 1984 and 1998 data protection laws. One could say that the laws were passed due to dual linkages between domestic rights activists such as Alex Lyon and Paul Sieghart, who championed the digital human rights being mandated by the Council of Europe (more economic in scope), and the European Union (included rights-based applications).

My next section will review the case of Germany.

4.3 Findings: Germany

The first law passed in Germany explicitly regarding data protection was the 1977 *Bundesdatenschutzgesetz* (BDSG), or the "Law on Protection Against the Misuse of Personal Data in Data Processing." The law was designed to protect against misuse of personal data that could be connected to a specific, physical person, during all phases of data use, including "storage, communication, modification and erasure…"[306] As pointed out by Professor Hans Peter Bull, one of the first German Data Protection Commissioners, data protection was a means to an end in Germany; the overall legal goal was to protect citizens against harm.[307] The first federal data law applied only to commercial data, and required data anonymization and use of

[306] Dammann 1977
[307] Flaherty 1989, p. 34.

data only for pre-specified tasks. It also required inaccuracies to be corrected, and once the original task was complete, the data should be erased. Violators could be punished with prison time.

Second only to the impact made by the 1973 data protection law of Sweden, Germany helped set the European standard for the legalization of personal data protection. As will be discussed further in the next chapter, German Data Protection advocates and Commissioners were frequently part of advisory committees and used for consultation in setting similar laws elsewhere across Europe during the 1970s and 1980s, during a time when data computerization raised fears over privacy loss across the region. To understand the evolution and impact of German data laws and the Data Protection Commissioners within Germany, it is necessary to trace the creation of laws at the regional, or *Länd* level, the laws that were passed for West Germany prior to unification, and the laws that applied to the united German state after 1990. See Table 11 (next page) for a summary of all national laws passed by Germany during Phase 1, as well as their coded intent.[308]

[308] For the remainder of this chapter, "Germany" will be used to refer to the federal level of governance that occurred in West Germany prior to 1991, and to the re-unified state after 1991.

Table 11: German Data Protection Laws, 1970-1999

Year	Name of law	Description	Total Coded Sentences	Text Analysis Scores	Net Score
1970	Population MicroCensus Law	Law permits some personal data release of information collected during the 1970 survey, for the use of correcting population registries, statistical use by central and Land authorities, for town planning, and for scientific use.	19	+7 Data Protect -5 Data Protect +4 Economy -1 Economy -2 Security	+2 Data Protect +3 Economy -2 Security
1971	Telecommunications Universal Services Act	Law outlining provision of telecom services, including voice telephony, rates for customers, and directory publications	2	+2 Data Protect	+2 Data Protect
1977	BDSG – Data Protection Law	First national data protection law, protecting against misuse during automatic processing.	200	+139 Data Protect -50 Data Protect +2 Economy +8 Security -1 Security	+89 Data Protect +2 Economy +7 Security
1983	Census Act	Discusses the protections required by the Basic Law, regarding personal data collected during the national Census. Also regulates the use of data collected for statistical and public administration purposes.	81	+58 Data Protect -12 Data Protect +5 Economy +3 Security -1 Security	+46 Data Protect +5 Economy +2 Security
1990	Data Protection Law Bundesdatenschutzgesetz (BDSG)	Revision of the 1977 law on federal level personal data protections. Includes details on responsibilities of federal Data Protection Officer, the mandates on data secrecy and transmission provisions, and right afforded to data subjects.	441	+259 Data Protect -117 Data Protect +34 Economy -4 Economy +24 Security -1 Security	+142 Data Protect +30 Economy +23 Security
1995	Broadcasting Act for North-Rhine Westphalia (	Addresses the licensure, functionality, and monitoring of broadcasting services in North-Rhine Westphalia. Includes specific protections for personal data of subscribers and their and personal viewing habits	62	+50 Data Protect -6 Data Protect +5 Economy -1 Economy	+44 Data Protect +4 Economy
11996	Telecommunications Act	Regulations regarding service installation, fee scheduling, environmental protection, and other aspects of telecom service provision. Also creates Regulatory and Advisory bodies.	81	+39 Data Protect -12 Data Protect +20 Economy -2 Economy +8 Security	+27 Data Protect +18 Economy +8 Security

1997	Telecommunications Universal Service Ordinance	Provision of public telephone equipment, as well as release of subscriber information, as long as subscriber has not barred release	2	-2 Data Protect	-2 Data Protect
1997	Digital Signature Act	Regulation of digital signature keys, including security measures and monitoring capability.	10	+9 Data Protect +1 Security	+9 Data Protect +1 Security
1997	Act on the Protection of Personal Data Used in Teleservices	Charges tele-services providers with protection of personal data during telecom service provision.	45	+37 Data Protect -3 Data Protect +4 Economy + 1 Security	+31 Data Protect +4 Economy + 1 Security
1997	Telecom Customer Protection	Various obligations of telecom service providers for billing, service and equipment provision	8	+5 Data Protect -3 Data Protect	+2 Data Protect
1997	Postal Act	Licensure requirements for postal delivery contractors. Law also discusses release of addressees' personal information and the protection of data used by commercial actors when sending postal content.	28	+ 16 Data Protect -3 Data Protect + 7 Economy -1 Economy + 1 Security	+ 13 Data Protect +6 Economy +1 Security

Sources: German Law Repository (University of Oxford), and Bundesgesetzblatt Online.

There are three factors that shaped the types of laws that emerged around data protection in Germany. These include a history of aggressive state surveillance, second, the types of challenges presented by a federal law-making structure, and last, the multiple stakeholders with interests in data policy outcomes.

First, the history of the state under the Gestapo mechanisms of the Nazis had led to a universal desire on the part of the German public for open accountability by central government authorities regarding data collected during surveillance of the public.[309] Similar to the other case countries, in the late 1960s and early 1970s, German public authorities wrestled with the decision to introduce regulations regarding computerized data banks used for public administration and by the private sector. Population statistics and general demographic data collection and use were permitted and utilized for civic planning and for scientific research purposes. All of the federal data protection laws that emerged during the Post World War II era rested upon the foundations

[309] Bennett 1992, p.5; Flaherty 1979, p. 141.

of the *Grundgesetz*, or "Basic Law." The Basic Law for the Federal Republic of Germany was enacted on 23 May, 1949. It served and continues to act as the basic constitution for the country. Within the Basic Law were provisions for fundamental human rights. "Human dignity shall be inviolable. To respect it shall be the duty of all state authority."[310] The Law also included outlines for the distinct obligations of the three branches and government, and constraints and responsibilities for the states, or *Länder*. Over fifty changes have been made to the constitution since 1950, but it still stands as the foundation for all federal laws, including those for data protections.

The scope of the normative culture of lawmaking in Germany aimed to balance two concerns: providing law and order on one hand, and setting limits for state use of personal information on the other hand. Data protection in the early years was seen as an extension of the core human rights protection for the "rights to a personality" or *persönlichkeitsrechte,* as there is no German concept for privacy encoded in the Basic Law.[311] Until the Constitution of 1949 was deemed inadequate to perform the task of protecting personality as it related to personal data use, little to no interest was shown by governmental or non-state actors to make laws specific to data protection. Since 1950 there have been a series of laws that gradually developed a national regime of human rights protections for personal and cyber data in Germany. The first law that indirectly affected personal data management was the 1953 Basic Law on Statistics. The statistics law allowed for use of data collection when needed to prepare federal laws and for use by the federal and *Länd* governments to effectively execute public administration. All data

[310] Grundgesetz, Artikel 1 (Basic Law, Article 1).
[311] Basic Law of 1949, Article 1(1); Bennett 1992, p. 1-2; Flaherty 1989, p. 22.

collected for such purposes was supposed to be protected for secrecy, but data dissemination among government authorities was unrestricted until the 1977 BDSG was passed.[312]

The identified need for more specific laws regarding data treatment gradually emerged with the diffusion of ICT adoption in the 1960s.[313] Bureaucratic efficiency via automatic data processing was hugely beneficial to society, and the escalating use of ADP by public and private actors was not correlated with public fears over privacy loss or data sharing amongst government agencies until later in the 1970s and 1980s.[314] In fact, another administrative law, the 1970 Census Law, permitted "widespread data dissemination under controlled conditions"[315] including use when correcting local population registries, for scientific research, and for local planning needs, as long as confidentiality was protected (data subject names were removed).[316] This permissive attitude was also reflected in the leverage granted public authorities to collect and disseminate individual data within the 1971 Law for Statistics on Higher Education. On the books these laws looked as if protection was extended over personal data, but in reality, the official Statistics Bureau had little power and no authority to enforce data confidentiality. The protections over personal data distribution lay entirely within responsibility of *Länd* authorities.

This split management over public governance between the federal and *Länd* governments added to the challenges of reaching national consensus on a federal data protection law. Some authority was held by federal authorities and the Bundestag (Parliament), while other responsibilities lay in the hands of *Länd* governments. In the 1960s, the *Länd* governments began to set up data centers for daily administrative planning purposes.[317] Hessian authorities instituted

[312] Flaherty 1979, p. 151.
[313] Riccardi 1983
[314] Flaherty 1974, 1989; Simitis, Spiros, "2 DVR 138 1973; Simitis, Spiros 1978
[315] Flaherty 1979, p. 153.
[316] Flaherty 1979
[317] Bennett 1992; Liedtke 1980.

the first data protection law in the world, albeit at the *Länd* level, rather than at the national level. The law applied to data use during automatic processing, and set up an independent Data Protection Commission to oversee application of the law. Rheinland-Pfalz followed suit in 1974 with a similar law.[318] Each of the *Länd* data commission offices were responsible for protecting automatically-processed data, and operated independently of national authorities, including the Ministry of the Interior, until the national law was passed in 1977. From the late 1960s until 1977 when the national law was passed, states bore the largest responsibility of evaluating the risks associated with personal data processing and storage. Once the 1977 law was passed, officials at both levels of government had to negotiate who would hold future responsibility over data protection.

Fears and gaps in agreement over the needed legal protection for privacy and personal data increased in the late 1960s, due to several factors. More and more databanks were being used to process personal data by public and private actors. The government use of personal identification numbers for public administration purposes led some to fear data breaches and unauthorized data linkages across large databanks, similar to the worries expressed by the British public. Finally, The Green party adopted the issue of data protection within its party platform alongside other non-material issues, such as environmental protections and civil liberties infringement, and began to challenge the national government to address the issue.[319] Meanwhile, settling what type of federal law would be necessary required solving disagreements among the various stakeholders involved with use of inter-federal data transfers. For instance, the ICT sector sought laws to cover manual files, in addition to computerized or automatically

[318] Bennett 1992, p. 77-90
[319] Bennett 1992, p. 74-82.

processed data. Otherwise, the ICT sector would be commercially disadvantaged by any new law that only applied to ADP processed data.[320]

The Bundestag requested general regulations on data protection in 1969. An interparliamentary working group was created, and subsequently submitted a draft proposal in January of 1970 for a "preliminary plan for the protection of privacy against the misuse of automatically processed personal data."[321] Brandt's SPD government did not prioritize laws specific to data privacy and protection until 1971.[322] The draft bill created by the working group in early 1970 was tabled until December 1971, despite having the support of the majority of political parties in the Bundestag.[323] Some raised concerns about the level of specificity in the law, which was much more detailed than the Hessian law. At this point, the judicial community, joined those pressuring the government for legal protections, a point I will return to when assessing the development of digital human rights in Germany. Though momentum was building toward passing a data protection law, the process continued to be fractious.

Public hearings on federal data protection in late 1972 resulted in industry and national administrators protesting the proposed law. It was a year later, on 29 November 1973, before another bill draft was presented to the Bundestag by the Brandt government, which pushed for a quick pass, but instead was met with opposition from various parties which asked for additional revisions. The Brandt proposed law was not only stronger than the *Länd* laws, it had weaker enforcement mechanisms. Bargaining continued throughout two more public hearings, a change in government leadership through Scheel (FDP Party) to Schmidt's Chancellorship (SPD), and a series of meetings on the topic by the Federal Interior Committee from 1974-1976, all in efforts

[320] Flaherty 1989, p. 22.
[321] Bull 1984, p. 104.
[322] Simitis, *Chancen und Gefahren der elektronischen Datenverarbeitung,* 1971.
[323] Federal Republic of Germany, Bundestag, *Drucksache*, 6/2885, December 1971.

to resolve the disagreements over the levels of stringency behind the law and the type of enforcement body that was needed to support it.[324]

Regional data protection advocates were called in to provide expert testimony on the type of control authority needed. Spiros Simitis, the Data Protection Commissioner for Hesse, strongly encouraged officials to choose an independent control authority, rather than utilize the self-regulatory model preferred by industry leaders.[325] The law had a second and third reading in the Bundestag, but the Interior Committee was continually displeased with wording of the draft. The CDU and CSU wanted the control authority to be under the umbrella of the Federal Audit Office, rather than operate an independent agency. *Länd* data protection agencies were also in an uproar over the bill, contending that an independent national DPC would threaten the rights of the *Länder* to oversee their own public agencies. The Joint Conference Committee designed a compromise in July of 1976, but the Lander were still displeased, and requested the committee to reconsider, which it refused. Despite CDU and CSU opposition, the Bundestag endorsed the bill on 10 November 1976; two days later it passed with formal opposition on record by Bavaria, Baden-Württemburg, Rheinland-Pfalz, and Schleswig-Holstein. The president signed the bill in January of 1977, and provisions took effect as of 1 January 1978. Although no one group was totally pleased with the final version of the law, data protection was legalized in Germany at the federal level.[326] In total, it took 39 months from the date of creation for the first government commission on data policy in 1973, to the making of an actual law in 1977.[327]

---

[324] Bennett 1992, p. 68-81.
[325] OECD 1976.
[326] Dammann 1977, p.70-107.
[327] Bennett 1992, p. 59.

4.3.1 Economy

Assessment of the outcomes of these policies and the contribution by the ICT sector requires a look at the West German economy prior to unification, and then at the unified state after 1991. The German approach to economic policy after World War II has followed the *Soziale Marktwirtschaft* model, combining decentralized autonomy for businesses with social protections for individuals.[328] This approach had historical roots in learned experiences during industrialization and the war years. The industrialization of the 18th and 19th centuries had produced multiple social problems that had not been adequately solved by the Marxist socialist system. The German ordoliberal economists in the Freiburg school of the 1930s directly influenced the response of German economic planners in the post war period, and up until today.[329] The ordoliberals observed the failure of Russian economic planners of the Soviet Republic to accurately predict and match production goals to current and future social conditions. On the other hand, while market-based systems produced greater economic opportunities than pure socialist systems, these economies failed to provide social protections for individuals in the event of market gaps.[330] The *Ordnungspolitik* plan called for institutional designs to inform economic processes. The German social market economy, therefore, was designed to rely upon three key goals: market conformity, defense of competition, and price level stability. Policy measures could be used insofar as the measures did not create levels of disequilibrium in the market that would warrant additional interventions. German economic policy would focus on defending the competitive order, provision of public goods, and prevention of monopolistic tendencies.

---

[328] Siebert 2005
[329] Mardellat 2011
[330] Berman 2006

West German policymakers after World War II achieved several important economic and trade goals. The Deutschmark was stabilized.[331] Produce markets were released from rationing in 1948, and prices allowed to fluctuate with market demands. GDP growth responded positively to the economic initiatives, with levels >8% from 1951-56, and again above 8% from 1959-1961. Admittedly, German economic growth was not consistently positive in the post-war era, given its exposure to the global economy. Germany suffered economic recessions facilitated by oil crises in 1973-1974, and again in 1979-1980. By the 1980s, GDP had fallen to 2%, and labor productivity was half of what it had been in the 1960s. West German trade policy was designed to encourage open markets and free trade, aside from subsidies to the coal and agricultural industries. The country joined GATT in 1951. From 1950-1970, the state pursued an aggressive export-led growth plan which relied upon low wages and production of high-tech engineered goods.[332] Exports increased throughout most of Phase 1, minus a slowdown after the merging of the two states in 1990.

Table 12: German Exports, % of GDP

1950	13.7%
1960	21.2%
1970	26.4%
1980	31.1%
1990	22.8%
2002	35%

Source: Siebert 2005

Export-driven growth eventually produced several challenges to the social market economy. Policy coordination in Germany relies upon corporatist bargaining between trade unions, firms, and government actors to set wage policies and adjust for market downturns that

[331] Siebert 2005, p. 12-14.
[332] Ahearn & Belkin 2010

negatively impact labour.[333] Unemployment in West Germany consistently rose after 1970, from a nearly full employment state[334] to some years having >10% of the working age population unemployed. Social welfare for unemployment provided up 67% of full-pay for an unlimited period for workers whose hours were reduced, actively de-incentivizing work-seeking. Fewer workers in production decreased growth further still during economic recessions. Despite these challenges, no political parties were willingly to promote the needed reforms which would require cutting taxes to reduce social spending when fiscal budgets were pressured.[335]

Suffice it say that the early to mid 1990s presented a challenge to the state as it merged two economies. Prior to unification the West German economy had price stability, a balanced budget, and a 5% surplus in current account. After December 1990, policy-makers set about privatizing the East German industries, and dealt with the challenges related to currency exchange between the Ostmark/DDM and the Deutschmark. East German currency was exchanged 1:1 with the Deutschmark, effectively quadrupling wage costs in East Germany, and making it less attractive to foreign investors. West German social benefits were immediately granted to East German residents, including early retirement and unemployment pay. This extension negatively impacted labor competitiveness in the east. Finally, to pay for the extended social welfare benefits to an additional 16 million people, government bonds were issued, which greatly increased government debt. Rather than reduce social benefits to any citizens, German policy-makers continued to pursue the dual goals of export-led growth alongside strong social welfare spending, and hoped that exports would offset the spending. I now turn to the role that high-technology firms in the ICT sector played in the German economy of Phase 1.

---

[333] Soskice & Hall 2013
[334] 0.7% of the population was unemployed in 1970. Source: Ahearn & Belkin 2010.
[335] Ahearn & Belkin 2010

As with the cases of Sweden and the United Kingdom, due to data availability, I primarily measured contribution of ICT to economic growth using two subsectors of ICT services: ICT services exports, and the insurance and financial services exports.

Table 13: ICT Services Sector Contribution, Germany, 1970-1999

Year	ICT Services Exports, % of services exports	Investment in ICT Supplies, % of total non-residential gross fixed capital formation	High Tech Exports, % of manufactured exports	Insurance & Financial Services, % of commercial services exports
1970	*	*	*	*
1971	15.17	*	*	*
1972	15.46	*	*	*
1973	16.22	*	*	*
1974	16.86	*	*	*
1975	17.11	*	*	*
1976	13.66	*	*	*
1977	13.90	*	*	1.16
1978	14.33	*	*	1.33
1979	14.16	*	*	1.27
1980	17.35	*	*	1.27
1981	15.17	*	*	1.32
1982	15.03	*	*	1.61
1983	16.16	*	*	1.51
1984	14.81	*	*	0.97
1985	14.33	*	*	1.06
1986	14.04	13.09	*	0.93
1987	15.04	13.36	*	3.44
1988	15.67	13.66	11.75	3.78
1989	17.94	13.79	12.38	3.62
1990	18.69	13.97	12.00	2.34
1991	20.49	13.76	13.10	1.01
1992	23.05	13.13	12.66	7.64
1993	23.06	13.21	13.43	8.26
1994	24.12	13.04	13.64	10.73
1995	26.76	13.29	13.71	12.17
1996	25.99	14.12	13.77	14.55
1997	27.74	14.44	14.65	14.80
1998	28.60	15.22	15.18	14.84
1999	28.50	16.47	16.49	16.64

Source: World Bank, World Development Indicators Database; OECD
* Indicates no data available for these years

Table 13 shows that the ICT sector has been an increasingly important portion of the German economy. Significant growth occurred in ICT services exports, which essentially doubled from 1971 to 1999. However, this growth was dwarfed by the rampant increases to

insurance and financial services exports, which rose from 1.16% to 16.64% of all services exports in Phase 1. No data is available from during the two recessions (1973-74, 1979-80) to determine what, if any, impact was felt by ICT firms regarding ICT investments and high tech exports. We do see a drop in insurance and financial services to 25% of prior levels in 1983. What is also noticeable from available data, is the reductions in growth for the ICT sector occurring around the timing of unification. Only ICT services exports managed to maintain upward growth from 1990-1994 without any down years. The other three variables show temporary retraction; insurance and financial services fell by over 50% in 1991, but quickly bounded back.

Economists noted that Germany, similar to most European states, lagged behind the U.S. and Japan for investment in R & D in the ICT sector during the 1970s and 1980s.[336] OECD analysts noted that one reason for this lag was the "insider system" of close relationships between firms and banks in Germany.[337]

> *First, to finance new industries, the financial system needs to facilitate the process of creative destruction This implies reallocating capital to new forms and new activities at the expense of declining ones…. Such a system differs from one primarily geared towards he accumulation of physical assets in large, stable firms in well-established industries, which were the basis for much economic growth in the post-war period.*[338]

A further challenge to Germany's ability to catch up with US first-mover advantage in the area of ICT development is due to the reliance upon mature industries such as steel and traditional manufacturing. Again, the OECD warned that for countries reliant upon such industries, economic adaptation occurs in increments, tied to knowledge accumulation and transfers. German investment in ICT remained consistent at around 13% from 1986-1995; even

---

[336] Australian Financial Review 1988
[337] OECD 2000
[338] OECD 2000, p. 33.

after this point, investment in ICT only reached 16.47% by the end of Phase 1. The level of investment built much more slowly in Germany than it did in either Sweden (15.04% to 28.8%) or the U.K. (13.95% to 27.18%).[339] Furthermore, in their 2000 report on the role of innovation and IT in economic growth, OECD analysts found that Germany relied much more upon use of others' inventions, contracting out of R & D, and purchasing of existing foreign tech firms, than did most of their OECD counterparts.[340] German firms were more reliant upon university research to facilitate adoption of advanced ICT, and as a whole fell back on developing "engineering excellence" since institutional incentives for creative measures did not exist. Between 1980-1996, the contribution of ICT to output growth fluctuated from 1.4% (1980-85) to 3.6% (1985-1990) then fell again to 1.8% (1990-96).[341] The only area where Germany showed a leading role within ICT during Phase 1 lay in the area of secure server hosting of the top domain names, a distinction it shared with Sweden and the United States.[342]

Based upon the data for ICT contribution to the German economy during Phase 1, there is **little evidence that German ICT firms were able to influence data legislation**. Though the country did increase investments, the majority of the export growth experienced by ICT in Germany was due to services-based industries, and not products exported. Given the fact that the German economy draws considerable strength from its manufactured goods exporting, ICT during Phase 1 did not contribute a great deal to manufacturing exports.

[339] See data in Tables 3 and 5.
[340] OECD 2000, p. 38. See appendix for Table 2 of this report.
[341] OECD 2000, p. 50.
[342] OECD 2000, p.66.

4.3.2 Security

Table 14: Security Incidents, Germany (West & East), 1970-1999

Year	Fatalities	Injuries	Casualties
1970	7	9	16
1971	0	0	0
1972	**23**	**45**	**68**
1973	1	1	2
1974	1	10	11
1975	1	12	13
1976	**4**	**36**	**40**
1977	6	2	8
1978	0	3	3
1979	0	10	10
1980	**17**	**218**	**235**
1981	2	31	33
1982	**5**	**44**	**49**
1983	2	25	27
1984	0	2	2
1985	**9**	**114**	**123**
1986	**9**	**242**	**251**
1987	2	32	34
1988	1	14	15
1989	5	8	13
1990	1	4	5
1991	**10**	**35**	**45**
1992	**17**	**217**	**234**
1993	*	*	*
1994	**2**	**85**	**87**
1995	10	26	36
1996	1	5	6
1997	0	27	27
1998	0	0	0
1999	**3**	**47**	**50**
Total	139	1304	1443

Source: Global Terrorism Database

As with the Swedish and British cases, the Global Terrorism database provided the data sourced on terror incidents in Germany. The main difference in the German case compared to the others relates to the effects of unification in 1990-91 upon security issues. The Federal Republic of Germany (RFD) faced many numerous attacks during Phase 1, primarily caused by the activities of radical left gangs and Neo-Nazi groups. The RFD was the base location for a

domestic terror group, previously referenced in the Swedish case discussion, the Baader-Meinhof group. Also called the RAF (*Rote Armee Fraktion),* the group operated from the 1960s to the 1980s, and perpetrated the major security incidents that occurred during Phase 1 in West Germany.[343] This extreme left-wing radical group borrowed ideology from the left-leaning student protest movement that arose in the mid 1960s in Germany. To understand the group's activities and the impact upon the German state and society, it is necessary to trace the origin of the RAF within student movement organizations (SMOs), and how the RAF evolved and moved away from the SMOs.

In the 1960s, a student protest movement emerged in West Germany, driven by an ideology of discontent with university and state authorities.[344] After World War II, many German universities had retrenched many of their existing faculty who had been complicit or at least compliant with National Socialist policies. This presented a staffing crisis, as replacement faculty were not quickly put in place, and the decision led to a shortage of teaching instructors. In response to the shortage, universities then reversed the decision and rehired previously fired faculty, despite their political and ideological history. Compounding the faculty problem was the content of German higher education which had become largely antiquated.[345] Subject matter fell behind the quality of the U.S. and Germany's neighbors in Europe. German students felt that university administrators were largely unresponsive to students' concerns over the non-democratic personal views of rehired faculty, the outdated facilities, and quality of content being provided to students. Student movement activists framed university authorities as authoritarian figures, similar to the Weimar Republic and Nazi regime leaders, who had forced compliance on

[343] Note: No security incidents data was available for East Germany during the period from 1970-1990. The data in Table 10 reflects West German data from 1970-1990, and data for the unified state after 1990.
[344] Becker 1977
[345] Becker 1977

the public and de-legitimized any forms of opposition. Former student activist Daniel Cohn Bendit, who later founded the Green Party, recalled in a 2007 interview with *Der Spiegel* that the protest movement's anti-fascist ideology was motivated by a desire "to make up for the fight against fascism that their parents had not led… but we failed to distinguish between the meaning of 'resistance' in a fascist state and that in a democracy."[346] In short, the SMOs saw state activities to suppress or manage the protests as anti-democracy.

The scope of student protests widened to include various actors and states that were connected to perceived failures of true democracy in the Federal Republic. The student protests came to height during the summer 1967, around a scheduled visit to Berlin by Reza Pahlevi, the Shah of Iran.[347] The Shah had made comments in newspaper interviews prior to coming to Berlin that the students felt revealed a leader largely out of touch with the plight of impoverished Iranians. Protests were organized by the leader of the Socialist Student Association, Rudi Dutschke, and planned for 2 June, and to be located just outside the Berlin opera, where the Shah, his wife, and German dignitaries were set to attend a performance of *The Magic Flute*.[348] After the uproar created by students outside the opera entrance during the arrival of the politicians and diplomats, a majority of students dissipated. A remaining 1000 protesters were chased by police with truncheons; many were injured and hospitalized after being attached.[349] One student, Benno Ohnesorg was shot and killed by an officer with a gun. Ohnesorg's death served as a symbolic catalyst for some whom had been present at the Berlin protest. It was from this point that individuals later connected to the RAF began to mount a more violent response to "fascist" police and state authorities.

---

[346] Der Spiegel 2007; Musolff 2011, p. 66.
[347] Aust 2006; BBC 2016
[348] Preece 2010
[349] della Porta 1999, p. 71, 72.

The RAF founders Andreas Baader and Gudran Ensslin increasingly self-identified as "resistance fighters" inside the protest movement, and sought to fight on behalf of the underprivileged against the Federal Republic of Germany and those the RAF felt were victimized by the United States and its allies.[350] Baader and Ensslin felt that peaceful protests were unsuccessful in forcing state authorities to retaliate and reveal the true nature of their fascist tendencies. Instead, what was needed was more violence to provoke the state to act aggressively in retaliation. In addition to West German targets, countries that were allied with West Germany, such as the U.S., were considered appropriate targets. RAF leaders correlated the American military actions in the Vietnam war as an example of imperialist aggression to suppress the socialist North Vietnamese. Further targets included Israeli, or Jewish connected persons or property, because according to one RAF propaganda pamphlet, "The Jews displaced by fascism have become fascists themselves, who in collaboration with US capital want to exterminate the Palestinian people."[351]

The group solidified its membership base, and accelerated plans for violent attacks. The first act of increased violence was arson attacks on two department stores in Frankfurt in April of 1968. After 1970, the group only planned and executed attacks designed to result in significant damage to property and/or life.[352] To get their "formal training", several of the group members dispersed throughout West and East Germany in 1970, left the area to go to Jordan. There they journeyed to a camp outside Amman, where they lived and trained alongside guerillas working to free Palestine from Israeli control.[353] This would serve as the basis for their later partnership with the People's Front for the Liberation of Palestine (PFLP), which desired Marxist revolutions

[350] Musolff 2011, p. 62.
[351] Aly 2008; Musolff 2011, p. 63.
[352] Aust 2007
[353] Aust 2008, p 65-70.

worldwide, and sought the overthrow of the nation of Israel. The PFLP aided Japanese, South American and German terrorist groups with reason for use of violence due to "righteous causes."[354]

Looking at the data, the RAF put their terrorist training to use once the group members returned to Germany in 1972. The RAF bombed the V-Corps headquarters of the U.S. Army Officers Club on 11 May of 1972, during which 1 person died, and 13 were injured. A second attack that year happened on 19 May 1972, when the RAF bombed the Springer Press building in Hamburg. The bombing was planned after the extreme right newspaper *Deutsche Nationalzeitung,* printed by Springer, called for the student protest leader Dutsche to be stopped due to his radical views. This attack resulted in over $100,000 in damages and 24 injured persons.[355] Last, but not least, eight members of a like-minded Palestinian terrorist group called the Black September Organization (BSO) attacked the Israeli athletic compound at the Munich Olympics on 5 September 1972, taking hostages, and torturing athletes. A failed rescue during a hostage exchange for Arab prisoners conducted by FDG authorities resulted in the deaths of 16 persons during a violent shoot-out, including deaths of the Israeli hostages and five terrorists.[356] Following the failed rescue, Interior Minister Hans-Dietrich Genscher launched a new program, the Grnzschutzgruppe-9, or GSG-9, which would be a SWAT-like task force designated to intervene during future crisis terror events.

RAF group leaders were gradually arrested during the summer of 1972, after a series of tipoffs by the public. Ironically, three founding members, Baader, Baader's lover Ulrike

[354] Becker 1977, p. 15.
[355] Aust 2008, p. 31-32; Global Terrorism Database.
[356] CBS 2016

Meinhof,[357] Ensslin, and RAF recruits Holger Meins and Ian Carl Raspe continued to plan RAF assassinations and killings whilst in prison awaiting trial. Yet by the spring of 1976, each of these individuals had either committed suicide or died by hunger strike while awaiting trial. After their deaths, other RAF followers kept the movement going.[358] A sister group to the RAF, the *Revolutionaïre Zellen*, or "Revolutionary Cells", was responsible for the June 1976 bombing of the Frankfurt headquarters of the U.S. Army, which injured 16, and carried out a December attack at the Frankfurt US Air Force Officers Club, where 18 were hurt. During that summer, on 27 June 1976, the Revolutionary Cells and the PFLP combined efforts to hijack an Air France plane en route from from Tel Aviv to Paris. After making a touchdown in Athens, hijackers forced the pilot to fly to Entebbe, Uganda, after which Jewish and non-Jewish passengers were separated by the terrorist, and the Jewish group help for hostage and ransom. Israeli paratroopers stormed the plane, freeing the hostages and killing the terrorists.[359] The liberation of the victims was framed as a defeat for the cause by "brutal, 'fascist' Israeli henchmen who had employed Nazi 'Blitkreig' tactics."[360]

Such splinter groups and second and third generation membership of the RAF kept up the organized plan to perpetrate domestic terrorism, including kidnapping and later killing of prominent industrialist Hans Martin Scheleyer in 1977.[361] That same year, a partner attack conducted by the PLO and German terrorists captured Lufthansa flight #181 after leaving Mallorca on its way to Frankfurt. The pilot was killed, and hostages taken, with demands of the

---

[357] Meinhof had been associate with the group first as a journalist covering their activities in the left-leaning *kronket* publication, then later ideologically supporting their radical causes, including helping Baader escape from prison for a theft charge back in 1970.
[358] Musollf 2011
[359] Musolff 2011, p. 63.
[360] Musolff 2011, p. 63.
[361] Preece 2010, p. 152; BBC 2016.

release of 11 RAF and Palestinian terrorists being held in prisons in Germany and Turkey. During refueling in Mogadishu, the plane was retaken by GSG-9 forces, and all four terrorists were killed.[362] Moving to the increased activity of the 1980s, members of the RAF were identified as being responsible for the 1985 bombings of the Frankfurt Alitalia airport hub (3 died, 42 injured), the Rhein Air base (2 died, 20 injured), and the La Belle Discotheque in West Berlin, during which 230 suffered injuries.[363] Although the concerns of the student social movement were largely addressed when university reforms were instituted in the early to mid 1970s, the radical actors in the RAF had only intensified their violent activities during the late 1970s and 1980s, moving away completely from the foundation of peaceful, student-led protesting.[364]

The RAF movement began to lose momentum and lessened their activities after 1990, and other groups rose to prominence in committing domestic terrorism in the unified state. Neo-Nazi extremist groups were responsible for the bulk of domestic terrorism in the 1990s. These attacks included attacking a Polish truck entering Germany in October 1991 (4 hurt), an assault on a Bonn home for immigrants in 1991 (10 injured), and a major onslaught by 400 Neo-Nazis who struck a police unit guarding a hostel frequented by foreign visitors (74 injured), in August of 1992. The terrorist events of 1994 included assaulting another police unit in Bremen (22 injured), attacking a group of Turkish immigrants (7 casualties), and a protest turned violent by left-wing extremist group targeting a Republican party rally in Ulm, who using stone projectiles caused 13 casualties. The most significant single attack at the end of Phase 1 took place in February of 1999; two hundred Kurdish rebels stormed the Israeli Consulate in Wilmersdorf,

---

[362] Tanner/NYTimes 1977
[363] The attack on the discotheque was a joint effort between RAF and the Anti-American Arab Liberation Front. Source: Global Terrorism database.
[364] Aust 2008; Becker 1977; Musolff 2011; Preece 2010.

Germany, during which 3 people died, and 43 were hurt.[365] In total, 139 people died, and 1304 were injured during domestic terrorist actions in Phase 1, from 1970-1999.

State responses to the above-mentioned attacks involved a multi-layered approach. After World War II, West German policy responses to domestic terror were seen by some as a test of the restored democracy, and how it would balance democratic rights against state accountability.[366] The state developed two main security goals that involved activity at both the domestic and international levels; these policies were chosen based on lessons learned from the past.[367] The first goal, tied to experiences during the Weimer Republic, was to avoid allowing "enemies of constitutional democracy" using the "grounds of the rule of law" to legally violate the principles of the state.[368] Practically speaking, this involved setting legislation that called for judicial review of any new legislation by the *Bundesnachrichtendienst*, or Constitutional Court, to ensure that any news laws dealing with terrorism complied with constitutional rights outlined and protected in the Basic Law of 1949.[369] The second goal related to experiences under the Nazi regime: control state surveillance and information accumulation, making use of surveillance an accountable process. Together these approaches would allow the state to respond in a balanced way to the current threats, whilst keeping in mind the lessons learned from the past.

Politically, the parties differed in their approaches to terrorism and personal information security. Social Democrats (SPD), were in control of the government in an alliance with the Free Democrats (FDP) from 1969-1982. The Christian Democratic Union (CDU) led the government for most of the latter period of Phase 1, from 1982-1998. In the early 1970s, the SPD wanted to

[365] Global Terrorism Database.
[366] Hanshew 2010
[367] Katzenstein 2003
[368] Katzenstein 2003, p. 740.
[369] Schwartz 2002

present calm responses to the increased terror activities; party leaders felt strongly that internal security would best be ensured via legal institutions that would constrain any heady use of power by the government during times of crisis.[370] To the SPD, the domestic terrorism during the 1970s and 1980s created a need for reforms of various institutions and powers that would not grant overarching power to government authorities, while preserving the rights to protest and oppose the government. Conservatives and CDU/CSU leaders perceived a weakness in SPD policies during the 1970s and 1980s, which failed to manage the ongoing threat of domestic terrorism.[371] Regardless of these differences, the SPD managed to get reforms in the 1970s that would modernize police and public management, and incorporate the use of new technology.[372] Counterterrorism efforts therefore shifted to proactive policing, as prevention would be better than catching criminals after terrorist acts had been committed. This led to a series of changes.

As previously mentioned, the Federal Criminal Office (BKU) was expanded, and the new agency head Horst Herold promoted computerized technology as a rational way to administer justice and simultaneously avoid the human biases of past governments.[373] Additionally, Hans-Dietrich Genscher, then Minister of the Interior, expanded the budget and staff of the Bundeskriminalamt (BKA), or Criminal Police Office, and centralized criminal investigative power especially as regards information gathering, which reduced the ability *Länder* officials to localize the handling of terrorist detection and counterterrorism.[374] The BKA was given power to use data processing for information gathering and police intervention purposes.[375] Herold also developed a computerized dragnet technique of profiling potential terrorists by cross-referencing

[370] Hanshew 2010
[371] Hanshew 2010
[372] Hanshew 2010
[373] Hanshew 2010
[374] Hancock 1994
[375] Herold 1968

multiple government databases and compiling a central record in the PIOS computer system used by the Suppression of Terrorism department (TE) and the Special Branch (ST). However, there were some limits to why and how personal data would be collected, how long it could be stored, and with whom it could be shared.[376]

Post-unification, and under CDU leadership, Germany shifted to a proactive counterterrorist agenda which included expanding efforts via technological means and by international cooperation beyond German borders to stop previously successful terrorist groups. German authorities increasingly expanded surveillance techniques as the technology developed to do so. By the 1990s, German law enforcement utilized wiretapping surveillance to monitor telecommunications by suspected criminals and terrorists, including land lines, cellphones, and email content.[377] Legislation in 1994 expanded the powers of the *Bundesnachrictendienst* or Constitutional Court which would allow surveillance of "letters, conversations, or communications" involving personal data to determine if an individual was exhibited behavior that threatened state survival or democracy. Law enforcement and security personnel were also authorized to practice "strategic surveillance" involving telephone, satellite, or other communications if needed to repent an armed attack against the state. This expanded law was a part of a package of policies that would allow information collection for all forms of illegal actions against the state, including terrorism.

Regional prevention and catching terrorists required evaluating records from the former East Germany and eliciting coordination of efforts across Europe and beyond. After committing acts of violence in West Germany, many RAF members had escaped across the border and either hidden or used East Germany as a travel hub for making plans to meet with sympathetic partner

[376] Katzenstein 2003; Schwartz 2002.
[377] Schwartz 2002

groups in the Middle East. State authorities were able to locate these individuals who had been given temporary shelter in East Germany, when on the run from West German police, sometimes using records from the Stasi files.[378] State leaders also opened additional doors to regional and international cooperation on larger efforts to thwart terrorism in Europe. German influence pushed for and achieved a European secretariat of Interpol in 1986.[379] Germany was also responsible for promoting the creation of Europol during the Maastricht treaty negotiations.

The number and frequency of domestic terror incidents led to gradual increases in the use of data securitization, with more use of data as a security tool in recent years. The Federal Republic of Germany certainly experienced a significant number of domestic terrorist threats during Phase 1, much more than Sweden, but five times less than the incident totals in the U.K. German authorities did increase access to informational acquisition tools and did expand interior security measures from 1970-1999. However, despite the increase in violence, neither the political nor social will was present to grant unimpeded access to personal data. The shadows of restrictions upon personal expression and dignity experienced under the National Socialist regime were long. The SPD government in charge during the decade of the 1970s worked diligently to enshrine fundamental human rights and to protect via legal institutions the rights to democratically protest the government in power. Even after the more conservative CDU party came to government in 1982, it was unwillingly to promote a highly intrusive use of data by the state. Several scholars attribute this self-imposed restriction to an underlying "civility" and "dignity" within the definition of individual self-determination in Germany's culture.[380] The constitutional framework for individual protections on dignity was largely unchanged once it was

[378] Several sources indicate the protection offered by various East German actors, for RAF and Revolutionary Cell members. Aust 2008; Katzenstein 1990, 1998, 2003.
[379] Katzenstein 2003
[380] Bennett 1992; Fuster 2016; Schwartz 2002.

granted by the Basic Law of 1949. To address why the protection of these rights are so strong in Germany, I now turn to examine the contribution by legal professionals and human rights activists.

4.3.3 Digital Human Rights

Early data protection laws beginning in West Germany and for the unified state after 1990 were motivated by two factors: strong norms of fundamental human rights within the Basic Law of 1949, and the advocacy of the legal community. As the German language has no specific word for privacy, the attempts at legislating protection for personal data utilized *persönlichkeitsrechte*, or the "right to a personality" in Article 1(1).[381] The right to develop their personality is protected within Article 2(1) as long as someone does not violate constitutional order. Legislation protecting data first emerged. The first data within individual *Länder*, and not at the federal level. In 1970, the state of Hesse passed the first data protection law in the world.[382] The Hessian law established oversight using an independent Data Protection Commission (DPC), which was accountable to the *Länd* Parliament. The law mandated security measures for all Hessen-stored data files. In addition, new data processing technology had to be reviewed by the DPC prior to implementation in public administration. Following Hesse, Rheinland-Pfalz passed a data protection law in 1974. The Rheinland-Pfalz law differed from the Hessian law, by giving supervisory power to a committee comprised of Landtag members and two officials or judges. Notably, this law only applied to data processed by *Länd* administrative agencies.[383] Other *Länder* followed with data protection laws; Bonn passed a law in 1976,

[381] Bennett 1992, p. 74-82.
[382] G.V. Gl. Hessen 625, W. Germany (Data Protection Act of the Land of Hesse).
[383] Bennett 1992, pgs. 78, 151; Hondius 1980

The demand for legal protection of personal data in Germany did not come from parliamentary ministers, or administrators incorporating the data processing technology, but was driven by the jurist community and public concerns. The author of the Hesse 1970 Data Protection Act was Professor Spiros Simitis, a trained and practicing jurist.[384] Simitis was Greek by birth, but had immigrated to West Germany to study jurisprudence. After university, Simitis later became the Professor of Labour and Civil Law in Gießen and Frankfurt, as well as at UCLA, Berkeley. Simitis advocated for data protection in Hesse, in Western Germany, and in Europe, and he was a part of a larger network of legal professionals who actively promoted adoption of regulatory framework for computer use in West Germany. At the National Conference of Lawyers in 1972 (*Deutsche Juristentag*), the group created a data protection group to research the topic.[385] Simitis' role in expanding data protection beyond the RFG into EU level legislation will be examined further in the subsequent chapter. In addition to the concerns of the legal community, public opinion polls revealed fears over computer network linking across sectors, the widespread sharing of personal ID numbers during automatic data processing (ADP), and use of ADP during the population census collection. In the 1970s and 1980s public opinion shifted away from trust in government management of personal data, toward an increased fear of ADP by public authorities. In 1976, 62% of people polled said the state should be able to know as much as possible about residents, but by 1983, 65% of the public felt the state should have as little access as possible to their personal information as was possible.[386] Recall that this period of distrust was highest during the height of the RAF domestic terror spree.

[384] Der Spiegel 1977
[385] Bull 1984
[386] Flaherty 1989, p.25

At the federal level, the Bundestag created a resolution in 1969 asking for regulation on data processing, and made a proposal for a "preliminary plan for the protection of privacy against the misuse of automatically processed personal data."[387] The first draft bill was tabled in December 1971, because of controversy over the level of specificity I the bill compared to the Hessian law, as well as the concerns by the ICT sector which wanted the law to apply to manual as well as computerized data in order to prevent competitive disadvantage.[388] Throughout 1972 and 1973, the Ministry of the Interior reviewed versions of the proposal and held public hearings to assuage concerns over weak enforcement mechanisms and continued preference for the looser Hessian model. Between 1974-1976, the Interior committee held more public hearings, and called on expert testimony by advocates including Spiros Simitis, who attempted to direct the parties toward support of a federal law that included an independent control authority, rather than a loose self-administering surveillance model.[389] Additional differences of opinion in 1976 among the CDU and CSU, added friction in the Bundestag over whether the control body would be within the Federal Audit Office, rather than be independent as Simitis had promoted. Despite disagreement over the independence aspect of the DPC, the Bundestag endorsed the bill in November of 1976, and the bill passed on 27 January 1977.[390] The wording was not perfect, but the *Bundesdatenschutzgesetz* (BDSG) had become national law.

The BDSG created a new and independent Data Protection Commission, led by a federal Commissioner. The new agency was to operate in tandem within the Federal Ministry of the Interior. The DPC was responsible for recommending updates to the law, and giving advice to

[387] Bull 1984, p. 104.
[388] Flaherty 1989, p. 22.
[389] Bennett 1992; OECD 1976, pgs. 83-94.
[390] The bill passed, but was opposed by several Länder, including Bavaria, Baden-Württemburg, Rheinland-Pfalz, and Schleswig-Holstein.

ministers or public authorities about special regulations for data protection. Initially the DPC could only provide information to the Bundestag and Interior Ministry; later powers were added to serve as ombudsman over data protection violation complaints made by individuals. Each public agency had to have its own personal data protection officer, to ensure that that the agency complied to the BDSG. Any data processor must be registered with the DPC authority. Lastly, the DPC produced an annual report of the state of data protection in the FRG; this report was submitted to the Bundestag for review on an annual basis.

Table 15: Commissioners of the National Data Protection Commission, FRG

Years Served in DPC	Name of Commissioners
1978-1983	Hans Peter Bull
1983-1988	Reinhold Baumann
1988-1993	Alfred Einwag
1993-2003	Joachim Jacob

The federal office was led by four different Commissioners during Phase 1, all of whom had previously held legal and/or academic careers.[391] Their legal training and experiences informed their management of the DPC Commission, as each promoted the continued protection for human rights within data protection, albeit using different styles. Hans Peter Bull acquired his Doctor of Law in 1963, and had worked as a lawyer and academic since 1967. Bull was a member of the Social Democrats when appointed as the first federal DPC, but saw himself as a federal civil servant, and used his platform to focus national attention on the social effects of computer technology diffusion.[392] To Bull, state bureaucrats including that of the DPC provided

[391] Flaherty 1989, pgs. 48-57.
[392] Munzinger Biographic Index sourced for professional information on Hans Peter Bull, Reinghold Baumann, Alfred Einwag, and Joachim Jacob.

a functional service for the state, not directly serving the public. When it became apparent that Bull may not be reinstated when his 5-year term ended, there was some discussion of Hessian DPC Spiros Simitis becoming the next federal Commissioner. In the end, Bull was succeeded by Dr. Reinhold Baumann, who had been a lawyer for 30 years within the federal Ministry of the Interior prior to coming to the DPC. His leadership style was more "managerial" than Bull's and placed more emphasis on public concerns rather than state's interests.[393] After Baumann retired, Dr. Alfred Einwag was appointed in 1988. Einwag acquired his doctorate in law from the University of Munich in 1952, after which he worked for district government offices and the Ministry of the Interior until 1964. His other public service posts included advisement on legal matters for the Federal Border Police after 1964. Finally, Joachim Jacob was appointed to lead the DPC in 1993. Jacob also held a doctorate in law; his previous positions in the Ministry of the Interior, and as a consultant to State Secretary Günter Hartkopf of the FDP.

Each DPC had liberty to choose his/her personnel. Agency staff were typically lawyers or jurists, or those with some data processing experience. Due to the career mobility framework of civil service in the FRG, it was difficult for any DPC to keep staff for very long, as career advancement was conditional upon moving around the Ministry of the Interior. Just as soon as staff had become trained and proficient in the tasks of the Commission, they often left, making long-term continuity and speedy action on complaints ongoing issues for the agency.

The purpose of the BDSG was to "ensure against the misuse of personal data during storage, communication, modification and erasure (data processing) and thereby to prevent harm to any personal interests of the person concerned that warrant protection."[394] Personal data was defined as "details on the personal or material circumstances of an identified or identifiable

[393] Flaherty 1989 p. 48.
[394] Flaherty 1989, p.30

physical person."[395] Prevention of harm to individuals required data processors to fulfil three main tasks. Manual and automated data files must be protected. Personal data could be stored as long as using the data was necessary for completion of a legitimate task. Finally, data subjects possessed the right to be informed of personal data existence, have their incorrect data amended, request that their data be restricted from additional use, and could request their personal data be deleted. As the first federal Data Protection Commissioner stated, the bill was to act, "As a kind of human rights protection in a technological society."[396] The BDSG was amended or updated in 1994, 1997, and 2001.[397] The 1997 and 2001 changes reflected the necessity of maintaining compliance with EU data law directives, including Directive 95/46/EC which will be discussed in detail in the next chapter.[398]

The law was challenged by two political events during Phase 1. First, public opposition to computerized data use arose around the proposed 1983 national Census, which would be an update to the 1970 census. An opinion survey conducted by the Klaus Lange Society for Mathematics and Data Processing discovered that 81% of the public surveyed feared a loss of privacy during the collection and storage of personal data during the national census.[399] Spiros Simitis, then the Hessian Data Protection Commissioner, stated that hundreds of citizens had called their office to complain over fears of government surveillance related to the propose census. The Constitutional Court delayed the national census collection while it reviewed public privacy concerns. On 15 December 1983, the Constitutional Court ruled that in the instance of personal data on rent and housing, West Germans had a "constitutional right to self-

[395] Riccardi 1983, p. 249.
[396] Flaherty 1989, p. 31.
[397] Bennett 1992, p 212.
[398] Flaherty 1979.
[399] Flaherty 1989, pgs. 30-32.

determination about the use of their own personal information on the basis of articles 1 and 2 of the Constitution."[400] This ruling served as yet another critical juncture during which German citizens received expanded power to determine whether they would relinquish information to a government agency. Meanwhile, public protests were held in 1983 and 1987 over the proposed collection of personal data which during the upcoming census. 25% of surveyed households admitted they were planning on not completing the census forms.[401] After adjustments to data management plans, the census was finally carried out in 1987.

Secondly, the DPC faced opposition to its oversight from various aspects of the national security community. As mentioned in the domestic terrorism discussion, BKA head Dr. Herold Horst had adopted the PIOS data retrieval system for profiling of suspected terrorists during BKA investigations. The DPC felt this use of personal information was dangerous, as data collection could potentially involve the information of non-suspects, without their consent. Horst clashed with Bull regarding the control and use of this police data. Bull requested the BKA delete some fingerprint data in storage, and offered a set of guidelines in 1981 that involved data collection best practices.[402] In 1986, Baumann complained that security officials were not following Commission advice for limits to police power over personal data according to a new article of the Code of Criminal procedures. Ministers of the Interior Zimmerman complained of DPC interference with security measures, but Baumann took the issue to the Interior Committee of the Bundestag in 1986 and won his case. Like his predecessor, Baumann and Bull had argued that security officials were still subject to constitutional law and must provide protection for personal information.[403]

---

[400] Flaherty 1989, p. 45; Webb 2003, p.1.
[401] International Herald Tribune survey, 28 March 1983, p.2.
[402] Deutscher Bundestag 1981; Flaherty 1989, pgs. 71-72; Third Activity Report of the BfD 1982.
[403] Flaherty 1989, p. 76.

In the case of Germany, there is substantial support for the development of a digital human rights regime. The Hessian state developed its own data protection law and Commission in 1970, under the influence of legal professional and human rights advocate Spiros Simitis. Simitis then went onto influence the national legislative debate in the early to mid 1970s, by providing expert testimony to the Bundestag and various investigative bodies. In addition, the state was pressed to create national data protection legislation by the *Deutsche Juristentag,* a highly organized network of lawyers and jurists. After the BDSG law was passed in 1977, the implementation of the law was challenged by the previously scheduled census collection order, and by security services in pursuit of terrorist organizations. In both instances, the power of the law and the validity of DPC efforts were supported, and not weakened by judicial and Parliamentary review.

4.4 Summary of National Case Findings

4.4.1 Economic Commodification

Comparing the cases in the area of economic dependence upon ICT, I found that in **Sweden,** whatever the contribution of the ICT sector, data laws were not written to allow firm freedom in personal data management. In the United Kingdom, ICT firms were granted more significant freedom over data treatment than were their competitors in Sweden or Germany. The uniqueness of **British** ICT firms pressuring the government to adopt data protection in order to strengthen competitiveness was an unforeseen direction of legislative pressure. Regarding **Germany**, though ICT firms did increase their market share of economic contribution during Phase 1, the continued strength of the manufacturing sector diminished the ICT impact upon data law provisions.

4.4.2 Security Incidents and Threats

Swedish society did not face significant threats from domestic terrorism to warrant any adjustments to data protection. However, in the **United Kingdom**, overwhelming numbers of security problems in Northern Ireland contributed to the desire in Parliament to increase access for law enforcement to personal data. In the German case, I found mixed support for law enforcement access to data during Phase 1. When challenged by DPC officials, security officers had to comply with the digital rights protections of the BDSG passed in 1977.

4.4.3 Digital Human Rights

Among all my cases, there was the most evidence across all countries for the mounting influence of the legal epistemic community upon data protection creation and ongoing compliance. **Swedish** lawyers served to advise the regulatory bodies of the Riksdag and held DIB positions of power. Data rights advocates among Parliament and the legal community faced more difficulty in getting a law passed in the **U.K.**, than did their colleagues in Sweden or Germany. Only by creating linkages between concerned MPs such as Alex Lyon, with British advocates like Paul Sieghart, and the pressure of ICT firms, did the Thatcher government U.K. establish data rights. Finally, **German** legal professionals began the institutionalization of data protection at the Lander levels, and promoted the same rights in federal law. This hypothesis had the most support of the three.

I now turn to examine the development of data legislation during Phase 2 (2000-2015). In particular, I focus on the efforts made by the EU Commission and Working Party 29. As the data will show, these individuals were very influential in shaping supranational legislation into a regional regime of digital human rights.

5 DATA PROTECTION LAWS AT THE EUROPEAN UNION LEVEL

5.1 Theory

The theoretical argument posits that data governance in the EU occupies a space of regime complexity.[404] Regimes are a type of institution, or the rules used around a given issue area. Creation of or membership in a data protection regime involves commitments to organizational norms and policy expectations around data treatment that are driven either by domestic interests (national regimes) or international interests (international organizations or regimes). Regime complexity occurs in the presence of multiple national or international regimes which offer competing ideas on how to manage an issue.

Figure 3: Data Regime Complex

The development of data governance regimes is divided into two time periods: Phase 1 (1970-1999) and Phase 2 (roughly the late 1980s-2016). Data governance was managed at the

[404] For this chapter, I have included the most pertinent documents which propelled forward the regimes of data legislation in the EU. An exhaustive examination of all documents within the Member States legislative repositories, the Council of Europe database, the OECD database, and the Official Journal of the European Communities is beyond the scope of this dissertation.

national level during Phase 1 but moved to the international level of policy coordination during Phase 2. Policy-making followed the causal pathway of Putnam's two-level games and that of Milner's spatial negotiations arguments.[405] National policymakers move back and forth between their national legislative environment and the international stage, seeking policy compromises that please their obligations in both arenas. At both the domestic and international levels, policy-makers will utilize epistemic professionals for the purpose of advising for present needs and long-term implications of any proposed policies. As the human rights literature notes, norm "entrepreneurs" can and will often diffuse norms throughout the international system by calling attention to issues of importance and attempting to link with elites who hold decision-making power.[406]

From the 1970s-present, data legislation in European states has involved competition among domestic interests along the three main areas introduced in the national case chapters: ICT firms continually sought economic gains from data use, national security authorities increasingly tried to use personal or cyber data during criminal investigations and anti-terrorism efforts, and human rights activists pushed back against free use of personal or cyber data, asking for human rights protections. As has been established in Chapter 4, at the national level states had to choose a hierarchical preference when these interests conflicted with one another. Various individual states legalized data protection as a fundamental human right, a fact I labeled as a regime of "digital human rights." Digital human rights originated in Sweden and Germany and diffused across Europe.

[405] Milner 1987; Putnam 1988.
[406] Finnemore and Sikkink 1998; Keck and Sikkink 1998.

5.2 National Efforts in Phase 1 (1970-1999)

To recap the national policies chosen during Phase 1, in the case studies of Sweden, Germany, and the United Kingdom I examined how each of the three domestic interests attempted to influence national data legislation. Did the state have an economic dependence upon the ICT sector (Information and Communications Technology), a history of domestic security incidents, or to what degree was there advocacy by legal and human rights experts? These factors contributed to diverse types of domestic regimes that would govern data to the advantage of the three primary interests.

Sweden experienced few to no domestic security problems during Phase 1, and the ICT sector was minimally influential upon economic growth. The country did, however, have a history of public access to government records. In the 1970s, government records were computerized, causing public concern about privacy loss. Legal professionals advocated for the first national law in Europe for personal data protection. As a result, the *Datalagen* of 1973 protected personal data very heavily. Since the 1970s, Sweden has continued to push for digital human rights across Europe.

West Germany experienced a significant number of security attacks by extreme left-wing gangs and neo-Nazi groups during the 1970s-1990s. Despite the casualties associated with the attacks, a pervasive public fear of government surveillance prohibited the *Bundestag* from developing a law with unrestricted access to personal data for governmental authorities, including security and law enforcement. In addition, when West German lawmakers decided to create national data protection, regional data laws were already in place in the *Länder*. The national government consulted with regional data protection authorities (DPA) who were mostly legal professionals for the *Länder*, and the DPAs suggested a policy of restrictive protections for

personal data. Combined with the lagging development of the German ICT sector compared to technology firm growth in other states, and Germany had the highest number of data protection laws passed among my cases. Germany and German legal rights experts have continued to push for the internationalization of data protection norms.

The U.K. experienced an enormous domestic security problem due to terrorists' actions in Northern Ireland during the Troubles Years (1960s-1990s). Though nearly 8000 people were hurt or killed during in this time period, security officials did not heavily pressure the Commons or the government to gain access to personal data in the U.K. Here, ICT interests were the most aggressive. Tech firms were very concerned about losing comparative advantage to the Americans and other European states within the global marketplace. This fear was predicated by the fact that Britain had not ratified Convention 108 of the Council of Europe, which outlined personal data protection for all members, so that data mobility would be safe throughout the OECD trade community. The British ICT sector feared they would lose business if other OECD states had data protection laws that would allow for transborder data movement, but the UK did not. The Thatcher government eventually acquiesced to the pressure from ICT firms and passed the Data Protection Act in 1984.[407]

5.3 European Efforts in Phase 2 (late 1980s-2016)

Applying the theoretical expectations to data governance in the European Union, **I argue that states occupy international spaces that include overlapping, nesting, or duplicative international regimes that may compete with their domestic regimes on data governance.[408]**

[407] Convention 108 advised member states to create national policies of protection for personal data during automatic processing. Such policies were to include allowances for transborder movement of personal data within the OECD membership, foreseen as a necessary mechanism for ICT business growth. This will be discussed later in this chapter.
[408] This statement serves as my theoretical argument for EU-level policies on data protection.

Since international regimes involve a commitment to some degree of policy-matching among members, states that have domestic laws in place for data governance will also face a second decision point for data policy. Within the international system of organizations (regimes), national representatives will advocate for the international agreements to match the preference of domestic interests on data treatment. The EU is an example of such an international regime in which national laws must be harmonized across many issue areas.

Following the logic of complex interdependence, the more powerful states of the EU should be able to get their preferred data policies passed into EU legislation.[409][410] I therefore traced the level of influence of the most powerful EU states - France, Germany, and the U.K. - upon the EU data policy process from the 1980s to present. To assess the argument, I needed predictions for how the individual states will pressure other organizational member states toward specific policies. I measured for each of these three countries the levels of economic dependence upon the ICT sector. Measures were in two forms. First, I looked at Value Added as a % of GDP; this data was sourced from the OECD. Second, I developed a new composite of ICT variables to measure the additive export effect of all these sectors within the economy. These findings will be discussed below. To assess the impact of domestic security problems to preferences for using data in security surveillance, I utilized the Global Terrorism database for a gross measure of numbers of domestic terror incidents from the 1970s-2014.[411] Finally, to evaluate the role of

[409] This statement provides my hypothetical predictions for the EU policymaking process from the 1980s to present.

[410] Keohane and Nye 1989. Complex interdependence argues that states with larger amounts of military and/or economic power can more readily create international organizations, and that once created, they can pressure small and mid-sized states to follow the policy preferences of the more powerful states. Once the organization (regime) is created, even if the power of the state declines, due to institutional rigidity, these preferences/rules will persist.

[411] Data points through 2016 were not available for all case countries, so the date cut-off point was set at 2014 to capture consistency of available data for the three countries.

legal and human rights experts in pressuring the EU to pass data protection, I looked for the presence of individuals from these professions who either advised EU legislators during the policy-making process, or when such individuals were given oversight on data legislation compliance. Understanding the national preferences of each powerful state in the three structural areas allowed me to predict individual states' preferences for EU data policy and to evaluate the success of these predictions.

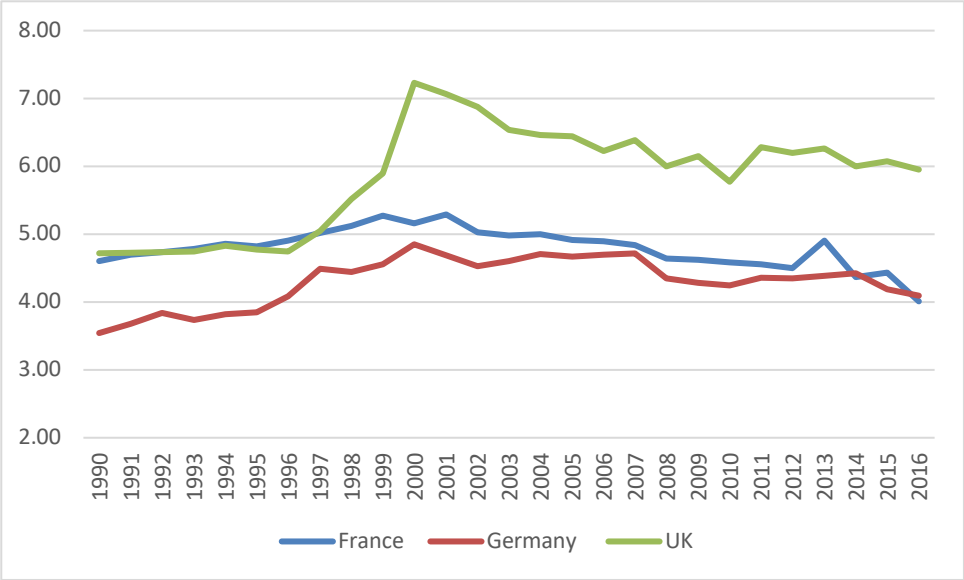
5.3.1 ICT Sector Dependence

To what extent did the powerful states have dependence upon the ICT sector in the national economy? The purpose of this dissertation is not to show that the ICT sector was more important than other sectors to each national economy. However, it is necessary to show that the ICT sector was growing in importance for the national economies of Europe, due to the financial value of data to these firms. It is also important to establish that the economic impact of ICT firms differs across countries. Chart 5.1 represents the impact of data upon the digital economy, based upon how much these firms contributed to the overall GDP in each country. The ICT sector was broadly measured with the following variables: share of the ICT sector in GDP, share of the ICT sector personnel in total employment, the growth of the ICT sector in value added, the share of ICT investment in research and development, and the share of the ICT sector used in research and development personnel expenses. ICT manufacturing and services includes the variables manufacturing of electronic components, computers, communication equipment, magnetic media, consumer electronics, ICT equipment, software, telecommunications, computer programming and data processing, and repair of computer and computer-related equipment. All data was sourced from Eurostat and the OECD.[412]

[412] https://ec.europa.eu/eurostat/cache/metadata/en/isoc_se_esms.htm "Units of measure: The units published are: % of the ICT sector in total value added at factor cots, % of the ICT sector in total

We see that the contribution to each economy among the more powerful EU states differs significantly. The German ICT sector grew the least, contributing from 3.5% to a maximum of 4.5% of GDP in the years under discussion. Both France and the UK started the 1990s with levels between 4.6-4.7%. The UK reached a high point of 7.23% in 2000, and although the sector retracted in the early 2000s, levels have remained about 6%. Finally, French growth was relatively stable, hovering between 4-5% until recent years with a decline.

Table 16: ICT Value Added, % of GDP, Powerful EU States



Data Sources: World Bank WDI Database, OECD, Eurostat

Given the fact that the U.K. showed the most growth by the ICT sector, and therefore the highest contribution made to the national economy, **the United Kingdom should be the most**

employment, % of the ICT sector in total R&D expenditure of businesses and % of the ICT sector in total R&D personnel."

likely of the three powerful states to push for more open data access and data commodification in EU data legislation, followed by France.[413]

The challenge with the above measure is the inability to isolate the value created within the export market. As seen in the UK case study chapter and will be discussed at the EU level in this chapter, ICT firms have not been hesitant to argue for data legislation based on the use of data as a mobile commodity, as it moves across state lines during all types of business activity. The "Value Added" measures does not capture this aspect of data value. I therefore created my own measure of the value of data exportability, which is called the **Data Technology Export Contribution Composite (or DTEC)**. The DTEC contains four variables used by the OECD, IMF, and World Bank when measuring the export value of data-based firms; ICT goods exports, ICT services exports, high-tech exports, and insurance-financial services exports. The data below reports values of the powerful states of France, Germany, and the United Kingdom.[414] All variables were standardized in STATA, then averaged for 5-year periods for simplification. The DTEC composite table below reflects the five-year mean percentage of contribution by the ICT sector within the exports of each country.

Table 17: Data Technology Export Contribution (DTEC) Composite

Country	1985-1989	1990-1994	1995-1999	2000-2004	2005-2009	2010-2014	2015-2016
France	-0.94	-0.90	-1.91	0.01	-0.90	0.34	1.44
Germany	-4.22	-3.49	-1.56	-0.15	-0.55	-0.41	0.01
U.K.	0.36	0.36	1.73	5.42	3.54	1.89	1.98

Sources: Eurostat, OECD

[413] Note the dip in economic contribution in the UK and Germany immediately following the 2008 global financial crisis. The consistent growth of ICT in France during this time was particularly interesting.
[414] The choice of these states to exemplify powerful states in the EU aligns with the arguments made by Keohane and Nye in chapter 2 of *Power and Interdependence* (1989).

Again, the United Kingdom experienced a higher percentage of ICT products and services exported as compared to the other two states. All years under consideration revealed positive contribution to the export market, even following the 2008 financial crisis. Although France and Germany made considerable gains across time in ICT exports, they still lagged behind the UK. I therefore expected that the UK would advocate against any EU legislation that would restrict data mobility. As France showed the next highest level of ICT exports, French representatives could hesitate to provide any data protections that would impede data flows across borders.

5.3.2 Influence of Security Risks

Table 18: Domestic Terror Casualties, 1970-2014, France/Germany/UK

Total Casualties	1970-1974	1975-1979	1980-1984	1984-1989	1990-1994	1995-1999	2000-2004	2005-2009	2010-2014	Totals
France	70	138	617	470	67	333	56	35	36	1823
Germany	97	74	346	436	371	119	58	8	4	1513
United Kingdom	1772	1250	1202	1494	1312	956	103	934	101	9124

Source: Global Terrorism Database

5.3.3 United Kingdom

The greatest number of security casualties occurred in the United Kingdom. Notably, the volume of domestic attacks peaked from 1984-1989, and peaked again between 2004-2009. The U.K. figures are largely attributed to the Troubles Years of unrest in Northern Ireland between 1968-1998, and to the rise in increased domestic terrorism following the 2005 bombings in the London Underground. EU parliamentarians debating on data legislation in the Commons during the Troubles frequently noted the importance of information access to law enforcement and security officials. As domestic terror attacks have been an issue in the past and have risen to the fore again more recently for the state, **British representatives should be the most likely to prefer**

granting more freedom of access to national security officials. However, British security officials will have to balance their desire to access data with the legislative preferences for data profiteering desired by the technology sector.[415]

5.3.4 France

France experienced the second largest number of domestic terror casualties among the most powerful states of the EU. Broadly speaking, after World War II when France was led by Charles de Gaulle, national security policy focused on nuclear deterrence development and acquiring security partnerships that limited the global hegemony of the United States.[416] Then in the 1970s and 1980s, France experienced a series of domestic security attacks by individuals linked to a variety of ideological goals. Carlos the Jackal, a self-styed "professional revolutionary" carried out grenade, rocket, and bombing attacks, which killed and injured dozens in the 1970s-1980s.[417] During the 1980s, the country was also plagued by a series of attacks on the Turkish consulate, and on retail stores, airports, and public spaces (hotels, train, cafes, cinema, and offices). ASALA (Armenian Secret Army for the Liberation of Armenia), Hezbollah, and Action Directe were believed to be responsible for much of the violence in this decade.[418]

After the September 11 bombings in the U.S., French security white papers linked domestic and international security together, highlighting the importance of information-gathering by national intelligence agents, and cited a need for cyber strategy to protect ICT firms. 419

---

[415] See the UK case chapter for the full discussion on competitiveness in data mobility related to Convention 108 by the OECD. As a part of the Convention, the OECD promoted personal data protection, so that the transborder movement of data would not be prohibited between OECD states due to differences in protection between data sending and data receiving states.
[416] Gordon 1993
[417] NBC News 2017
[418] Domingo 2010
[419] Domingo 2010; French White Paper, 2013; Defence and National Security Strategic Review, 2017; NY Times 1986; Segell 1999

Additional attacks after 9/11 involved an Air France hijacking by the Armed Islamic Group (GIA), and the Nice bombing by the National Liberation Front of Corsica (FLNC). 420 Most recently, the 2015 incidents of the Charlie Hebdo shootings by adherents to Al-Qaeda, and the Paris sports and music venue attacks in November were attributed to ISIS members. The Bastille Day celebration in Nice was targeted by a truck driver who turned out to be a Tunisian extremist.[421]

These occurrences caused France to shift national security approaches from perceiving mainly external aggressors, to investigating domestic terrorists. French authorities expanded the powers of existing law enforcement agencies responsible for counter-terrorism, intelligence gathering, and internal security. Important to this dissertation, information-gathering was expanded.[422] In 2006, data collection powers were expanded to include traveler information, [423] internet and telecom firms are now required to grant police access to customers' data, and a biometric data collection program is now administered by Air France during flights through the Roissy airport (*Programme d'Expérimentation d'une Gestion Automatisée et Securisée*).[424] France started with with an externally focused security policy in the 1960s. With the increased numbers of domestic attacks by nationalist and fundamentalist terrorists, data and information use by security has evolved and expanded from the 1970s forward. I therefore expected **French representatives to support higher levels of data access for national security reasons when negotiating EU data policy.**

[420] Nundy 1994; BBC News World Edition 2002.
[421] Rawlinson, Chrisafis and Dodd 2016
[422] The Ministry of the Interior has the power to administer information databases on passengers and non-citizens entering the country. The new database was an expansion of the *Fichier National Transfrontière* database created in 1991. The new database expanded the information gathering and data available to security officials. See Domingo 2010, p. 123.
[423] Domingo 2010, p. 149.
[424] Passenger participation was voluntary. See Domingo p. 150, 151.

5.3.5 Germany

Turning to Germany, as outlined in the case studies chapter, the state had the least number of domestic security attacks of the three countries. The country did experience a large number of bombings related to domestic terrorism during the 1980s and 1990s. The majority of these attacks were attributed to an extreme leftist group, the Baader-Meinhof gang, which was neutralized in the mid 1990s. As shown in the case chapter, the German public continues to remain skeptical of granting overarching surveillance power to the state. When these fears are combined with the fact that Germany has more personal data protection laws than the other states under consideration, I expected to see that Germany will allow for security access to information, as long as this access does not override the individual protections for personal information that are imbedded in both regional and national laws.

5.4 The Role of Legal Professionals and Human Rights Advocates

The final internal influence upon EU policymaking on the issue of data governance could be made by the legal and human rights community. When a policy-making environment includes uncertainty and institutional coordination is required for policies that concern politicized issues, epistemic professionals have served as technical experts and information providers for policy-makers during the research phase of designing a new law.[425] Furthermore, the advice of technical experts often reflects their shared normative beliefs that may or may not involve systemic policy bias among the profession.[426] Haas (1992) points out that researchers looking to assess the power of epistemic communities should identify community members, trace community beliefs among common to the profession, and then posit credible outcomes that would occur as a result of the

[425] Haas 1992
[426] Haas 1992, p. 25.

consulting work for lawmakers.[427] This requires examining advisory publications, testimonies, press releases, etc. to identify content promotion and subsequent suggested policies. As noted in the case chapters, Germany and the U.K. each had legal professionals, academic elites, and jurists that served as consultants for national parliaments when making domestic data laws. In this section I draw from the the content of national data protection laws, the professional background of those who head each national data protection authority, and the role afforded to legal and human rights experts during the EU legislative process.

Table 19: Summary of National Data Law Content - France, Germany, UK, 1970-1999

Country	Total # of Data Laws, Phase 1	Coding Results	Percentage of Provisions for Security Access	Percentage of Provisions for Data Protection	Percentage of Provisions for Economic Use
France	1	+ 14 Data Protect	0	100%	0
Germany	12	+42 Security Access +405 Data Protect + 72 Econ Use	4.3%	41.4%	7.4%
United Kingdom	3	+36 Security Access +360 Data Protect +17 Econ Use	5.2%	52.4%	2.5%

When the content of the French law is added to the data, it reveals a stark difference to that of the German and British Laws. Though the original French data law is much shorter than either the first UK or German laws, it is devoted entirely to data protection rights, with no provision for security authorities to violate the human rights protections, nor any content that allows for data commodification exclusive of digital human rights. It is important to discuss the process of choosing data legislation in France, since this was not covered in Chapter 4.

[427] Haas 1992, p. 34.

5.4.1 France

Year	Name of law	Description
1978	Law No. 78-17 (French Data Protection Act)	Initial data protection law, applying to *"informatique et libertés"* covering computer data processing, data files, and personal freedoms; created the *Commission nationale de l'informatique et des libertés* (CNIL), the national data protection authority

From 1970-2016, France passed three data protection laws. The first data protection law became law in 1978. This law was in response to public outcry over a proposed government database known as SAFARI (Système *Automatise´ pour les Fichiers Administratifs et le Ré´ pertoire des Individus*).[428] The French government had been planning a national data base to organize personal data to be used in all public records and databanks. The Minister of Justice appointed an investigative commission to determine the potential for rights violations; the "Tricot Commission" proposed the need for

> *"…measures to ensure that the development of data processing in the semi-public and private sectors will take place in the context of respect for private life, individual liberties, and public liberties."*[429]

After so much public concern, the government passed the French Law on Informatics, Data Banks and Freedoms which provided personal data protection, such that "information technology should be at the service of every citizen."[430] Though the law was brief, it provided the foundation not only for significant personal data protection in France, the law would also inform EU policymakers when designing EU data laws, a point I return to later.

First, provisions within the 1978 law established a permanent agency charged with monitoring data protections, but the agency staff selection has been somewhat controversial. The

[428] Flaherty 1989, p. 166.
[429] P. 7, Council of Europe 1976 English translation of the *Report of the Committee on Informatics and Liberties* 1975; Flaherty 1989, p. 166.
[430] Loi no. 78-17 du 6 janvier 1978 relative à la informatique, aux fichiers et aux libertés

National Commission on Informatics and Freedoms (CNIL) oversees and regulates data protection. The CNIL is comprised of a college of 17 persons, drawn from a variety of political institutions in France. The mix includes two National Assembly deputies, two Senators, two members of the Economic and Social Council, two state attorneys from the General Assembly, individuals from the court system (Administrative Supreme Court, Financial Supreme Court, and French Judicial Court), as well as one individual appointed by the President of the National Assembly, one appointed by the President of the Senate, and three people chosen based on their expertise in the area of data protection.[431] The college itself votes to determine who will serve as the college President. Since its creation, some academics have argued that the functional structure of the CNIL has kept control over data privacy sequestered within the CNIL, rather than allowed it to be openly debated in the national Assembly.[432] In other words, those that make it onto the CNIL come from a variety of political backgrounds and a majority are politically appointed. However, once they join the CNIL college, their data policy suggestions and the amount of independent power wielded by the CNIL college is significant. The CNIL college members have a great deal of autonomy and there are few obligations to accept input from any of the external stakeholders involved in the issue of personal data protection, including individuals, human rights organizations, businesses, or the security segments of government.

---

[431] Commission nationale de l'Informatique et des Libertés 1978; Righettini 2011.

[432] Flaherty 2014

Table 20: French National Commission on Informatics and Freedoms

Presidents of the CNIL	Term Length	Professional Background
Pierre Bellet	1978-1979	Attorney, Jurist
Jacques Thyraud	1979-1983	Mayor, Politicians
Jean Rosenwald	1983-1984	President of the Court of Auditors
Jacques Fauvet	1984-1999	Former Director of *Le Monde*
Michel Gentot	1999-2004	State Councilor/Attorney
Alex Türk	2004-2011	Politician, Chairman of Schengen Committee, French Europol Supervisor
Isabelle Falque-Pierrotin	2011-2019	State Councilor, OECD Expert on Internet, Chair of EU Article 29 Working Party
Marie-Laure Denix	2019-2024	Administrative Court Auditor, Telecom Regulator

As seen in Table 20, the CNIL presidents have included those with legal expertise, as well as politicians, and a journalist. This mix of professions and training has contributed to the variety of missions pursued by the CNIL as each president attempted to shape the mission in accordance with government goals as well as their own interpretation of the needs of the time. The longest serving presidents, such as Fauvet, Türk, and Falque-Pierrotin have had the greatest impact. Fauvet led the CNIL when Directive 95 became EU data legislation; this Directive forced EU states to adjust any national laws in place in order to implement EU data protections. Directive 95 will be discussed in the sections to follow. Türk served as CNIL president following 9/11 and the Madrid and London bombings, after which all Western states revised their data surveillance practices. Falque-Pierrotin is the most powerful and impactful CNIL president; her influence spread much beyond France to the hugely influential Article 29 Working Party of the EU which worked to expand the scope of personal data protection to establish digital human rights.

Regardless of the background of CNIL presidents, the 1978 law and the CNIL have set new boundaries for data treatment that differed from the influence by Swedish or German laws. France introduced the right to be forgotten, and prohibited large-scale data collection on data

subjects, both of which have subsequently been added into EU data legislation.[433] The French law was amended in 2004 to protect personal data used during digital marketing purposes, and a further decree added in 2011 which regulated the trafficking of personal data when developing online content. Regarding organizational functionality, unlike in Sweden or Germany, the Presidents and members of the CNIL have not always come from a legal background, but often served in political or private sector positions prior to coming to the CNIL. Given the politicized nature of CNIL college appointments, and due to the increased use of information surveillance by French security authorities as a result of increased domestic terrorism, I expect that **French representatives will promote digital human rights alongside promoting national sovereignty over data surveillance used during domestic anti-terrorism efforts.**

5.4.2 Germany

Table 21: German Data Protection Laws, Phase 1: 1970-1999

Year	Name of law	Description
1970	Population MicroCensus Law	Law permits some personal data release of information collected during the 1970 survey, for the use of correcting population registries, statistical use by central and Land authorities, for town planning, and for scientific use.
1971	Telecommunications Universal Services Act	Law outlining provision of telecom services, including voice telephony, rates for customers, and directory publications
1977	BDSG – Data Protection Law	First national data protection law, protecting against misuse during automatic processing.
1983	Census Act	Discusses the protections required by the Basic Law, regarding personal data collected during the national Census. Also regulates the use of data collected for statistical and public administration purposes.
1990	Data Protection Law Bundesdatenschutzgesetz (BDSG)	Revision of the 1977 law on federal level personal data protections. Includes details on responsibilities of federal Data Protection Officer, the mandates on data secrecy and transmission provisions, and right afforded to data subjects.

[433] In Europe, the right to be forgotten has been applied to various aspects of personal information, including having a history of criminal convictions and participation in pornographic media. A full discussion on this right cannot be fully explored in this dissertation, but the right has evolved and expanded within Europe, due to many court cases. https://gdpr-info.eu/issues/right-to-be-forgotten/

1995	Broadcasting Act for North-Rhine Westphalia	Addresses the licensure, functionality, and monitoring of broadcasting services in North-Rhine Westphalia. Includes specific protections for personal data of subscribers and their and personal viewing habits
1996	Telecommunications Act	Regulations regarding service installation, fee scheduling, environmental protection, and other aspects of telecom service provision. Also creates Regulatory and Advisory bodies.
1997	Telecommunications Universal Service Ordinance	Provision of public telephone equipment, as well as release of subscriber information, as long as subscriber has not barred release
1997	Digital Signature Act	Regulation of digital signature keys, including security measures and monitoring capability.
1997	Act on the Protection of Personal Data Used in Teleservices	Charges tele-services providers with protection of personal data during telecom service provision.
1997	Telecom Customer Protection	Various obligations of telecom service providers for billing, service and equipment provision
1997	Postal Act	Licensure requirements for postal delivery contractors. Law also discusses release of addressees' personal information and the protection of data used by commercial actors when sending postal content.

As with the other countries studied, German authorities struggled to define legal protections for personal data when computerization of government data began. German politicians began to investigate the possibility of a data law in 1969. The eventual law passed in 1977 was based upon regional laws in the *Länder*, and the 1949 Basic Constitutional Law for the Federal Republic, which stated that "Human dignity shall be inviolable. To respect it shall be the duty of all state authority."[434] The Data Protection Directors from the *Länder* argued not only for a strong national law, but wanted an independent, national agency to oversee country-wide implementation. [435] Professionally, German Data Protection Commissioners had all received legal training, and had extensive experience with the Minister of Interior or other Civil Service branches.**German Data Protection Commissioners, Federal Level**

[434] Grundgesetz, Artikel 1 (Basic Law, Article 1).
[435] OECD 1976.

Table 22: German Data Protection Commissioners, Federal Level

Name of Commissioner	Term Length	Professional Background
Hans Peter Bull	1978-1983	Lawyer, Academic
Reinhold Baumann	1983-1988	Lawyer, Civil Servant with Minister of Interior
Alfred Einwag	1988-1993	Doctorate in Law, Federal Border Police Career
Joachim Jacob	1993-2003	Doctorate in Law, Deputy to Federal Data Protection Commission

In addition to the epistemic background in law by all federal DPC leaders, other DPC staff and regional Data Protection Commissioners often served as outside consultants for various international organizations when these IGOs investigated data policy suggestions for state members. For example, the Data Protection Commissioner for Hesse since 1970, Spiros Simitis, was consulted by Interior Ministry officials when the design was being chosen for the data agency structure.[436] Simitis also served as legal consultant for data policy in the OECD treaty of 1980, and was an advisor during European Union policy debates in the 1990s. German human data rights experts had a profound impact not only within their own country, but outside as well. For the purposes of this chapter, as supported by the findings in the national case study in Chapter 4, **German law provided the most extensive data legislation based on legal and human rights** at the regional and national levels. **Germany also used legal experts as leaders over data protection oversight more than the other powerful states** and gave the data protection authorities the most significant power for investigating data protection**. I therefore expected German officials to advocate quite extensively for European Union data protection laws.**

[436] Der Spiegel 1977

5.4.3 United Kingdom

Table 23: UK Data Laws, Phase 1: 1970-1999

Year	Name of law	Description
1974	Consumer Credit Act	Individuals granted right of access to credit source information for correction purposes.
1984	Data Protection Act	Regulates use of automatically processed personal data regarding individuals; designed to ensure compliance with Council of Europe Convention 1981
1998	Data Protection Act	Created new provisions for regulation of processing personal information; designed to ensure compliance with EU Directive 95/46/EC

The United Kingdom was the last of my case states to adopt data protection legislation (Sweden 1973, Germany 1977, UK 1984). As noted in the British national case chapter, the UK lacked the written constitutional structure for human rights protections. Britain also experienced a a very politicized struggle for data protection, with political will cycling up and down based on which party held the majority in Parliament. Conservatives were very hesitant to provide data protection and ignored repeated efforts by various MEPs from other parties who attempted to introduce data protection legislation. Human rights advocates like Paul Sieghart and various MEPs outside the Tory party introduced multiple data protection bills in the late 1960s and the 1970s that were unsuccessful until the ICT sector pressured Margaret Thatcher to pass data protection legislation in the early 1980s.[437]

The 1998 Data Protection Act created the initial permanent position of Data Protection Registrar (DPR). In 2000, Parliament passed the Freedom of Information Act, granting all British citizens rights of access to documents held by the Government. As a result of the 2000 law, the

[437] Bennett 1992

DPR was changed to the Information Commissioner's Office and given oversight not only of personal data protection (established in the 1984 law, and updated in 1998), but also granted oversight of the 2000 Information Act (and later also the Environmental Regulation Act of 2004). The agency is led by an individual appointed by the crown the Crown, typically serving a five year term.[438] Term lengths for the UK Commissioners have varied somewhat due to changes in the law that created the Commission. The ICO falls under the jurisdiction of the Justice Committee.[439]**Data Protection Register/Information Commissioner's Office (ICO)***

Table 24: Data Protection Register/Information Commissioner's Office (ICO)*

Registrar/Commissioner	Dates of Term	Professional Background
Eric Howe	1984-1993	BBC Journalist
Elizabeth France	1994-2001	Magistrate, Legal Expert
Richard Thomas	2002-2008	Civil Service
Christopher Graham	2009-2015	Politician, BBC Secretary, Advertising Standard Agency Head
Elizabeth Denham	2016-present	Human rights advocate, Privacy Commissioner in British Columbia

**Agency name was changed from the DPR to ICO in year 2000.*

Though the UK did create a full-time data protection agency to guard data protection, the agency was gradually given additional responsibilities that watered down the focus on digital human rights. Regarding the professional background and standing of the UK officials responsible for managing data legislation implementation, the government did a specific agency for this task following the passage of the 1984 Data Protection Law. However, as with the French CNIL, the DPR/ICO office of the UK was led by individuals from a variety of professional backgrounds. While some did have training in law or human rights, others had

[438] Hopping 2019
[439] https://publications.parliament.uk/pa/cm200809/cmselect/cmjust/146/14604.htm

experience in politics or media. Furthermore, the DPR/ICO leadership was expected to manage a variety of issues, not just data protection, indicating that the UK government had less intent on making digital human rights a separate and respected division of protections. **Going forward, I expected the UK officials to oppose rigid EU personal data legislation efforts and to also thwart attempts to expand the narrative around data beyond a human rights issue.**

To summarize my expectations of the behavior of France, Germany, and the U.K., during the EU legislative process for data governance, I predicted the **United Kingdom would push for data protections that would do not restrict data use or movement, so as not to threaten ICT sector growth and economic contribution. German authorities should seek great levels of personal data protection, seeking to align EU legislative protections with the scope of digital human rights. French authorities should seek a mix: stringent data protection, but promote national sovereignty over using data as surveillance and security tool against domestic terror.**

5.5 The Policy-Making Process in the European Union: Agenda and Influence

To reiterate: my expectations during EU law-making are two-fold. First, individual EU states will seek to promote an EU data policy that aligns with national policies already in place. (Thus, my predictions for each of the powerful states in the prior section.) This can be done by leveraging their influence when serving in the Commission or Council presidencies, or within the consultative committees. The predictions for these preferences were explained in the previous section. Second, borrowing from the international level of Putnam's two level game, EU policy-makers should also be influenced by pressures from any additional international organizations to which the EU states share membership. Within international organizations (regimes),

membership obligations will pressure states to pass laws that comply with the treaties or international agreement they sign. **EU Member States' International Organization Membership**

Table 25: EU Member States' International Organization Membership

Country	European Union	OECD	Council of Europe	United Nations	NATO
Austria	1995	1961	1956	1955	*
Belgium	1958	1961	1949	1945	1949
Bulgaria	2007	*	1992	1955	2004
Croatia	2013	*	1996		2009
Republic of Cyprus	2004	*	1961	1960	*
Czech Republic	2004	1995	1993	1993	1999
Denmark	1973	1961	1949	1945	1949
Estonia	2004	2010	1993	1991	2004
Finland	1995	1969	1989	1955	*
France	1958	1961	1949	1945	1949
Germany	1958	1961	1950	1973	1955
Greece	1981	1961	1949	1945	1952
Hungary	2004	1996	1990	1955	1999
Ireland	1973	1961	1949	1955	*
Italy	1958	1962	1949	1955	1949
Latvia	2004	2016	1995	1991	2004
Lithuania	2004	*	1993	1991	2004
Luxembourg	1958	1961	1949	1945	1949
Malta	2004	*	1965	1964	*
Netherlands	1958	1961	1949	1945	1949
Poland	2004	1996	1991	1945	1999
Portugal	1986	1961	1976	1955	1949
Romania	2007	*	1993	1955	2004
Slovak Republic	2004	2000	1993	1993	2004
Slovenia	2004	2010	1993	1992	2004
Spain	1986	1961	1977	1955	1982
Sweden	1995	1961	1949	1946	*
United Kingdom	1973	1961	1949	1945	1949

During the years under examination neither NATO nor the United Nations had a highly developed data policy regime.[440] I therefore anticipate that the data policy suggestions offered

[440] The United Nations Global Pulse project emerged following the 2008 financial crisis. The project includes data privacy recommendations built into the program which was introduced from 2011-2014. Guardian 2011; United Nations 2019.

by the agreements made in the Organisation for Cooperation and Development (OECD) and the Council of Europe to have significant influence upon EU states and the European Union.

5.6 International Regimes

The OECD originated the first international effort at harmonization of data processing protection, as a result of the desire among members to prevent disruption to data use as computer diffusion occurred.[441] [442] Multiple OECD member states had already adopted national legislation during the 1970s, including Sweden (1973), the U.S. (1974), and Germany (1977). Simultaneous to the interest by governments, academics and human rights advocates brought additional attention to the issue with several published works on the topics, such as Alan Westin's *Privacy and Freedom* (1967), and Paul Sieghart's *Privacy and Computers* (1976).

OECD progress on recommendations followed several conferences in 1974 and 1977 which looked at privacy, citizens' access to data, and cross-border data mobility. The OECD (European Union 1973) Peter Gassman (Germany, engineering and economics consultant), Louis Joinet (France, drafter of French *Informatique et Liberté* law), and Professor Peter Seipel (Sweden, Professor of Law).[443] They raised concerns about "reconciling fundamental but competing values such as privacy and the free flow of information."[444] The OECD Council formally adopted the *OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* on 23 September 1980. The Guidelines had eight core principles, including:

- Limit personal data collections to lawful means, preferably with data subject consent
- Collect personal data only for original use purposes, and limit use to these purposes
- No disclosure of personal data without either data subject consent OR the authority of the law

[441] Gassman 1976.
[442] OECD 2011, p. 15.
[443] Computer Networks 5 (1981), p. 127-141; OECD 2010; OECD 2011.
[444] OECD 2011, p. 19.

- Provide security measures against unauthorized data access or disclosure
- Provide a transparent policy on policies concerning personal data.
- Data subject rights shall allow confirmation of data held, and data corrected/ erased when requested by the data subject

Member governments were encouraged to incorporate the Guidelines into national practices, but no formal enforcement mechanism was in place. Concurrent to the work being done by the OECD on setting guidelines for data use, was activity within the Council of Europe also dealing with data protection measures.

5.7 International Regimes for Data Governance

5.7.1 Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, "Convention 108"

The Council of Europe's foundational principles include the *Convention for the Protection of Human Rights and Fundamental Freedoms* (ECHR), of which Article 8 of the ECHR states that "Everyone has the right to respect for his private and family life, his home, and his correspondence…"[445] The origin of the Council of Europe (CoE) data protection regime began in the late 1960s: the CoE Legal Committee handled two motions coming from the Consultative Assembly of 1967 which requested the Committee examine the impact of technological developments upon privacy.[446] In 1973 the CoE adopted Resolution 73 (22), which targeted protection of privacy of individuals inside electronic databanks used by private sector firms. At the 236th meeting of the Ministers' Deputies, the Council of Europe passed Resolution (74) 29, *On the Protection of Privacy of Individuals Vis-à-vis Electronic Data Banks in the Public Sector*, which noted the increased use of computerized data banks by member

[445] Council of Europe 1950
[446] Fuster 2016, p. 83.

governments and expressed similar fears to those raised by the OECD. Resolution 74 (29) suggested protections by states should include:

- Informing the public of government use of electronic data banks for storage or processing of personal information.
- Keeping information current and using it only for designated purposes
- Creating storage time limits
- Precautions should be set, and codes of conduct designed to limit misuse of information
- Databank access should be restricted to authorized users with necessity of use
- Statistical use of such information must assure anonymity

The CoE formalized the final treaty designed to protect personal data during automatic processing, thereafter known as Convention 108, on 28 January 1981, **creating the first truly international regime for personal data protection**. Original signatory states from the EU included France, Germany, and Sweden. The CoE regime had much more impact on the EU states that did the OECD Guidelines for several reasons: it asked specifically for "data protection", it linked protection to the obligation to provide fundamental rights, and it **invited regional institutions, such as the EU to pressure their member states for implementation.**

Though the CoE Convention asked states to protect data to include *during* transborder flows – an economic goal – the framing of personal data protection as a human right would be incorporated into the strategy of legal and rights experts working within the EU to set supranational policy in the decades to come.

The CoE Convention 108 treaty finally entered into force on 1 October 1985, following ratification by five CoE members, including Sweden (1982), France (1983), Norway and Spain (1984,) and Germany (1985). Note that Germany and Sweden are two of the national case states from Phase 1, both of whom had stringent national data protection laws in place from the early 1970s. States that delayed ratification included the U.K., which did not ratify the convention

until 1987; this delay of ratification supports my prediction that for the British, data protection was driven by the fear of reduced trade if they country did *not* adopt some form of data protection, rather than human rights concerns about personal data.

5.8 EU Member States' Actions during EU Policy-making: The Commission, Council of Ministers, Parliament

As the Commission is the point of origin for putting topics on the EU legislative agenda, I looked at the calls for data legislation made by the EU Commission, as this would indicate an opening political opportunity for personal data protection.[447] If a powerful state holding the EU Commission presidency requests to add data protection onto the legislative agenda in a format that matches national laws, this would substantiate the claim that powerful states attempt to shape EU policy around domestic preferences of their interest groups.

The first calls for EU legislation occurred in 1973 and 1974, and the narrative on data legislation singularly focused on the economic value of data processing under French Commission president François-Xavier Ortoli. Ortoli[448]. Ortoli asked the Parliament and Council to take up the issue of data governance, contextually framing the issue as relevant to the growing economic potential in the data processing industry.[449] [450] In 1974, the Commission requested a study group comprised of "governmental experts" to offer advice on such legislation.[451] [452] [453] This was followed by a motion submitted by a mixed coalition of MEPs in April, 1976, who

[447] Garrett and Tsbelis 1996; Kassim et al 2001; Moravcsik 1998; Nugent 2002; Peters 1994.
[448] Ortoli had previously served in a variety of economic policy advisement posts with the French government.
[449] Information Memo P-63/73, SEC (73) 4300 final, p. 2.
[450] Council Resolution of 15 July 1974, on a Community policy on data processing No C 86/1.
[451] (1975) Commission proposal for second series of priority projects in data processing at a cost of 23 million units of account. Information Memo P-55/75, September 1975.
[452] This study group is later referred to as the "Steering Committee."
[453] *COM (78) 347 final*

asked the Commission to draft Community legislation regarding "protection of the rights of the individual, aware of the legitimate concern of the public at the risks of misuse or abuse of information stored in regional, national or international data banks." [454] The Commission agreed; a lack of data protection legislation would be costly to the economies of EU states, prompting a statement released on 29 July 1981, in which Commission asked that members sign and ratify Convention 108 by the end of 1982. The strong action taken by the Commission to coerce EU Member States to ratify Convention 108 **supports to my argument concerning the influence of international regime membership upon national and regional policy**. [455]

The next Commission President, Roy Jenkins (UK), did not promote a particular data legislation agenda. [456] Following Jenkins, Commission President Gaston Thorn (Luxembourg) tied data protection to the need for a "common commercial policy, to the progressive abolition of restrictions on international trade."[457] [458] Despite the persistent pressure by the EU Commission that EU States ratify and adopt the CoE Convention 108 regime, few EU community states ratified or adopted it early on. By March of 1983, two members of the European Parliament (Sieglerschmidt of West Germany, and Glinne of Belgium) submitted a Working Document on behalf of the Socialist Group asking exactly when the Commission would follow-up with a draft proposal for a Directive "to ensure a uniform level of data protection within the European Community."[459] Only under the Delors Commission (France, 1985-1995) did EU data protection legislation cross the tipping point of momentum toward becoming real law. Jacques Delors'

---

[454] *EU Parliament Working Document 46/76*
[455] 29 July 1981, COM (81) 679/EEC
[456] Ludlow 2016
[457] Address by Mr. Gaston Thorn, President of the Commission of the European Communities to the European Parliament, Strasbourg, Monday 12 January 1981).
[458] *European Parliament Working Document 1-4272/83*, and *EU Commission Document 1-1232/83 – COM (83) 658 final.*
[459] *European Parliament Working Document 1-42/83, (Oral Question 0-173/82)*

goals for the Commission of 1985-89 largely revolved around successful completion of the single market programme by 1992.[460] However he had no specific initiatives that involved data processing industries nor personal data protection; his work on data protection would come under the umbrella of his promotion of the tech sector for EU economic growth.

Regarding efforts by the Council presidents to lead data policy efforts, in the mid to late 1980s, the Council presidency was held by the United Kingdom (Margaret Thatcher, 1981), West Germany (Helmut Kohl, 1983), France (Francois Mitterrand, 1984), back again to the UK (Margaret Thatcher, 1986), then again to France (Francois Mitterrand, 1989). I found no documentary evidence that any of these leaders were focused on data processing or personal data protection legislation as a part of their agenda when leading the European Council. The Council did promote legislative process for personal data protection, albeit built into policy for common market telecommunications.[461] It took an additional two years for the Commission to issue a proposal for a Directive on protecting individuals' personal data.[462]

5.9 The Decade of Change for EU Data Legislation – The 1990s and the Role of Epistemic Advisors

The decade of real change for data protection was most definitely the 1990s. **The influential factors during this decade include the increased utilization of investigatory bodies staffed with industry and legal experts** and a momentum of activity to legislate the issue among all three units of Community leadership to produce data legislation. In April 1990, consultants to the Commission advised that since "information is considered more and more as a

---

[460] Endo 1999

[461] *Council Resolution of 30 June 1988 on the development of the common market for telecommunications services to 1992*, 88/C 257/01.

[462] *Commission Communication on the protection of individuals in relation to the processing of personal data in the Community and information security*, COM (90) 314 final – SYN 287 and 288, 13 September 1990.

tradeable commodity…[a] resource of great value which is sold at high prices by specialized companies" within Europe, thus the Community should develop policy for this issue area.[463] [464] In July 1990, the Commission presented a new proposal to the Council asking for a Directive on data governance.[465] The Economic and Social Committee reviewed the request in 1991, and the Delors Commission formally presented the proposal for a Council Directive on the legal protection of databases on 13 May 1992.[466] In the midst of these negotiations on data policy, general changes to core EU treaties impacted data policy as well. Maastricht set norms of secrecy around Community use of data and gave states permission to exchange data during police cooperation.[467] [468] When Jacques Santer (Luxembourg) became Commission president in January of 1995, he continued the efforts of generating data legislation, based on economic goals. The Council of Ministers follow Parliament early in 1995, by adopting of the amended position on data governance passed in 1992, and it accepted Parliament's agreement on the common position in June of 1995. Directive 95/46/EC came into effect on 24 October 1995.

Though it started as an economic initiative, the final wording of Directive 95 became the premier regional framework for digital human rights in Europe. This Directive provides a **critical juncture for EU data legislation; after Directive 95, digital human rights became an accepted community norm.** As a Directive, it set a mandatory regulation for protecting information privacy via data protection by ALL Community members. Note that the directive also prohibited restrictions on cross-border data transmission. Directive 95 provisions included:

- Definitions of personal data, data processing, data controllers and processors, third party data recipients

[463] EU COM (92) 24 final – SYN 393, 13 May 1992, Section 1.5 and 2.1.1, pgs. 4-5.
[464] EU COM (92) 24 final – SYN 393, 13 May 1992, Section 1.5 and 2.1.1, pgs. 4-5.
[465] EU COM (95) 375 final-COD287, 18 July 1995.
[466] EU COM (92) 24 final – SYN 393, 13 May 1992
[467] See Article 20.
[468] Maastricht Treaty, p. 108, 92/C 191/01

- Applied the scope of protection on automatically processed data, in addition to provisions in national laws
- Restricted personal data use to legitimate uses, for originally collected purposes, with corrections during use, and anonymization post use
- Prohibited personal data use which reveals race, ethnicity, political/religious/philosophical opinions, trade union membership, health, or sex life
- Required consent for use by data subject, who is to be informed on data changes or change to use
- Mandated that Member States create (if not already in existence) a national office for personal data projection, led by a designated officer to monitor such protection

Exemptions built into the Directive allowed for personal data use in matters of national or public security, **preserving national sovereignty on security matters, which was of particular importance to France, as predicted** earlier in this chapter.

Other than the specified mandates on data protection within the Directive, the greatest impact of the Directive occurred around the establishment of an advisory Working Party comprised entirely of legal rights experts

5.10 The Article 29 Working Party (WP 29)

Article 29 of Directive 95 established a permanent and independent Working Party solely focused on the protection of personal data during processing (hereafter known as Article 29 Working Party, or WP 29). The group was charged with providing the Council of Ministers with information on any matters related to data protection. WP 29 met from 1997-2016, only being disbanded when the General Data Protection Regulation (GDPR) replaced Directive 95/46/EC. The Article 29 Working Party was not staffed by representatives chosen from a variety of backgrounds (potentially including civil society, private sector, or public actors), but the members came exclusively by those serving as directors or supervisors of the national Data Protection Authority (DPA) in Member States. Remember from the national chapters of Germany and Sweden, that **DPA directors were overwhelmingly from legal or academic**

professions trained in human rights advocacy. Also recall that the French CNIL was organized in such a manner that prohibited outside input by legislators or by civil society. The organizational structure of WP 29 replicated this insularity found in the French CNIL, combined with the single source staffing from legally trained individuals found in Sweden and Germany. Furthermore, the scope of competencies of WP 29 were particularly wide, including the abilities to:

- Oversee national application of Directive 95
- Give the Commission opinions on protection in third countries
- Advise the Commission on proposed amendments that would "safeguard the rights and freedoms of natural persons with regarding to the processing of personal data, and on any other proposed Community measures affecting such rights and freedoms."[469]
- Search for diverse levels of protection among Member States practices
- Make recommendations via reporting to the Commission on "all matters" relating to personal data protection; the Commission is obliged to respond with any actions taken
- Issue annual reports on the status of personal data protection within the Community and in third countries, reporting to the Commission, Parliament, and Council of Ministers.

To sum, WP 29 was staffed by "experts" in legal matters, given a wide range of responsibilities, with little to no oversight or input by multiple stakeholders inside or outside EU bodies. The structural arrangements of WP 29 would have profound effects upon the way that future data protection was framed in EU legislation, how protection would be implemented and changed across time, and how the Union would harmonize policies along the preferential lines of particular states. Between 1997 and 25 May 2018 when WP 29 was replaced with the new General Data Protection Board, the committee released hundreds of guidelines, letters, official opinions, annual reports, and press releases, all geared toward expanding digital human rights, and not toward a reduction in protection in any way.

---

[469] *Competences*, pg. 4, Directive 95/46/EC.

The proactive measures taken by WP 29 to expand the scope of EU data legislation following the passage of Directive 95 cannot be overstated. Working Party 29 submitted a stream of reports on a regular basis to both the EU Commission and Council of Ministers, all of which were used by these institutions when amending or creating new data legislation from 1997-2016. Using the methodology discussed in Chapter 3, the content analysis of the recommendations, opinions, and annual reports submitted by Working Party 29 to the EU Commission is seen in Table 26. 58 documents were analyzed for content. First, I assessed the 100 most common phrases of up to 4 words. Overwhelmingly, the most common phrases used discussed data protection during automatic processing. These words became the core words for my auto-coding scheme, along with the most common words that discuss security and/or economic interests. See Table 26 below for the findings.

Table 26: Communications Content of Article 29 Working Party, 1997-2016

Topics Discussed	**Percentage of Mentions**
Security terms (security, police, court, judicial)	49.05
Protection terms (processing of personal data, protection of personal data, consent, right to privacy, fundamental rights and freedoms)	37.96
economic terms (business, marketing, economic)	12.96
Free movement of data	0.03
Total	100
***N*= 6334 sentences coded**	

Note that as mentioned in the methodology chapter, this was a "blunt" auto-coding of the content. Each sentence with one of the mentioned words was auto-coded for presence of the word/phrase. While security terms comprise the largest mentions category, in reality, the words have both positive and negative framing within the text of the communications by WP 29. For example, some sentences with the words security are referencing the Common Foreign and

Security Policy instituted in the Maastricht treaty, but do not actually discuss data treatment at all. In other sentences, the security terms may be granted permission or setting restrictions on securitized use of data. In contrast, the protection and economic terms more generally reflect positive mentions.

5.11 Findings Summary of 1980s-1990s

The preferences for data protection in the EU started out in the 1980s following the national preferences of the UK, who had a big stake in data profiting tied to ICT growth. By the 1990s, data protection had shifted away from an economically-necessitated model (preferred by the UK), to a regime of digital human rights (preferred by Germany, and to a lesser degree, France. Subsequent changes to data protection established in the 1990s were driven by specific states with nationally tight data protection regulations (Sweden, Germany, France), and at the suggestion of legal and human rights experts (WP 29, Spiros Simitis, Britain's Paul Sieghart).[470]

Directive 95 would be adjusted via changes to EU law written into the Treaty of Amsterdam in 1997, and with the addition of a new Charter of Fundamental Human Rights. The Amsterdam Treaty guaranteed personal data protection, but allowed data transfers without data subject consent during police cooperation.[471] A new "Charter of Fundamental rights of the EU" incorporated data protection as a fundamental human right (something WP 29 had advocated during the formation of the Charter).[472] [473] Despite protest by the UK against the expanding scope of EU human rights, the Charter of Fundamental Rights of the EU became EU law on 7 December 2000 at Nice.

---

[470] See also Directive 97/66/EC and Commission Proposal 1999/C 376/E/04.
[471] Bačić 2012; Fuster 2016; Treaty of Amsterdam, Article K.2.b.
[472] Expert Group on Fundamental Rights 1999, p. 2, 8, 17.
[473] Article 29 Fourth Annual Report, WP 46, 5019/01; Article 29 Recommendation 4/99.

Regarding activity in the Commission, neither the Santer nor Marin Commissions expanded data protection, nor did the Prodi Commission (1999-2004), other than to emphasize the importance of technology growth in the Union.[474] Thus we see throughout the mid-1990s, the Commission's actions on increasing digital human rights came as a result of input from expert advisory bodies. Additional pressure came from Member States such as Germany and Sweden which already had firm national regimes for digital human rights. The only consistently dissenting state to the expansion of digital human rights was the UK whose representatives argued against rights expansion including that of data protection.[475] **Once the key epistemic experts in WP 29 linked the need for data protection to application of democratic human rights in the Union, it was difficult for hesitant states, such as the UK, to argue against protections when so many Member States also had national protections in place.** The Commission consistently followed all recommendations made by WP throughout the 1990s and into the 20002.

5.12 2000-2010 – Expanding the Scope of Digital Human Rights

The expanded provisions for data protection in the early 2000s were a result of applying data protection to newly developed areas of technology. Some changes also followed the 9/11 terrorist attacks in the United States and in Europe. In 2001 the EU Parliament and Council passed Regulation (EC) No 45/2001, which required additional measures for data protection during cross-border movement. In 2000, the US-EU Safe Harbour framework was created to allow such data transfers to the US, which had no similar law to Directive 95; this would later be

[474] https://www.cvce.eu/obj/speech_by_romano_prodi_strasbourg_14_september_1999-en-a4c723ef-383a-435d-ad90-581e0ee856d0.html
[475] Braibant 2001, p. 47.

replaced due to inconsistencies in the nature of compliance by US companies.[476] The Nice Treaty (2001) established a new EU oversight body - the regional European Data Protection Supervisor authority. Peter Johan Hustinx was appointed to the first five year term as Supervisor in 2004.[477]

The next significant shift in the EU narrative around data protection was driven by EU Commission President Manuel Barroso (Portugal, 2004-2005). Barroso was the first key EU leader to link **data protection and heightened anti-terrorism concerns.** In a statement, he argued that, "Preventing radicalisation and protecting our critical infrastructure are of pivotal importance…the implementation of the policies and legislative proposals…[may compromise] data protection and access to the Visa Information System."[478] His Commission acknowledged the ongoing and important role of expert advisors, who would continue to "reinforce and update [Commission] knowledge".[479] In an age of increasing amounts of terrorist activity, the Members of the European Parliament wanted data legislation to be moved out of third pillar competencies (under the control of national governments) and into the first pillar (supranational policy), in the jurisdiction of EU bodies. [480] After two years of "reflection", the Lisbon Treaty reworked the EU pillar structure; the treaty moved cooperation on issues of freedom, security, and justice (FSJ) between police and judicial authorities out of the third pillar into first pillar governance. These changes applied to data protection legislation.[481] **Thus the limits of data protection were redefined in a post 9/11 world: data protection would be a fundamental human right, but this right could be overridden due to national or regional security threats.** One last note

[476] Treaty 2013. Note: Safe Harbour had US firms voluntarily sign up to comply with Directive 95, in order to allow them to receive EU data transfers. The US Federal Trade Commission was given oversight on participating companies' compliance with EU law.
[477] European Parliament Council 2004/55/EC
[478] Commission 2005, p. 8.
[479] Commission 2005, p. 3.
[480] European Parliament C 304E/386 2005, p 6.
[481] Panizza 2018

should be made about the Lisbon framework; Denmark, Ireland, and the United Kingdom had exclusion clauses to reduce mandatory participation with rules on personal data sharing during judicial or police cooperation, **again an instance of resistance against EU supranational data policy from the UK.**[482]

Directive 95 had weaknesses along with strengths; these necessitated its eventual replacement by the General Data Protection Regulation (GDPR), effective in 2018.[483] Meetings were held between 2009-2011 to engage national data authorities, WP 29, and the European Data Protection Supervisor in discussions as to what changes should be made in the wake of exponential technological changes to the ways data was used along with the ongoing need for data cooperation for security officials. In January of 2012, the Barroso Commission released *Safeguarding Privacy in a Connected World: A European Data Protection Framework for the 21st Century.* The report asked for a new Regulation to replace Directive 95, and it requested rules for use of personal data during criminal investigations and judicial processes. The law should preserve individuals' "right to be forgotten" and set parameters for data breach notifications. The new data law should also encourage the growth of the Digital Single Market plan by keeping the burden placed on businesses as least cumbersome as possible. Finally, it should help security authorities in all Member States with the fight against terrorism by permitting the free flow of data during police cooperation. Notably, in *Safeguarding Privacy*", there was **no further mention of the responsibility to adhere to Council of Europe's Convention 108 that had been included in multiple EU-level documents on data protection and had served as the foundational motive for much of EU policy from the 1980s-2000s.** From this point forward, EU policy-makers and institutions "owned" the digital human rights

[482] Articles 6a and 7, Lisbon Treaty 2007/C 306/02, C 306/186, C306/190, 191.
[483] EU Commission COM (2012), 9 final, "Safeguarding Privacy", pg. 3.

regime, essentially asking EU Member States to initiate data protection legislation based solely on their obligations to the EU, rather than on their obligations to other IGOs like the Council of Europe or the OECD. Supranationalism reigned over data policy in this view.

5.13 General Data Protection Regulation (GDPR)

In 2014, Jean-Claude Juncker (Luxembourg), the new EU Commission President, announced a series of actions to strengthen the norm of data privacy. His agenda further entrenched digital human rights in the EU, but did so based upon internet-based data, or "cyber data." On 15 July 2014, Jean-Claude Juncker released his "Agenda for Jobs, Growth, Fairness and Democratic Change" which listed "A Connected Digital Single Market" as his first priority. Juncker wished to complete the data legislation overhaul within his first six months, because, "Information and Communications Technology (ICT) is no longer a specific sector but the foundation of all modern innovative economic systems."[484] Digital economic growth required data protection legislation that reduced the fragmentation within national legislation. Crafting such a law challenged regional cooperation within Europe *and* set up barriers with outside-EU business relationships.

The GDPR replaced the outdated Directive 95 and extends digital human rights in three key ways. First, the law harmonizes EU data protection to "protect people" *and* "ensure free data movement."[485] By providing for data mobility, GDPR keeps intact the goals of the OECD Convention 108, without explicitly mentioning it. Additionally, special provisions were made for the protection requirements set on small and mid-sized businesses in order to reduce the financial burden of firms that employ <250 persons, and for whom providing data protection may be disproportionately expensive. (This helped to address concerns raised by French representatives.)

[484] EU Commission (2015) 192 final, pg. 2.
[485] See points 3, 53, and 150.

Next, national authorities should cooperate on matters of data exchange, such as during security investigations and judicial proceedings (Articles 23, 45 and 50).[486] Finally, third countries are now required to meet the standards of intra-EU protections if the data of EU citizens will be collected by firms from third party states and/or if EU citizens data will be transferred outside the Union.[487] Growing resentment by EU ICT firms against US tech giants like Google motivated the latter provision, in combination with a series of violations by US firms against existing EU data protection laws. *(See Table 27.)*

[486] See point 5, Article 50, Article 61, point 73, point 104,
[487] Point 6

Table 27: EU Data Laws, Auto-coded Content

Year	Legislation	Source/Description	Percentage of Content with Mentions
1993	Maastricht Treaty	Includes brief mention of secrecy responsibilities for data accessible by some EU staff	Security 37% Economics 57% (N=236)
1995	Directive 95/46/EC , Article 1 *	EU Commission: Establishes fundamental rights of natural persons as regarding processing of personal data; forbids restriction of free flow of personal data between Member States	Security 10% Economics 6% Data Protection 19% (N = 258)
1997	Directive 97/66/EC	EU Commission: Proposal for Council Directive on personal data/privacy as relates to public digital telecommunications and mobile networks	Security 23% Economics 27% Data Protection 50% (N=48)
1997	Amsterdam Treaty	Incorporates protection for personal data during automatic processing alongside facilitation of free movement of data	Security 63% Economics 32% Data Protection 2% (N=168)
2000	Treaty of Nice	NO mention of data protection at all	Security 72% Economics 29% (N=95)
2000	Charter of Fundamental Rights	Included the right to protection of personal data; UK opposed this, stating Convention did not have this competency	Security 45% Economics 35% Data Protection 20% (N=20)
2001	Regulation No. 45/2001	EU Commission: Provisions for processing personal data by Community; created European Data Protection Supervisor (EDPS)	Security 8% Economics 3% Data Protection 17% (N=587)
2002	Directive 2002/58/EC	EU Commission: Regulates protection of data and privacy during use by electronics and telecommunications firms	Security 7% Economics 6% Data Protection 19% (N=500)
2006	Directive 2006/24/EC	EU Commission: Requires traffic data retention for 6 mos-2 yrs. for prosecution of serious crimes	Security 9% Economics 4% Data Protection 4% (N=108)
2007	Lisbon Treaty	EU: Modified legal structure by abolishing pillar structure, including past Treaty Provisions for protection of personal data; establishes data protection as a fundamental right by this moving of the issue into a first pillar area of competency	Security 70% Economics 25% Data Protection 4% (N=673)
2008	Directive 2008/977/JHA	Justice and Home Affairs Council framework for data protection during police cooperation	Security 19% Data Protection 14% (N=246)
2012	Code of EU Online Rights, Chapter 4	EU Commission: Establishes basic rights for EU citizens when using online networks and services.	Security 4% Economics 18% Data Protection 24% (N-49)
2016	General Data Protection Regulation 2016/679	EU: Extends the protection of processing of personal data as a fundamental right; preserves free flow of data; mandates third country compliance	Security 10% Economics 3% Data Protection 20% (N=1051)
2016	EU-US Privacy Shield	EU Commission: Establishes minimal standards of processing protection for EU citizens' personal data transferred to US during use of digital marketplace or social media	Security 80% Economics 12% Data Protection 8% (N-352)
Totals	14 Laws		Security 33% Economics 14% Data Protection 13% N=3804 sentences auto-coded

As with the WP documents, when auto-coded, the content of EU data laws reveal that digital human rights has maintained importance in EU law across time since it became a matter of supranational law in 1995. Recall that mention of the security terms can indicate either positive or negative permission for access to personal or cyber data. Economic concerns can also

be worded as to promote or constrain data commodification. However, all of the data protection terms concern positive provision of digital human rights. While the auto-coded method is not ideal for revealing the exact changes to EU data law, it does show the constancy of data protection across time. The numbers of laws that mandate data protection harmonization across the Union has increased since 1995. What began as data protection for economic cooperation purposes, has spread into data protection during information exchanges as a part of police cooperation as well as data protection for the sake of human rights alone.

5.14 Chapter Summary

Table 28: Powerful States Efforts to Shape EU Data Laws

Country	Predicted Policy Preference	Fulfilled Y/N
France	1) Digital human rights 2) Security Access	Yes; Delors Commission opened door for digital human rights. French also pushed for national controls and security access post 9/11.
Germany	Digital human rights	Yes; pressed the Commission for digital human rights.
United Kingdom	1) Data commodification 2) Security Access	Somewhat. Opposed digital human rights multiple times. Less pressure to achieve security access.

EU data legislation has evolved across time. Initial legislation was motivated by pressure from the Council of Europe Convention 108, which laid the groundwork for data protection premised upon technological growth and the growing economic value of data. When EU data protection was under negotiation, the Commission presidents of France and Luxembourg played a crucial role by opening the door of opportunity for data protection to be legislated for the Union. However, it was the presence of epistemic experts within advisory committees such Working Party 29, which had long-term impact. These legal and academic elites advised the Commission to gradually expand the scope of data protection to match up with the preferences of EU states who already had powerful data protection legislation, such as Germany and Sweden,

and to a lesser extent, France. Directive 95 and the Charter of Fundamental Human Rights both codified digital human rights as an area of supranational EU competence, despite frequent opposition by the UK. Today, the GDPR has expanded data protection further still by setting obligation for third party states such as the US to comply when using EU citizens' data. One could argue that this last component is an effort by the EU to globalize the norm of digital human rights.

Digital human rights are likely here to stay, but these rights do have limits. Preserving national security in a post 9/11 world has led EU states to open data access not only to national law enforcement authorities, but also for use by outside security authorities across state lines. Combined with the ongoing financial value of the digital economy, and the question must be asked as to whether digital human rights provide the extent of coverage that the national and supranational laws claim to provide. As things exist, data continues to be seen as an economic commodity and as a tool for preserving national security. Ultimately, states remain sovereign over all that concern citizens, including their personal and cyber data. The rights of individual data subjects are protected only in so far as these individuals are able to understand and adjudicate for protection and control over their own personal and cyber data. Individual data subjects and epistemic legal elites will continue to need to advocate for personal data protection in an atmosphere of data commodification and security fears.

6 DISCUSSION, IMPLICATIONS, FUTURE RESEARCH

This dissertation has contributed additional knowledge to the field of political science as regards data governance, but the findings have implications for social science more broadly in many other areas.

First, supranational EU data legislation occurred as a result of particular domestic changes, namely technological change. Sweden was the first European country to adopt national data protection legislation due to a history of open records access legislation. When records were paper-pound, the population knew others could access government held personal information, but it was not easy to do so. With the advent of computerized data banks, open records access meant sharing of personal data not only between government agencies, but this technological advancement increased the risk that personal information could easily go public in exponential ways. In Germany, computer technology raised the risk of a return to the surveillance state. People living in West Germany recalled Nazi record-keeping as a tool to facilitate genocide. East Germans remembered the mass surveillance state practices of the Stasi under the USSR. Regional data protection moved up to become federal law in Germany and set a precedent of legal norms and legal epistemic experts driving data protection legislation. British human rights advocates and politicians were unsuccessful in achieving data protection legislation introduced in the 1960s and 1970s. The OECD emphasis on data protection legislation raised economic concerns in the minds of the nascent ICT sector of the UK in the 1980s. Without some form of data protection legislation, British firms could be shut out of business opportunities dependent upon data security assurances. The Thatcher government supported and passed data protection laws when it was linked to the potential for economic loss. The primary domestic interests that shaped national laws formed the basis for each state's preferences for EU data legislation when

the window for such policy opened in the late 1980s and early 1990s. We would do well to remember that individual interests differ among states, and that successful introduction of new national legislation often hinges upon links between interest groups.

For researchers studying supranational policymaking in the EU, the path taken from economic to human rights to security concerns about data governance can inform our understanding of EU policymaking as a whole. As noted by several EU scholars, openings within the EU legislative agenda are controlled by the EU Commission. EU data protection began as a mechanism to facilitate EU economic growth. The Delors Commission opened the door for data policy solely because of the economic potential in growing ICT firms within the Single Market. *After* the door was opened for general data protection, human rights experts were able to expand the scope of basic protections to include not just storage and movement requirements, but also added data subject consent, data retention limits, and the right to be forgotten. Finally post 9/11 and the London and Madrid bombings, states' willingness to cooperate in data exchanges during anti-terrorism missions increased significantly. Security attacks expanded the "shared information space" beyond typical state borders to an external EU border. EU data legislation began as an economic issue, transformed into a human rights issue, and then became a security issue. Today, it remains all three albeit in mixed percentages. The fact that data legislation is not an either-or issue exposes the reality that regional policy-making is driven by multiple issue concerns, which happen simultaneously. The complexity of settling shared policies in a globalized world means that policy coordination difficulties are likely to persist, rather than wane.

The third important finding from this dissertation concerns the power of epistemic professionals to influence regional norms around a particular issue. From the very beginning

when the national debate opened for data legislation in Sweden and Germany, both countries relied extensively on legal experts for information and suggestions about the structure of new law to be created. After the laws were made, each of the case countries established a national agency tasked with oversight of both private and public sectors. In Sweden and Germany, the data protection administrations were led by attorneys and judges who brought to government the human rights norms associated with identity-based protections. In contrast, the UK chose a director for their Data Protection Registry who was a former BBC journalist, highlighting the fact that the British linked data protection to concerns about limits to press freedom rather than human rights. Later, leadership of the DPR/ICO shifted to those with legal expertise, *after* EU Directive 95 passed, which mandated data protection harmonization across the Union. Directive 95 included digital human rights and data protections which were much more specific and detailed than the 1984 British data protection law. This required someone with greater professional training in human rights to oversee the adaptation of British law and future EU law compliance in Britain.

The influence of legal elites did not end with the formation of national data legislation and the creation of national data oversight agencies. As theorized in the norm diffusion literature, the DPA leaders of Germany, Sweden, and later France, acted as "norm entrepreneurs" when serving as advisors and consultants to the EU Commission and Council. They successfully spread the digital human rights framework beyond their respective national borders to push for expanded data protection obligations in the EU. The Article 29 Working Party had a tremendous impact on the direction chosen by the Commission and Council regarding changes to Directive 95 and subsequent initiatives that concerned data treatment. The various documents released by WP 29 from 1997-2016 served as the major source of information for the Commission during the

entire period when Directive 95 was the primary EU data law. Serving as the primary source of input during the legislative process around one issue gave the committee a large amount of power over the framing of data governance. They used this power to shift the narrative away from economic-based concerns toward human rights expansion for EU data laws. Even after regional security problems mounted with the increased terror attacks and the refugee crisis of 2015, WP 29 was able to keep the focus of EU data legislation as one of fundamental human rights, despite the competition from economic and security concerns.

Fourth, the policy power held by Working Party 29 speaks to the larger debate about EU democratic deficit. Advisory bodies such as Working Party 29 are not elected by EU citizens in any way. All the members of WP 29 were and are the heads of national data agencies. Their positions as national DPAs are appointed, often by the executive or the Ministry of Justice or Interior. These individuals have not been elected by their own citizens nor were they elected in an EU election. Though the official documents of WP 29 were publicly available online, the committee deliberations were not open to the public nor minutes released for the meetings. There is no indication that they consulted with any of the multiple stakeholders involved in the process of data use, such as ICT firms, members of the public, or law enforcement or security officials. One could argue that the advisory perspective they brought to the EU Commission could have been driven entirely by legal community norms. While this was good for human rights protections, it did not contribute in a meaningful way to the demand for increased accountability and accessibility among EU institutions and bureaucracy. The ongoing complaints about disconnect between Brussels bureaucrats and the EU public is fed by just such levels of disassociation between the EU legislative process and EU citizens. The process and people that

worked seemingly well for EU data policy-making could be exacerbating feelings of democratic deficit.

Furthermore, the EU is changing the global environment for data management in profound ways. The Court of Justice for the European Union and the European Court of Human Rights (ECHR) have shown the willingness and ability to prosecute violators of EU digital human rights. The main oversight body for EU data protection compliance, the European Data Protection Supervisor (EDPS), keeps an online website informing the public of ongoing cases involving violations of data protection.[488] The EDPS has also released working documents outlining current and pending cases in the CJEU and ECHR regarding the cases.[489] The EDPS documents also outline national cases pending on data violations. The courts have not shied away from pursuing high profile targets, such as Google, accused of misuse of personal data in several cases (*Vidal-Hall, Hann and Bradshaw v Google Inc* and *Google v Spain*). The EDPS tackles potential cases involving data protection, net neutrality, encryption, the Charter of Fundamental Human Rights, surveillance, border and immigration issues, biometrics, and police and judicial cooperation. All such areas utilize personal data, and the EDPS has been called on to intervene in cases before the Court of Justice as well as before General Court and the Civil Service Tribunal. All such hearings or cases involve personal or cyber data. Litigants can be individuals, firms, or countries. Through the EU courts, digital human rights have an enforcement mechanism which solidifies these rights alongside more traditional human rights.

Another way the EU has impacted the diffusion of the digital human rights norm is via the mandates of the recently passed General Data Protection Regulation (GDPR). The GDPR expects third countries to comply with all aspects of the data protections included in the law. In a

[488] https://edps.europa.eu/data-protection/eu-institutions-dpo/case-law-guidance_en
[489] EDPS 2015

practical sense this solidifies practices that emerged after Directive 95 which held outside countries and firms in those countries accountable for how they were managing the data of EU citizens. The EU attempted to allow "self-policing" of non-EU firms when it signed the Safe Harbour agreement with the United States. The Safe Harbour agreement permitted data controllers outside the EU within the US to transfer personal data to the US when voluntarily complying with EU data protections. The US Federal Trade commission was given oversight of compliance. In reality, not all US firms that used EU data fully complied. In 2013, the EU Commission requested an audit of the agreement and its outcomes.[490] The Commission action was taken at the request of German regulators who felt that US assurances of compliance were less than accurate. The issue was taken to the Court of Justice, which ruled in October of 2015 in *Schrems v Data Protection Commissioner* that Safe Harbour was invalid as a protection tool.[491] The topic was carried into the discussion about changing needs of data protection in the 21st century. Safe Harbour was replaced with a more stringent agreement with the US, known as the EU-US Privacy Shield. Free transfers of EU citizens' data are permitted when the firms are registered with the EU. In addition, Directive 95 was replaced with the GDPR. With the GDPR, lawmakers considered the recommendation made by the Article 29 Working Party, which had suggested that cloud computing firms were susceptible of skirting the protection requirements. The GDPR requires compliance with EU data law outside the EU, whether the third country has a similar law in place or not, applicable to all countries outside the EU. With the GDPR and the Privacy Shield, the EU is attempting to export the norm of digital human rights.

Finally, this dissertation shows the growing importance of non-state actors in the EU legislative process and within intergovernmental organizations (IGOs). The ICT sector pushed

[490] Treacy 2013
[491] Davidson 2017

through data protection in the UK when the government had resisted it for twenty years. German and Swedish attorneys successfully achieved human rights protections for data less than ten years after computerized databanks were adopted by public administrators, and diffused protections to cover private sector use as well. Certain human rights advocates (Spiros Simitis, Paul Sieghart) moved back and forth between their home countries, EU advisory panels, and committees in the OECD and Council of Europe, testifying before decision-makers in all of these places as to the importance of digital human rights. Individuals and firms have been accused of data violations before national courts and called to account for their accused crimes. Returning to the story told in the introduction, after the Cambridge Analytica scandal, Mark Zuckerberg and Cambridge Analytica executives were asked to testify before Members of European Parliament and the House of Commons to explain how and why the extensive use and perhaps abuse of personal data is justified given data legislation in the EU.[492] Originally, executives attempted to explain the overreach of third party actors, arguing that personal and cyber data abuse was neither intended nor sanctioned. Now, Zuckerberg is attempting to control the digital human rights narrative by offering an op-ed in the New York Times, advising lawmakers on what areas of data governance they should better focus upon, namely "harmful content, election integrity, privacy, and data portability."[493] It would seem that data brokers are moving from the defense to the offense in the battle for control over digital human rights.

Ultimately, personal and cyber data is forever linked to the individual. This link intrinsically gives it both economic and security value. Powerful data brokers like Facebook and Google cannot function without data; it is the core of a business model that relies upon surveillance capitalism as its fuel. However, as seen with the Cambridge Analytica, and various

[492] BBC 2018; Parliament UK 2018.
[493] Isaac/New York Times 2019

other recent data breaches that have received press coverage, the public does not like the thought that third parties are using their data – particularly data tied to personal beliefs. Because data can expose an individual's religious, political, or ethical values, there are aspects of data use that may not be as tolerated by the data creators – the public. This is where epistemic elites within the legal and human rights community have leverage to bridge between governments and the public to continue to shape the evolution of data governance. In a world continually threatened by security and economic demands upon data use, the competition between state actors, economic interests, and the human rights community is likely to continue. For now, we live in a data-driven world that at least within the EU, does have digital human rights protections in place.

BIBLIOGRAPHY

2001. September 3. Accessed December 20, 2018. https://www.munzinger.de/search/portrait/Hans+Peter+Bull/0/15205.html .

n.d. https://www.cvce.eu/obj/speech_by_romano_prodi_strasbourg_14_september_1999-en-a4c723ef-383a-435d-ad90-581e0ee856d0.html .

Abbott, Kenneth W., and Duncan Snidal. 1998. "Why States Act Through Formal International Organizations." *Journal of Conflict Resolution* 42 (1): 3-30.

Acharya, Amitav. 2004. "How Ideas Spread: Whose Norms Matter? Norm Localization and Institutional Change in Asian Regionalism." *International Organization* 58: 239-275.

Acharya, Amitav. 2011. "Norm Subsidiarity and Regional Orders: Sovereignty, Regionalism, and Rule-Making in the Third World." *International Studies Quarterly* 55: 95-123.

Aggarwal, Venod K., ed. 1998. *Institutional Designs for a Complex World: Bargaining, Linkages, and Nesting.* Ithaca, NY: Cornell University Press.

Aggarwal, Vinod K. 2005. "Reconciling Institutions: Nested, Horizontal, Overlapping, and Independent Institutions." *Memo.* February 13.

https://www3.nd.edu/~ggoertz/rei/reidevon.dtBase2/Files.noindex/pdf/2/Aggarwal%20memo.pdf.

Ahearn, Raymond J., and Paul Belkin. 2010. *The German Economy and U.S.-German Economic Relations.* CRS Report for Congress, Washington, DC: Congressional Research Service .

Alcantara, Chris. 2017. *46 years of terrorist attacks in Europe, visualized.* July 17. Accessed May 16, 2018. https://www.washingtonpost.com/graphics/world/a-history-of-terrorism-in-europe/.

Aldrich, John H. 1995. *Why Parties? The Origin and Transformation of Political Parties in America.* Chicago, IL: Chicago University Press.

Alter, Karen J., and Sophie Meunier. 2009. "The Politics of International Regime Complexity." *Perspectives on Politics* 7 (1): 13-24.

Anderson, Christina, and Alan Cowel. 2018. *Was the Killer of Sweden's Leader in 1986 Under Investigators' Noses All This Time?* May 24. Accessed September 16, 2018.

https://www.nytimes.com/2018/05/24/world/europe/sweden-olof-palme-killing.html.

Anderson, Stanley V. 1973. "Public Access to Government Files in Sweden." *American Journal of Comparative Law* 21 (3): 419-473.

Article 29 Working Party. 2016. "Statement of the Article 29 Working Party on the Opinion of the EU-U.S. Privacy Shield." Brussels, BE: Europa, April 13.

—. 2015. "The Court of Justice of the European Union invalidates the EU Commission Safe Harbor Decision." *Press Release.* Brussels, BE: Europa, October 6.

Aust, Stefan. 2008. *Baader-Meinhof: The Inside Story of the RAF.* Oxford: Oxford University Press.

Australian Financial Review. 1988. "EUROPE POOR PERFORMER IN HIGH-TECH STAKES." *Australian Financial Review* 25.

Ayoub, Phillip M. 2015. "Contested norms in new-adopted states: International determinants of LGBT rights legislation." *European Journal of International Relations* 21 (2): 293-322.

Bačić, Nika. 2012. "Asylum Policy in Europe - Competence of the European Union and Inefficiency of the Dublin System." *Croatian Yearbook of European Law and Policy* 8: 41-76.

Bache, Ian, Simon Bulmer, Stephen George, and Owen Parker. 2015. *Politics in the European Union.* Oxford: Oxford University Press.

Bamberger, Kenneth A., and Deirdre K. Mulligan. 2013. "Privacy in Europe: Initial Data on Governance Choices and Corporate Practices." *George Washington Law Review* 81 (5): 1529-1664.

Bamford, Bradley W. C. 2005. "The role and effectiveness of intelligence in Northern Ireland." *Intelligence and National Security* 20 (4): 581-607.

Bank, World. n.d. *World Development Indicators.* WDI.

Barnett, Michael N., and Martha Finnemore. 1999. "The Politics, Power, and Pathologies of International Organizations." *International Organization* 53 (4): 699-732
.

Barroso, José Manuel Durão. 2013. "State of the Union address 2013." *European Parliament plenary session.* Strasbourg, FR: European Commission, September 11.

BBC News. 2005. *On this Day - 24 April.* Accessed September 2016, 2018. http://news.bbc.co.uk/onthisday/hi/dates/stories/april/24/newsid_2523000/2523095.stm.

—. 2017. *Swedish 'laser man' Ausonius on trial for 1992 German murder.* December 13. Accessed September 18, 2018. https://www.bbc.com/news/world-europe-42340711.

BBC News World Edition. 2002. October 19. Accessed February 5, 2019. http://news.bbc.co.uk/2/hi/europe/2341659.stm.

BBC News. 2018. *Zuckerberg's European Parliament testimony criticised.* May 22. Accessed April 2019. https://www.bbc.com/news/technology-44210800.

BBC World News. 2016. *Who were Germany's Red Army Faction militants?* January 19. Accessed December 5, 2018. https://www.bbc.com/news/world-europe-35354812.

Becker, Jillian. 1977. *Hitler's Children: The Story of the Baader-Meinhof Terrorist Gang.* Philadelphia, PA: J.B. Lippincott Co.

Benford, Robert D., and David A. Snow. 2000. "Framing Processes and Social Movements; An Overview and Assessment." *Annual Review of Sociology* 26: 611-639.

Bennett, Andrew, and Jeffrey T. Checkel, . 2015. *Process Tracing: From Metaphor to Analytic Tool.* Cambridge: Cambridge University Press.

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

—. 1992. *Regulating Privacy: Data Protection and Public Policy in Europe and the United States.* Ithaca, NY: Cornell University Press.

—. 1982. *The Concept of Open Government and its Interpretation and Development in British Politics.* Cardiff: University College of Cardiff.

Berman, Sheri. 2006. *The Primacy of Politics: Social Democracy and the Making of Europe's Twentieth Century.* Cambridge, NJ: Cambridge University Press.

Betts, Alexander. 2013. "Regime Complexity and International Organizations: UNHCR as a Challenged Institution." *Global Governance* 19: 69-81.

Birkland, Thomas A. 2016. *An Introduction to the Policy Process: Theories, Concepts and Models of Public Policy Making.* Fourth. New York, NY: Routledge.

Bourn, Colin, and John Benyon. 1983. *Data Protection: Perspectives on Information Privacy.* Conference Proceedings, Leicester: University of Leicester.

Braibant, Guy. 2001. *La Charte des Droits fondamentaux de l'Union européenne.* Paris, FR: Points Sueil.

Breindl, Yana, and Francois Briatte. 2013. "Digital Network Repertoires and the Contentious Politics of Digital Copyright in France and the European Union." *Policy and Internet* 1: 27-55. Accessed June 6, 2018.

Brooking, Emerson T., and P.W. Singer. 2016. "War Goes Viral: How Social Media is Being Weaponized." *The Atlantic* 70-83.

Bull, Hans Peter. 1984. *Datenschutz oder die Angst vor dem Computer.* München : Piper.
—. 1984. *Datenschutz oder die Angst Vor Dem Computer.* München, DE: Piper.

Burton-Jones, Alan. 1999. *Knowledge Capitalism: Business, Work and Training in the New Economy.* Oxford: Oxford University Press.

Butchart, R.L. 1987. "A new UK definition of the high-technology industries." *Economic Trends* 400: 82-88.

Byers, Angela. 2015. "Big Data, Big Economic Impact?" *Journal of Law and Policy for the Information Society* 10 (3): 757-764.

Cacaly, Serge, and Yves-François Le Coadic. 2007. "Fifty years of scientific and technical information policy in France (1955-2005)." *Journal of Information Science* 33 (3): 377-384.

Cardenas, Sonia. 2004. "Norm Collision: Explaining the Effects of International Human Rights Pressure on State Behavior." *International Studies Quarterly* 6 (2): 213-231.

Carothers, Thomas. 1999. *Aiding Democracy Abroad: The Learning Curve.* Carnegie Endowment for International Peace.

Cassini, Sandrine. 2016. "'Safe Harbor': Gattaz tire le signal d'alarme' (Safe Harbor: Gattaz rings the alarm bell)." *Le Monde.* Paris: http://www.lemonde.fr/economie/article/2016/01/09/fin-du-safe-harbor-gattaz-tire-la-sonnette-d-alarme_4844356_3234.html, January 9.

Cattaneo, Gabriella, Mike Glennon, Rosanna Lifonti, Giorgio Micheletti, Alys Woodward, Marianne Kolding, and David Osimo. 2016. *European Data Market SMART/2013/0063.* D8- Second Interim Report, European Commission, DG Connect, Luxembourg: IDC.

Cavelty, Myriam Dunn. 2013. "From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discource." *International Studies Review* 15: 105-122.

CBS Evening News. 2016. *September 6, 1972: World learns of Munich Olympics Massacre.* September 6. Accessed December 19, 2018. https://www.cbsnews.com/news/on-this-day-september-6-1972-world-learns-of-munich-olympics-massacre/.

Cette, Gilbert, Christian Clerc, and Lea Bresson. 2015. "Contribution of ICT Diffusion to Labour Productivity Growth: The United States, Canada, the Eurozone, and the United Kingdom, 1970-2013." *International Productivity Monitor* (28): 81-88.

Chanley, Virginia A. 2002. "Trust in the Government in the Aftermath of 9/11: Determinants and Consequences." *Political Psychology* 469-483.

Checkel, Jeffrey T. 1997. "International Norms and Domestic Politics: Bridging the Rationalist-Constructivist Divide." *European Journal of International Relations* 3 (4): 473-495.

Cheneval, Francis. 2017. "Towards Property-Owning Democracy by Private Property of Personal Data." *Centre for Technology and Global Affairs.* Accessed January 1, 2017 . https://www.ctga.ox.ac.uk/event/towards-property-owning-democracy-private-property-personal-data.

Chong, Dennis, and James N. Druckman. 2011. "Chapter 13: Identifying Frames in Political News." In *The Sourcebook for Political Communications Research: Methods, Measures, and Analytical Techniques*, edited by Erik P. Bucy and R. Lance Holbert, 238-267. London: Routledge.

Choucri, Nazli. 2012. *Cyberpolitics in International Relations.* Cambridge, MA: Massachusetts Institute of Technology.

Clarke, Richard A. 2016. "The Risk of Cyber War and Cyber Terrorism." *Journal of International Affairs* 179-181.

Colarik, Andrew Michael. 2006. *Cyber Terrorism: Political and Economic Implications.* Hershey, PA: Idea Group.

Comité des Sages. 1996. *For a Europe of civi and social rights.* Comité des Sages chaired by Maria de Lourdes Pintasilgo, Brussels: Office for Official Publications of the European Community.

Commission Informatique et Libertés. 1975. "Rapport de la Commission Informatique et Libertés, "Tricot Report"." Paris.

Commission of the European Communities. 1990 (13 September). "Commission Communication on the protection of individuals in relation to the processing of personal data in the Community and information security." *COM (90) 314 final - SYN 287 and 288.* Brussels: European Union.

Commission of the European Communities. 7 December 2005. *Communication from the Commission to the Council and the European Parliament.* Interim report on the follow up to the informal meeting of Heads of State and Government at Hampton Court, Brussels, BE: European Union.

—. 1995. "Opinion of the Commission pursuant to Article 189 b (2)(d) of the EC Treaty, on the European Parliament's amendments to the Council's common position regarding the proposal for a European Parliament and Council Directive on the protection of individuals." *COM (95) 375 final-COD287.* Brussels, BE: Official Journal of the European Communities, July 18.

Commission of the European Communities. 1992. *Proposal for a Council Directive on the legal protection of databases.* COM (92) 24 final - SYN 393, Brussels, BE: European Union.

Commons Select Committee. 2018. *Alexander Nix to appear again before the committee.* June 7. Accessed April 2019. https://www.parliament.uk/business/committees/committees-a-z/commons-select/digital-culture-media-and-sport-committee/news/fake-news-nix-evidence-17-192/.

Cornford, James. 1981. "The Prospects for Privacy." *The Political Quarterly.*

Council of Europe. 1950. *Convention for the Protection of Human Rights and Fundamental Freedoms.* Rome, 4.XI.1950, Amended 2010, Rome, IT: Council of Europe.

Council of Europe. 2001. *Convention on Cybercrime.* Budapest: Council of Europe.

Council of Europe. 2001. *European Treaty Series No. 185: Convention on Cybercrime.* Strasbourg, FR: Council of Europe.

Council of Foreign Relations. 2018. *Cyber Operations Tracker.* Accessed May 10, 2018. https://www.cfr.org/interactive/cyber-operations.

Council of Ministers. 1974. "Council Resolution of 15 July 1974, on a Community policy on data processing No C 86/1." Strasbourg, FR: European Union, July 15.

Council of the European Communities. n.d. *Council Decision of 5 October 1987 introducing a communications network Community programme on trade electronic data interchange systems (TEDIS).* 87/499/EEC, Brussels, BE: European Union.

Council of the European Communities, Commission of the European Communities. 1992. "Treaty on the European Union." Accessed April 6, 2019. https://europa.eu/european-union/sites/europaeu/files/docs/body/treaty_on_european_union_en.pdf.

Council of the European Community. 1988. "Council Resolution of 30 June 1988 on the development of the common market for telecommunications services to 1992." *Official Journal of the European Union, 88/C 257/01.* Brussels: European Union.

Custers, Bart, Simone van der Hof, and Bart Schermer. 2014. "Privacy Expectations of Social Media Users: The Role of Informed Consent in Privacy Policies." *Policy & Internet* 6 (3): 268- 295.

DALK . 1978. "DALK Report on the Revision of the Data Act/Statens ofentliga utredningar."

Dammann, Ulrich. 1977. *Data protection legislation : an international documentation.* Frankfurt: Metzner.

—. 1977. *Data Protection Legislation: An International Documentation.* Frankfurt: Frankfurt am Main.

Davidson, Rosemary. 2017. "Brexit and Criminal Justice: the Future of the UK's Cooperation Relationship with the EU." *Criminal Law Review* (Thomson Reuters) 5: 379-395.

Davis, Christina L. 2009. "Overlapping Institutions in Trade Policy." *Perspectives in Politics* 7 (1): 25-31.

Deibert, Robert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain. 2010. *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace.* Cambridge, MA: MIT Press.

Deibert, Ronald J. 2013. *Black Code: Surveillance, Privacy, and the Dark Side of the Internet.* McClelland & Stewart.

della Porta, Donatella. 1999. "Protest, Protesters, and Protest Policing: Public Discourses in Italy and Germany from the 1960s to the 1980s." In *How Social Movements Matter*, edited by Marco Giugni, Doug McAdam and Sidney Tarrow, 66-96. Minneapolis, MN: University of Minnesota Press.

Der Speigel. 2007. "Immer radikaler: Interview mit Daniel Cohn-Bendit." *Der Spiegel.*

Der Spiegel. 1977. November 14. Accessed December 19, 2018. http://www.spiegel.de/spiegel/print/d-40764083.html .

—. 1977. "Professor Spiros Simitis." November 14.

Directorate-General for Internal Policies. 2015. "Policy Department C: Citizens' Rights and Constitutional Affairs." *Big Data and Smart Devices and Their Impact on Privacy.* Study for the LIBE Committee.

Directorate-General: Telecommunications, Information Industries and Innovation. 1987 (28-29 September). *ESPRIT '87 Achievements and Impact Part 2: Proceedings of the 4th Annual EPSPRIT Conference.* Brussels, BE: Commission of the European Community
.

Domingo, Bruno. 2010. "National Borders, Surveillance, and Counter-Terrorism Tools in France before and after 9/11." In *Border Security in the Al-Qaeda Era*, by John A. Winterdyk and Kelly W. Sundberg, 121-158. Boca Raton, FL, USA: Taylor & Francis Group.

Downs, Anthony. 1957. *An economic theory of democracy.* New York, NY: Harper.

Drezner, Daniel W. 2007. *All Politics is Global: Explaining International Regulatory Regimes.* Princeton, NJ: Princeton University Press.

Dunleavy, P., H. Margetts, S. Bastow, and J. Tinkler. 2006. *Digital Era Governance: IT Corporations, The State, and E-Government.* Oxford: Oxford University Press.

Dworkin, Gerald. 1973. "The Younger Committee Report on Privacy." *The Modern Law Review* 36 (4): 399-406
.

Edgar, Timothy H. 2017. *Beyond Snowden: Privacy, Mass Surveillance, and the Struggle to Reform the NSA.* Washington, DC, USA: Brookings Institution Press.

Elmore, Richard, Gunnel Gustafsson, and Erwin Hargrove. 1986. "Comparing Implementation Processes in Sweden and the United States." *Scandinavian Political Studies* 9.

Eltantawy, Nahed, and Julie B. Wiest. 2011. "Social Media in the Egyptian Revolution: Reconsidering Resource Mobilization Theory." *International Journal of Communications* 5: 1207-1224.

Endo, Ken. 1999. *The Presidency of the European Commission under Jacques Delors: the Politics of Shared Leadership.* London, UK: Macmillan Press Ltd.

EU Economic and Social Committee. 1987. "Opinion on the communication by the Commission entitled 'Towards a dynamic European economy – Green Paper on the development of the common market for telecommunications services and equipment." *Opinion on 11 November 1987; 87/C 356/12.* Brussels: European Commission.

European Commission. 2015. *COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS A Digital Single Market Strategy for Europe.* COM/2015/0192 final, Brussels: EUR-Lex.

European Commission. 1975. "(1975) Commission proposal for second series of priority projects in data processing at a cost of 23 million units of account ." *Information Memo P-55/75,.* Brussels, BE: European Union, September.

—. 1978. "Annual Report of the Data-Processing Departments of the Commission." *COM (78) 347 final.* Brussels: European Union, July 21.

—. 1981. "Commission Recommendation of 29 July 1981 relating to the Council of Europe convention for the protection of individuals with regard to automatic processing of personal information." *81/679/EEC.* Brussels, BE: Official Journal of the European Communities, July 29.

—. 2012. "COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS." *Safeguarding Privacy in*

a Connected World A European Data Protection Framework for the 21st Century. Brussels, BE: European Union, January 25.

—. n.d. *Data Protection: Legislation.* Accessed December 7, 2017. http://ec.europa.eu/justice/data-protection/law/index_en.htm.

—. 2011. "Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EE." *Code of EU Online Rights: OJ L 304.* Luxembourg: European Union, November 22.

European Commission. 2017. *Enter the Data Economy: EU Policies for a Thriving Data Ecosystem.* EPSC Strategic Notes of the EU Commission President, Brussels: European Political Strategy Centre.

—. 2012 . "European Commission launches accelerated infringement proceedings against Hungary over the independence of its central bank and data protection authorities as well as over measures affecting the judiciary." *PRESS RELEASE.* Strasbourg, FR, January 17.

—. 1994. "Growth, competitiveness and unemployment, White Paper follow-up." *Report on Europe and the global information society, Interim report on trans-European networks, Progress report on employment.* Luxembourg: Office for the Official Publications of the European Communities, February.

—. 2014. "PRESS RELEASE No 53/14: Commission v Hungary." *By prematurely bringing to an end the term served by its Data Protection Supervisor, Hungary has infringed EU law.* Luxembourg, April 8.

—. 1994. "Press Release, Bangemann Report." *High level group in information society.* Brussels: CORDIS: European Commission, February 15.

European Commission. 2015. *Why we need a Digital Single Market.* Brussels: EU Commission.

European Community. 1992. "Treaty on European Union: OJC 191, 29.7.1992, p.1-112." *Eur-Lex.* July 29. Accessed February 14, 2019. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:11992M/TXT&qid=1550177766903&from=EN.

European Court of Justice. 2003. "http://curia.europa.eu/juris/document/document.jsf?docid=48382&doclang=en." *Judgment of the Court.* Luxembourg: InfoCuria: Case-Law of the Court of Justice, November 6.

European Data Protection Supervisor. 2016. *Case Law Overview 1 December 2014-31 December 2015: Working Document.* March 15.

—. n.d. *Case-Law and Guidance.* Accessed April 2019. https://edps.europa.eu/data-protection/eu-institutions-dpo/case-law-guidance_en.

European Data Protection Supervisor, Policy & Consultation, Supervision & Enforcement Units. 2016. "Working Document, Case Law Overview, 1 December 2014-31 December 2015." Luxembourg, LU: European Data Protection Supervisor, March 15.

European Parliament and of the Council. 1997. "Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector." Brussels, BE: Official Journal of the European Communities, December 15.

—. 1999. "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 by the institutions and bodies of the Community and on the free movement of such data." *1999/C 376 E/04.* Brussels: Official Journal of the European Commission, September 17.

European Parliament and The Council of Ministers. 1995. *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.* Directive, Brussels: EUR-Lex.

European Parliament. 24 February 2005. *Commission legislative and work programme (2005) C304 E/386.* European Parliamentn resolution on the Commission's legislative and work programme for 2005, Brussels, BE: Official Journal of the European Union.

European Parliament Council. 2004. "Decision of the European Parliament and of the Council of 22 December 2003 appointing the independent supervisory body for in Article 286 of the

EC Treaty (European Data Protection Supervisor)." *2004/55/EC.* Brussels, BE: Official Journal of the European Union, December 22.

European Parliament. 1995. "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data nd on the free movement of such data." *No L 281/31.* Brussels: Official Journal of the European Communities, November 23.

—. 2019. "Rules of Procedure 2014-2019." Strasbourg, Brussels: European Union, February.

—. 1983. "Working Document 1-42/83." *Oral Question (0-173/82): Drawing up of a Community Directive on the proteciton of the rights of the individual in the face of technical development sin data processing.* Strasbourg, FR: European Communities, March.

—. 1976. "Working Documents 1976-1977." *Motion for a Resolution on the protection of the rights of the individual in the face of developing technical progress in the field of automatic data processing.* Strasbourg, FR: European Union, April 6.

European Parliament, Office of the President. 2018. *Answers from Facebook to questions asked during Mark Zuckerberg meeting.* May 23. Accessed May 25, 2018. Why did Europe, and the EU in particular, have a more aggressive policy stance toward protecting cyber data than did other regions? .

European Union. 2000. *Charter of the Fundamental Rights of the European Union.* Directive 2000/C 364/01, Brussels, BE: Official Journal of the European Communities.

European Union Commission. 1973. *Communication by the Commission of the European Communities Concerning a Community Policy for Data Processing.* Information Memo P-63/73, SEC (73) 4300, final, Brussels, BE: European Union.

European Union. 2014. "COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS A Digital Single Market Strategy for Europe." *EUR-Lex.* July 15. Accessed December 1, 2017. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwiyu_2NxOnXAhWDQiYKHRKUB48QFggpMAA&url=http%3A%2F%2Feur-lex.europa.eu%2Flegal-

content%2FEN%2FTXT%2F%3Furi%3Dcelex%253A52015DC0192&usg=AOvVaw0r4zq-qZFhJD83xzd81Hpc.

—. 2007. "Consolidated Version of the Treaty on the Functioning of the European Union." *C 326/146.* Brussels, BE: Official Journal of the European Union.

European Union. 1995. *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.* Brussels: European Commission.

—. 2007. "Final Act: Treaty of Lisbon." *2007/C 306/02.* Brussels, BE: Official Journal of the European Union, December 17.

—. 1973. "Information Memo, P-63-73." *SEC (73) 4300 final.*

—. 2016. "REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016." *EUR-Lex.* May 4. Accessed November 15, 2017. http://data.europa.eu/eli/reg/2016/679/oj.

European Union. 2016. *Regution (EU) 2016/679 of the European Parliament and the Council of 27 April 2016.* Brussel: Official Journal of the European Union.

European Union. 2016. *Summaries of EU Court Decisions Relating to Data Protection 2000-2015.* Brussels: OLAF European Anti-Fraud Office.

Expert Group on Fundamental Rights. 1999. *Affirming Fundamental Rights in the European Union: Time to Act.* Brussels, BE: European Commission.

Fairfield, Joshua A.T., and Christoph Engel. 2015. "Privacy as a Public Good." *Duke Law Journal* 65 (3): 385-457.

Federal Republic of Germany. 12 February 1981. *Deutscher Bundestag.* Bonn, FRG: Bundestag, 907-909.

Federal Republic of Germany. 1982. "Third Activity Report of the BfD." INPOL, Bonn, FRG.

Finnemore, Martha. 1996. "Norms, Culture, and World Politics: Insights from Sociology's Institutionalism." *International Organization.*

—. 2003. *The Purpose of Intervention: Changing Beliefs About the Use of Force.* Ithaca, NY: Cornell University Press.

Finnemore, Martha, and Kathryn Sikkink. 1998. "International Norm Dynamics and Political Change." *International Organization* 52 (4): 887-917.

Flaherty, David H. 1979. *Privacy and Government Databanks.* London: Mansell.

—. 1989. *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States.* Chapel Hill, NC: University of North Carolina Press.

Florini, Ann. 1996. "The Evolution of International Norms." *International Studies Quarterly* 40: 363-389.

Foyle, Douglas C. 1997. "Public Opinion and Foreign Policy: Elite Beliefs as a Mediating Variable." *International Studies Quarterly* 41: 141-169.

Foyle, Douglas. 2003. "Foreign Policy Analysis and Globalization: Public Opinion, World Opinion, and the Individual." *International Studies Review* 5 (2): 155-202.

Francois, Joseph, and Bernard Hoekman. 2010. "Services Trade and Policy." *Journal of Economic Literature* 48: 642-692.

Franda, Marcus. 2001. *Governing the Internet: The Emergence of an International Regime.* Boulder, CO: Lynne Reinner Publishers.

—. 2001. *Governing the Internet: The Emergence of an International Regime.* Boulder, CO: Lynne Rienner Publishers, Inc.

Friedwald, Michael, J. Peter Burgess, Johann Cas, Rocco Bellanova, and Walter Peissl, . 2017. *Surveillance, Privacy and Security: Citizens' Perspectives.* London: Routledge.

Fuster, González. 2016. *The Emergence of Personal Data Protection as a Fundamental Right of the EU.* Springer.

Garrett, Geoffrey, and George Tsebelis. 1996. "An Institutional Critique of Intergovernmentalism." *International Organization* 50 (2): 269-99.

Garrett, Geoffrey, and George Tsebelis. 1996. "An Institutional Critique of Intergovernmentalism." *International Organization* 50 (2): 269-299.

Gassman, H.P. 1976. "OECD guidelines governing the protection of privacy and transborder flows of personal data." *Computer Networks* 5 (2): 127-141.

George, Alexander L., and Andrew Bennett. 2005. *Case Studies and Theory Development in the Social Sciences.* Cambridge, MA: MIT Press.

Gilbert, Mark. 2012. *European Integration: A Concise History.* Lanham, MD: Rowman & Littlefield Publishers, Inc.

Gilpin, Robert. 1987. *The Political Economy of International Relations.* Princeton, NJ: Princeton University Press.

Global Terrorism Database. 2017. University of Maryland. Accessed May 2018. https://www.start.umd.edu/gtd/.

Godberg, G. 2011. "Rethinking the Public/Virtual Sphere: the Problem with Participation." *New Media & Society* 1: 1-11.

Godberg, G. 2011. "Rethinking the Public/Virtual Sphere: the Problem with Participation." *New Media & Society* 1: 1-11.

Goldsmith, Jack L., and Tim Wu. 2006. *Who Controls the Internet? : Illusions of Control in a Borderless World.* New York, NY: Oxford University Press.

Goldstein, Judith, and Robert O. Keohane. n.d. *Ideas and Foreign Policy: Beliefs, Institutions, and Political Change.* Ithaca, NY: Cornell University Press.

Gordenker, Leon, and Thomas Weiss. 1995. "Pluralising Global Governance: Analytical Approaches and Dimensions." *Third World Quarterly* 16 (3): 357-387.

Gordon, Philip H. 1993. *A Certain Idea of France: French Security Policy and the Gaullist Legacy.* Princeton, NJ, USA: Princeton Press.

Government of Sweden. 1985. *Public Attitudes to Data-Processing in the Information Soceity.* Data inspektionen, Stockholm, SW: Swedish Central Bureau of Statistics.

Government of the United Kingdom. 1987. *Third Report.* Data Protection Registrar, London, UK: Her Majesty's Stationary Office (HMSO), 40-45.

Government of the United Kingdom. 2010. *UK Growth Across Time.* London, UK: ONS Annual Abstract of Statistics.

Gowan, Richard, and Franziska Branter. 2008. *A Global Force for Human Rights? An Audit of European Power at the UN.* Policy Paper, London: European Council on Foreign Relations.

Granville, Kevin. 2018. *Facebook and Cambridge Analytica: What You Need to Know As Fallout Widens.* March 19. Accessed March 27, 2018. https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html.

Gros, Valentin, marieke de Goede, and Beste Isleyen. 2017. "The Snowden Files Made Public: A Material Politics of Contesting Surveillance." *International Political Sociology* 11 (1): 73-89.

Gwiazda, Anna. 2012. "The Europeanisation of regional policy in Poland: did political parties make a difference?" *East European Politics* 29 (2): 226-244.

Haas, Ernst B. 1961. "International Integration: The European and the Universal Process." *International Organization* 15 (3).

Haas, Peter M. 1992. "Epistemic Communities and International Policy Coordination." *International Organization* 46 (1): 1-35.

Haas, Peter M. 1992. "Introduction: Epistemic Communities and International Policy Coordination." *International Organization* 46 (1): 1-135.

Hafner-Burton, Emilie M. 2008. "Sticks and Stones: Naming and Shaming the Human Rights Enforcement Problem." *International Organization* 62: 689-716.

Hafner-Burton, Emilie M. 2009. "The Power Politics of Regime Complexity: Human Rights Trade Conditionality in Europe." *Perspectives in Politics* 7 (1): 33-37.

Hafner-Burton, Emilie M., Miles Kahler, and Alexander H. Montgomery. 2009. "Network Analysis for International Relations." *International Organizations* 63: 559-92.

Hafner-Burton, Emilie M., Miles Kahler, and Alexander H. Montgomery. 2009. "Network Analysis for International Relations." *International Organizations* 63: 559-592.

Hafner-Burton, Emilie, Miles Kahler, and Alexander H. Montgomery. 2009. "Network Analysis for International Relations." *International Organizations* 63: 559-592.

Hall, Peter A., and David Soskice, . 2013. *Varities of Capitalism: The Institutional Foundations of Comparative Advantage.* Oxford: Oxford University Press.

Hancock, William L. 1994. "Counterterrorism in Great Britain, Germany, and France: 1968 to the Present." Winnepeg, Manitoba: Department of Political Studies, October.

Hanshew, Karrin. 2010. "Daring More Democracy: Internal Security and the Social Democratic Fight against West German Terrorism." *Central European History* 43: 117-147.

Hathaway, Oona A. 2007. "Why Do Countries Commit to Human Rights Treaties?" *The Journal of Conflict Resolution* 51 (4): 588-621.

Herb, Michael. 2017. "Discussion of Cross-Case Analyses." Atlanta, GA: Georgia State University, Political Science Department, April 3.

Herold, Horst. 1968. "Organisatorische Grundzuge der elektronischen Datenverarbeitung im Bereich der Poizei." In *Taschenbuch fur Kriminalisten*, 240-254.

Heuser, Stefan. 2008. "Is There a Right to Have Rights? The Case of the Right of Asylum." *Ethic Theory Moral Practice* 3-13.

Hijmans, Hielke. 2016. *The European Union as guardian of Internet privacy : the story of Art 16 TFEU.* Springer.

Hillebrecht, Courtney. 2012. "Implementing international human rights law at home: Domestic politics and the European court of human rights." *Human Rights Review* 13 (3): 279-301.

Hintz, Arne, and Stefania Milan. 2009. "At the Margins of Internet Governance: Grassroots Tech Groups and Communications Policy." *International Journal of Media and Cultural Politics* 5 (1-2): 23-38.

Hix, Simon, and Christopher Lord. 1997. *Political Parties in the European Union.* New York, NY: St. Martin's Press.

Hofmann, Stephanie C. 2009. "Overlapping Institutions in the Realm of International Security: The Case of NATO and ESDP." *Perspectives in Politics* 7 (1): 45-52.

Holsti, Ole R. 2007. *Public Opinion and American Foreign Policy.* Ann Arbor, MI: University of Michigan Press.

Hondius, Frits W. 1980. "Data Law in Europe." *Stanford Journal of International Law* 16: 87-111.

Hopping, Clare. 2019. *Who is the Information Commissioner, what powers do they have, and how will the ICO enforce GDPR?* January 4. https://www.itpro.co.uk/information-commissioner/31751/what-is-the-information-commissioner-s-office-ico.

Hornero, Antonia Calvo, Francisco J. Fonseca Morilla, and Marcelino Oreja. 1998. *El Tratado de Amsterdam de la Unión Europea : Análisis y comentarios.* Madrid, SP: McGraw-Hill.

House of Lords. 1973. *HL Debate* . Vol. 343, London, UK: United Kingdom, cc104-78.

Huddy, Leon. 2013. "From Group Identity to Political Cohesion and Commitment." In *Oxford Handbook on Political Psychology*, edited by Leone Huddy, David O. Sears and Jack S. Levy, 738-764. Oxford: Oxford University Press.

Huddy, Leonie, Stanley Feldman, Charles Taber, and Gallya Lahav. 2005. "Threat, Anxiety, and Support of Antiterrorism Policies." *American Journal of Political Science* 49 (3): 593-608.

Huddy, Leonie, Stanley Feldman, Theresa Capelos, and Colin Provost. 2002. "The Consequences of Terrorism: Disentangling the Effects of Personal and National Threat." *Political Psychology* 23 (3): 488-510.

Hussain, Muzammil M. 2014. "Digital Infrastructure Politics and Internet Freedom Stakeholders After the Arab Spring." *Journal of International Affairs* 68 (1): 37-56.

Ilshammer, Lars. 2007. "When Computers Became Dangerous: The Swedish Computer Discourse of the 1960s." *Human IT* 9 (1): 6-37.

Inglehart, Ronald F. 2008. "Changing Values Among Western Publics from 1970-2006." *West European Politics* 31 (1-2): 130-146.

International Monetary Fund. 2018. *Measuring the Digital Economy.* Staff Report, Washington, DC: IMF.

Isaac, Mike. 2019. "Mark Zuckerberg's Call to Regulate Facebook, Explained." *The New York Times*, March 30.

Jervis, Robert. 1982. "Security Regimes." *International Organization* 36 (2): 357-378.

Johansson, Magnus. 1993. "Informationssamhällets rötter ur ett svenskt per- spektiv." In *Brus över landet: om informationsöverflödet, kunskapen och människan.*, edited by Lars Ingelstam and Lennart Sturesson. Carlssons.

Johnson, Loch K., Richard J. Aldrich, Christopher Moran, David Barrett, Glenn Hastedt, Robert Jervis, Wolfgang Krieger, et al. 2014. "An INS Special Forum; Implications of the Snowden Leaks." *Intelligence and National Security* 29 (6): 793-810.

Jolly, Leuan, and Loeb & Loeb. 2017. *Data protection in the United States.* July 1. Accessed April 20, 2018. https://uk.practicallaw.thomsonreuters.com/6-502-0467?transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1.

Jorgensen, Rikke Frank. 2017. "What Platforms Mean When They Talk About Human Rights." *Policy and Internet* 9 (3): 280-296.

Jorgensen, Rikke Frank, and Tariq Desai. 2017. "Right to Privacy Meets Online Platforms: Exploring Privacy Complains against Facebook and Google." *Nordic Journal of Human Rights* 35 (2): 106-126.

Jorgensen, Rikke Frank, and Tariq Desai. 2016. "Right to Privacy Meets Online Platforms: Exploring Privacy Complaints against Facebook and Google." *Nordic Journal of Human Rights* 35 (2): 106-126.

Joyce, Daniel. 2015. "Internet Freedom and Human Rights." *The European Journal of International Law* 26 (2): 493-514.

Kaarbo, Juliet. 2015. "Foreign Policy Analysis Perspective on the Domestic Turn in IR Theory." *International Studies Review* 16 (2): 189-216.

Kaarbo, Juliet. 1997. "Prime Minister Leadership Styles in Foreign Policy Making: A Framework for Research." *Political Psychology* 18 (3): 553-581.

Kahneman, Daniel, and Amos Tversky. 1979. "Prospect Theory: An Analysis of Decision Under Risk." *Econometrica (pre-1986)* 47 (2).

Karpf, David. 2016. *Analytic Activism: Digital Listening and the New Political Strategy.* New York, NY: Oxford University Press.

Kassim, Hussein. 2001. "Co-ordinating Action in Brussels." In *The National Co-ordination of EU Policy: The European Level*, edited by Hussein Kassim, Anand Menon, B. Guy Peters and Vincent Wright, 4-43. Oxford: Oxford University Press.

Kassim, Hussein, Anand Menon, B. Guy Peters, and Vincent Wright, . 2001. *The National Co-ordination of EU Policy: The European Level.* Oxford: Oxford University Press.

Katzenstein, Peter J. 1998. *Left-Wing Violence and State Response: United States, Germany, Italy, and Japan, 1960s-1990s.* Working Paper 98, Cornell University, Ithaca, NY: Institute for European Studies.

Katzenstein, Peter J. 2003. "Same War - Differnt Views: Germany, Japan, and Counterterrorism." *International Organization* 57: 731-760.

—. 1990. *West Germany's Internal Security Policy: State and Violence in the 1970s and 1980s.* Edited by Occasional Paper 28. Cornell Studies in International Affairs. Ithaca, NY: Cornell University Press.

Keck, Margaret E., and Kathryn Sikkink. 1998. *Activists beyond Borders: Advocacy Networks in Transnational Politics.* Ithaca, NY: Cornell University Press.

Keeble, D.E. 1989. "High-technology industry and regional developmen in Britain: the case of the Cambridge Phenomenon." *Environment and Planning C: Government and Policy* 7: 153-172.

Kello, Lucas. 2017. *The Virtual Weapon and International Order.* New Haven, CT: Yale University Press.

Kelly, T., and D. Keeble. 1988. "Locational change and corporate organisation in high-tech industry; computer elctronics in Great Britain." *Tijdschrift voor Economische en Sociale Geografie* 79: 2-15.

Kenyon, Andrew T. 2016. "Defamation and privacy in an era of 'more speech'." In *Comparative Defamation and Privacy Law*, 1-16. Cambridge: Cambridge University Press.

Keohane, Robert O. 2005. *After Hegemony: Cooperation and Discord in the World Political Economy.* Princeton, NJ: Princeton University Press.

Keohane, Robert O., and Joseph S. Nye. 1989. *Power and Interdependence.* Glenview , IL: Foresman Scott.

Keohane, Robert O., and Jr., Joseph S. Nye. 1998. "Power and Interdependence in the Information Age." *Foreign Affairs* 77 (5): 81-94.

King, Gary, Robert O. Keohane, and Sidney Verba. 2012. *Designing Social Inquiry: Scientific Inference in Qualitative Research.* Princetone, NJ: Princeton University Press.

Kingdon, John W. 1984. *Agendas, Alternatives, and Public Policies.* Boston: Little, Brown.

Kolb, Felix. 2005. "Chapter 5: The Impact of Transnational Protest on Social Movement Organizatios, Mass Media and the Making of ATTAC Germany." In *Transnational Protest and Global Activism*. Lanham, MD: Roman & Littlefield.

Kolb, Felix. 2004. "The Impact of Transnational Protest on Social Movement Organizations: Mass Media and the Making of ATTAC Germany." In *Transnational Processes and Social Activism*, edited by Donatella dell Porta and Sidney Tarrow, 95-118. Lanham, MD: Rowman & Littlefield.

konkret. 2008. "Talar-Muffel von Hamburg, konkret 12/1967." *Go ̈tz Aly: Unser Kampf. 1968 – ein irritierter Blick zuru ̈ck.* Frankfurt: Fischer, December.

Krasner, Stephen D. 1982. "Structural causes and regime consequences: regimes as intervening variables." *International Organization* 36 (2): 185-205.

Krasner, Stephen. 1983. *International Regimes.* Ithaca, NY: Cornell University Press.

Krook, Mona Lena, and Jacqui True. 2010. "Rethinking the life cycles of international norms: The United Nations and the global promotion of gender equality." *European Journal of International Relations* 18 (1): 103-127.

Löblich, Maria, and Manuel Wendelin. 2011. "ICT Policy Activism on a National Level: Ideas, Resources, and Strategies of Germany Civil Society in Governance Processes." *New Media & Society* 14 (6): 899-915.

Lake, David A., and Robert Powell. 1999. *Strategic Choice and International Relations.* Princeton, NJ: Princeton University Press.

Lee, John. 2013. "Cyber Kleptomaniacs." *World Affairs* 73-79.

Legro, Jeffrey W. 1996. "Culture and Preferences in the International Cooperation Two-Step." *American Political Science Review* 90 (1): 118-137.

Lenard, Thomas M., and Paul H. Rubin. 2010. "In Defense of Data: Information and the Costs of Privacy." *Policy & Internet* 2 (1): 149-183.

Lenard, Thomas M., and Paul H. Rubin. 2010. "In Defense of Data: Information and the Costs of Privacy." *Policy & Internet* 2 (1): 149-183.

Lewis-Beck, Michael S., and Martin Paldam. 2000. "Economic Voting: An Introduction." *Electoral Studies* 19: 113-121.

Liberti, Fabio, and Camille Blain. 2011. *France's National Security Strategy, White Paper.* Madrid, SP: Real Instituto Elcano.

Liedtke, Werner. 1980. "Das Bunesdatenschutzgesetz: Eine Fallstudie zum Gesetzgebungsprozess." Dusseldorf: Mannhold.

1978. "Loi no. 78-17 du 6 janvier 1978 relative à la informatique, aux fichiers et aux libertés." Paris, FR: Journal Officiel de la Republique Francaise, January 6.

Longo, Matthew. 2018. *The Politics of Borders: Sovereignty, Security, and the Citizen after 9/11.* Cambridge: Cambridge University Press.

Ludlow, N. Piers. 2016. *Roy Jenkins and the European Commission Presidency, 1976-1980: At the Heart of Europe.* London, UK: Palgrave Macmillan.

Lynn III, William J. 2010. "Defending a New Domain: The Pentagon's Cyberstrategy." *Foreign Affairs* 89 (5): 97-108.

Lyon, David. 2014. "Surveillance, Snowden, and Big Data: Capacities, consequences, critique." *Big Data & Society* 1-13.

Lyon, David. 2014. "Surveillance, Snowden, and Big Data: Capacities, consequences, critique." *Big Data & Society* 1-13.

Madgwick, Donald, and Tony Smythe. 1974. *The Invasion of Privacy.* London: Pitman.

Magnussun, Lars. 2000. *An Economic History of Sweden.* London: Routledge.

Majone, Giandomenico. 1989. *Evidence, Argument, & Persuasion in the Policy Process.* New Haven, CT: Yale University Press.

Manners, Ian. 2002. "Normative Power Europe: A Contradiction in Terms?" *Journal of Common Market Studies* 235-258.

Mardellat, Patrick. 2011. "The Political (and also Economic) Consequences of the Euro: Lessons from the Crisis." Working Paper, Political Economy, Sciences Po, Lille, FR.

Margetts, Helen Z. 2009. "The Internet and Public Policy." *Policy & Internet* 1 (1): 1-21.

Margetts, Helen, Peter, John, Scott Hale, and Taha Yasseri. 2016. *Political Turbulence: How Social Media Shape Collective Action.* Princeton, NJ: Princeton University Press.

Mayer-Schönberger, Viktor. 2015. "Generational Development of Data Protection in Europe." In *Technology and Privac: The New Landscape*, edited by Philip E. Agre and Marc Rotenberg, 219-241. Cambridge, MA: MIT Press.

Mayer-Schönberger, Viktor, and Kenneth Cukier. 2013. *Big Data: A Revolution That Will Transform How We Live, Work, and Think.* London: John Murray.

Mayer-Schönberger, Viktor, and Thomas Ramge. 2018. *Reinventing Capitalism in the Age of Big Data.* London: John Murray.

Mazanec, Brian M. 2015. *The Evolution of Cyber War: International Norms for Emerging-Technology Weapons.* Washington , DC: Potomac Books/University of Nebraska Press.

McAdam, D., J.D. McCarthy, Zald, and M.N. 1996. *Comparative perspectives on social movements: Political opportunities, mobilizing structures, and cultural framings.* New York, NY: Cambridge University Press.

McIntyre, T.J. 2008. "Data retention in Ireland: Privacy, policy and proportionality." *Computer Law & Security Report* 326-334

McKinsey & Company. 2006. *Sweden's Economic Performance: Recent Development, Current Priorities (Executive Summary).* McKinsey Global Institute, New York, NY, USA: McKinsey & Company .

Mearsheimer, John. 2014. *Tragedy of Great Power Politics.* New York, NY: W. W. Norton & Company.

Meijers, Huub. 2014. "Does the internet generate economic growth, international trade, or both?" *International Economics & Economic Policy* 11: 137-163.

Meunier, Sophie, and Kalypso Nicolaidis. 1999. "Who Speaks for Europe? The Delegation of Trade Authority in the EU." *Journal of Common Market Studies* 37 (3): 477-501.

Meyer, John W., John Boli, George M. Thomas, and Francisco O. Ramirez. 1997. "World Society and the Nation-State." *American Journal of Sociology* 103 (1): 144-181.

Michalowitz, Irina. 2007. "What Determines Influence? Assessing Conditions for Decision-making Influence of Interest Groups in the EU." *Journal of European Public Policy* 14 (1): 132-151.

Migdal, Joel S. 1988. *Strong Societies and Weak States: State-Society Relations and State Capabilities in the Third World.* Princeton, NJ: Princeton University Press.

Milner, Helen. 1997. *Interests, Institutions, and Information.* Princeton, NJ: Princeton University Press.

Mitrany, David. 1948. *The Functional Approach to World Organizations.* Toronto: University of Toronto Press.

Moghadam, Assaf. 2012. "Failure and Disengagement in the Red Army Faction." *Studies in Conflict & Terrorism* 35: 156-181.

Moravcsik, Andrew. 2002. "In Defense of the 'Democratic Deficit': Reassessing Legitimacy in the European Union." *Journal of Common Market Studies* 40 (4): 603-624.

Moravcsik, Andrew. 1993. "Preferences and Power in the European Community: A Liberal Intergovernmentalist Approach." *Journal of Common Market Studies* 31 (4): 473-524.

Moravcsik, Andrew. 1997. "Taking Preferences Seriously: A Liberal Theory of International Politics." *International Organization* 51 (4): 513-553.

—. 1998. *The Choice for Europe: Social Purpose and State Power from Messina to Maastricht.* London: University College London Press.

Moravcsik, Andrew. 2000. "The Origins of Human Rights Regimes: Democratic Delegation in Postwar Europe." *International Organization* 54 (2): 217-252.

Morgan, Patrick M. 2010. "Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm." In *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, by National Research Council, 55-76. Washington, DC: National Academies Press.

Morgenthau, Hans. 1948. *Politics Among Nations: The Struggle for Power and Peace.* New York: Alfred A. Knopf Publishing.

Mueller, Milton L. 2010. *Networks and States: The Global Politics of Internet Governance.* Cambridge, MA: Massachusetts Institute of Technology Press.

Musolff, Andreas. 2011. "Hitler's Children Revisited: West German Terrorism and the Problem of Coming to Terms with the Nazi Past." *Terrorism and Political Violence* 23: 60-71.

National Research Council. 2010. *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy.* Policy and Global Affairs Division, Computer Science and Telecommunications Board, Washington, D.C., U.S.A: The National Academies.

National Research Council. 2010. *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy.* Workshop , Washington, DC, USA: National Research Council of the National Academies.

NBC News. 2017. *'Carlos the Jackal' Goes on Trial Over 1974 Paris Grenade Attack.* March 13. Accessed February 5, 2019. https://www.nbcnews.com/news/world/carlos-jackal-faces-paris-trial-over-1974-grenade-attack-n732591.

New Scientist. 1976. "Protection for Whose Data?" *New Scientist*, July.

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

Nocetti, Julian. 2015. "Contest and Conquest: Russia and Global Internet Governance." *International Affairs* 91 (1): 111-130.

Nordic Business Report. 1999. "Swedish Journalist Documenting Neo-Nazis Injured in Car Bomb." M2 Communications, July 5.

Norris, Pippa. 2001. *Digital Divide: Civic Engagement, Information Poverty, and the Internet Worldwide.* New York, NY: Cambridge University Press.

North, Douglass C. 1990. *Institutions, Institutional Change and Economic Performance.* Cambridge: Press Syndicate of the University of Cambridge.

Nugent, Neill, ed. 2002. *At the Heart of the Union: Studies of the European Commission.* Second. Basingstoke: MacMillan Press Ltd.

Nundy, Julian. 1994. *Jet hijackers die as 170 are freed.* December 27. Accessed February 5, 2019. https://www.independent.co.uk/news/uk/jet-hijackers-die-as-170-are-freed-1390663.html.

Nussbaum, Matthew. 2018. "Trump campaign sprints away from Cambridge Analytica." *Politico.eu.* March 20. Accessed March 29, 2018. https://www.politico.eu/article/cambridge-analytica-trump-campaign-tries-to-distance-itself-from-scandal-ridden/.

NY Times. 1986. *France Arrests 9 in Paris Bombings.* September 26. Accessed February 5, 2019. https://www.nytimes.com/1986/09/26/world/france-arrests-9-in-paris-bombings.html.

Nye, Joseph S. 2014. *The Regime Complex for Managing Cyber Activities.* Paper Series No. 1, Global Commission on Internet Governance, Waterloo, CA; London, UK: Centre for International Governance Innovation and the Royle Institute for International Affairs.

OECD. 2000. *A New Economy? The Changing Role of Innovation and Information Technology in Growth.* Information Society, Paris, FR: Organisation for Co-operation and Economic Development.

OECD. 1976. *Establishing Institutional Structures to Monitor and Enforce Data Protection.* Policy Issues in Data Protection and Privacy, OECD Informatics Studies, Paris: Organization for Economic Cooperation and Development, 83-94.

OECD. 2010. *Joint Roundtable of the Committee for Information, Computer and Communications Policy (ICCP) and its Working Party on Information Security and Privacy (WPISP).* Address by Hans Peter Gassman, Paris: Organisation for Economic Cooperation and Development.

OECD. 2009. *The Developmental Dimsion: Internet Access for Development.* Paris, FR: Organization for Economic Cooperation and Development.

Olson, Parmy. 2018. *EU Probes Facebook's Data Sharing With Cambridge Analytica, Raising Prospect Of Fines.* March 19. Accessed March 29, 2018. https://www.forbes.com/sites/parmyolson/2018/03/19/eu-probe-facebook-cambridge-analytica-fines/#6ebabb685fd6.

Organisation for Economic Cooperation and Development. 2003. *ICT and Economic Growth: Evidence from OECD Countries, Industries, and Firms.* Information and Communications Technologies, Paris: OECD.

Organisation for Economic Cooperation and Development. 2018. *ICT Total, % of value added, 2011 (indicator).* ICT Database, Paris: OECD.

—. 1985-2018. *OECD Digital Economy Papers.* Accessed April 5, 2019. https://www.oecd-ilibrary.org/science-and-technology/oecd-digital-economy-papers_20716826?page=16.

Organisation for Economic Cooperation and Development. 2013. *Privacy Framework.* Revised Report, Paris: OECD.

Organisation for Economic Cooperation and Development. 2001. *STI Working Papers 2001/7: ICT Investment and Economic Growth in the 1990s: Is the United States a Unique Case?* Paris: OECD.

Organisation for Economic Cooperation and Development. 2011. *Thirty Years after the OECD Privacy Guidelines.* Paris, FR: OECD.

Organisation for Economic Development and Cooperation. 2002. *Share of ICT value added in business sector value added, 2000.* Paris: OECD.

Organization for Economic Co-ooperation and Development. n.d. *Country Statistics.* Accessed December 2017. http://stats.oecd.org.

Organization for Economic Cooperation and Development. 2011. *TERMS OF REFERENCE FOR THE REVIEW OF THE OECD GUIDELINES GOVERNING THE PROTECTION*

OF PRIVACY AND TRANSBORDER DATA FLOWS OF PERSONAL DATA. DSTI/ICCP/REG(2011)4/FINAL, Paris: Working Party on Information Security and Privacy .

Orsini, Amandine, Jean-Frederic Morin, and Oran Young. 2013. "Regime Complexes: A Buzz, A Boom, or a Boost for Global Governance?" *Global Governance* 19: 27-39.

Osnos, Evan, David Remnick, and Joshua Yaffa. 2017. "Active Measures - What lay behind Russia's interference in the 2016 election - and what lies ahead?" *The New Yorker* 93 (3): 40-55.

Owens, William A., Kenneth W. Dam, and Herbert S. Lin. 2009. *Technology, Policy Law, and Ethics Regarding U.S. Acquisiting and Use of Cyberattack Capabilities.* Washington , DC: National Academic Press.

Oxford Dictionary of National Biography. n.d. *Sir Kenneth Gilmour Younger.* Biography, Oxford, UK: Faculty of History, University of Oxford.

Oyedemi, Toks. 2015. "Internet access as citizen's rights? Citizenship in the digital age." *Citizenship Studies* 19 (3/4): 450-464.

Palmer, John. 2007. *François-Xavier Ortoli: President of the European Commission and chariman of Total.* December 10. Accessed February 9, 2019. https://www.theguardian.com/news/2007/dec/10/guardianobituaries.eu.

Panizza, Roberta. 2018. *The Treaty of Lisbon, Fact Sheets on the European Union.* October. Accessed February 26, 2019. http://www.europarl.europa.eu/factsheets/en/sheet/5/the-treaty-of-lisbon.

Papacharissi, Zizi. 2010. "The Virtual Sphere 2.0: The Internet, the Public Sphere and beyond." In *Routledge Handbook of Internet Politics*, edited by Andrew Chadwick and Philip Howard. London: Routledge .

Parliament of the United Kingdom. 1984. HC Debs, London, UK, Col. 43.

Parliament of the United Kingdom. 1983. "HC Deb 11 April 1983." Vol. 40, London, UK, cc553-628.

Parliament of the United Kingdom. 1972. "HC Deb 21 April 1972." Vol 835, cc967-1012.

Parliament of the United Kingdom. 1973. "HL Deb 6 June 1973." Vol. 343, London, UK, cc104-78.

Parliament of the United Kingdom. 1961. "HL Debs." March, London, UK, 5s., col. 607.

Parliament of the United Kingdom. 1972. "Order for Second Reading, C Deb." Vol. 835, London, UK, cc967-1102.

—. 2014. "The Criminal Justice and Data Protection (Protocol No. 36) Regulations 2014." *Draft Regulations laid before Parliament under section 2 (2) of, and paragraph 2 (2) of Schedule 2, to, the European Communities Act 1972, for approval by resolution of each House of Parliament.* London: www.parliament.uk, November 10.

Pérez, Efrén. 2015. "Ricochet: How Elite Discourse Politicizes Racial and Ethnic Identities." *Political Behavior* 37: 155-180.

Peters, B. Guy. 1994. "Agenda-setting in the European Community." *Journal of European Public Policy* 1 (1): 9-26.

Pew Research Center. 2016. "Internet access growing worldwide but remains higher in advanced economies." *Global Attitudes and Trends.* February 2016. Accessed December 1, 2017. http://www.pewglobal.org/2016/02/22/internet-access-growing-worldwide-but-remains-higher-in-advanced-economies/.

Pollack, Mark A. 2010. In *Policy-Making in the European Union*, by Mark A. Pollack, and Alasdair R. Young edited by Helen Wallace, 15-44. Oxford: Oxford University Press.

Pollack, Mark A. Winter 1997. "Delegration, Agency, and Agenda Setting in the European Community." *International Organization* 51 (1): 99-134.

Pollack, Mark A. 2015. "Theorizing EU Policy-Making." In *Policy-Making in the European Union*, by Helen Wallace, Mark A. Pollack and Alasdair Young, 12-45. Oxford: Oxford University Press.

Post, Jerrold M., and Alexander L. George. 2004. *Leaders and Their Follower in a Dangerous World: The Psychology of Political Behavior.* Ithaca, NY: Cornell Univeristy Press.

Poullet, Yves, and Serge Gutwirth. 2008. *The contribution of the Article 29 Working Party to the construction of a harmonised European Data protection system: an illustration of 'reflexive governance'?* Vols. p. 570-610, in *Défis du droit à la protection de la vie privée : perspectives du droit européen et nord-américain (Challenges of privacy and data proteciton law)*, by Veronia Perez Asinari and Pablo Palazzi. Bruxelles: Bruylant.

Powers, Shawn M. 2015. *The Real Cyber War: The Political Economy of Internet Freedom.* Urbana, IL: University of Illinois Press.

Preece, Julian. 2010. "The lives of the RAF revisited: The biographical turn." *Memory Studies* 3 (2): 151-163.

Price, David. 1984. "The Emergence of a UK Data Protection Law." *Yearbook of Law Computers and Technology* 1: 131-135.

Putnam, Robert D. 1988. "Diplomacy and domestic politics: the logic of two-level games." *International Organization* 42 (3): 427-460.

—. 1993. *Making Democracy Work: Civic Traditions in Modern Italy.* Princeton, NJ: Princeton University Press.

Röller, Lars-Hendrik, and Leonard Waverman. 1996. "Working Paper Telecommunications infrastructure and economic development: a simultaneous approach." WZB Discussion Paper, No. FS IV 96-16, WZB Berlin Social Science Center, Berlin.

Rawlinson, Kevin, Angelique Chrisafis, and Vikaram Dodd. 2016. *From Charlie Hebdo to Bastille Day: France reels after new deadly attack.* July 14. Accessed February 5, 2019. https://www.theguardian.com/world/2016/jul/15/charlie-hebdo-bastille-day-france-reels-after-deadly-nice-attack.

Reimann, Kim D. 2006. "A View from the Top: International Politics Norms and the Worldwide Growth of NGOs." *International Studies Assocation* 50: 45-67.

1972. *Report of the Committee on Privacy.* Cmnd. 5012, Younger Committee.

Republic of Germany Ministry of Justice. n.d. *Ministry of Justice, Laws on the Internet (Bundesministerium der Justiz und für Verbraucherschutz).* Accessed 2018-2019. https://www.gesetze-im-internet.de/index.html.

République Française. 2017. "Defence and National Security Strategic Review 2017." Paris, FR.

République Française. 2013. "French White Paper: Defence and National Security 2013." Paris, FR.

Riccardi, J. Lee. 1983. "The German Federal Data Protection Act of 1977: Protecting the Right to Privacy?" *Boston College International and Comparative Law Review* 6 (1): 243-271.

Righettini, Maria Stella. 2011. "Institutionalization, Leadership, and Regulative Policy Style: A France/Italy Comparison of Data Protection Authorities." *Journal of Comparative Policy Analysis* 143-164.

Riker, William H. 1996. *Agenda Formation.* Ann Arbor, MI: University of Michigan Press.

Riker, William H. 1982. "The Two-Party System and Duverger's Law: An Essay on the History of Political Science." *The American Political Science Review* 76 (4): 753-766.

Risse, Thomas, and Tanja A. Börzel. 2004. *One Size Fits All! EU Policies for the Promotion of Human Rights, Democracy and the Rule of Law.* Working Paper, Center for Development, Democracy, and the Rule of Law, Workshop on Democracy Promotion, Stanford University, Research Gate.

Risse, Thomas, Stephen C. Ropp, and Kathryn Sikkink, . 2013. *The Persisten Power of Human Rights: From Compliance to Commitment.* Cambridge: Cambridge Universit Press.

Risse-Kappen, Thomas, ed. 1995. *Bringing transnational relations back in: Non-state actors, domestic structures and international institutions.* Cambridge: Cambridge University Press.

Risse-Kappen, Thomas, Steve C. Ropp, and Kathryn Sikkink. 1999. *The power of human rights : international norms and domestic change.* New York, NY: Cambridge University Press.

Ron, James, Howard Ramos, and Kathleen Rodgers. 2005. "Transnational Information Politics: NGO Human Rights Reporting, 1986-2000." *International Studies Quarterly* 49: 557-587.

Rosecrance, Richard. 1996. "The Rise of the Virtual State." *Foreign Affairs* 75 (4): 45-61.

Rubin, Herbert J., and Irene S. Rubin. 2005. "Chapter 10: The First Phase of Analysis - Preparing Transcripts and Coding Data." In *Qualitative Interviewing: The Art of Hearing Data*, by Herbert J. Rubin and Irene S. Rubin, 201-223. Thousand Oaks, CA: SAGE Publications Limited.

Ruggie, John Gerard. 1982. "International Regimes, Transactions, and Change: Embedded Liberalism in the Postwar Economic Order." *International Organization* 379-415.

Ruggie, John Gerard. 1998. "What Makes the World Hang Together." *International Organization* 52 (4): 855-885.

Sakwa, Richard. 2015. *Frontline Ukraine: Crisis in the Borderlands.* London: I.B. Tauris.

Salamon, Lester M., and John J. Siegfried. 1977. "Economic Power and Political Influence: The Impact of Industry Structure on Public Policy." *The American Political Science Review* 1026-1043.

Santaniello, Mauro, and Francesco Amoretti. 2013. "Electronic Regimes: Democracy and Geopolitical Strategies in Digital Networks." *Policy & Internet* 5 (4): 370-386.

Schattschneider, Elmer E. 2013. *The Semisovereign People: A Realist's View of Democracy in America.* Boston, MA: Wadsworth.

Schmidt, Vivien A. 2006. *Democracy in Europe: The EU and National Polities.* Oxford: Oxford University Press.

Schmidt, Vivien A. 2004. "The European Union: Democratic Legitimacy in a Regional State?" *Journal of Common Market Studies* 42 (5): 975-997.

Schneider, Volker. 2001. "Institutional reform in telecommunications: the European Union in transnational policy diffusion." In *Transforming Europe*, edited by Maria Green Cowles, James A. Caporaso and Thomas Risse-Kappen, 22-35. Ithaca, NY: Cornell University Press.

Schneier, Bruce. 2015. *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World.* New York, NY: W. W. Norton & Company Publishers.

Schreyer, Paul. 2000. *The Contribution of Information and Communication Technology to Output Growth: A Study of G7 Countries.* Science, Technology and Industry Working Papers, Paris: OECD.

Segell, Glen M. 2000. "French Cryptography Policy: The Turnabout of 1999." *International Journal of Intelligence and Counterintelligence* 13: 345-358.

Shamsi, Hina, and Alex Abdo. n.d. *Privacy and Surveillance Post-9/11, Vol. 38, No. 1.* Accessed August 6, 2018. https://www.americanbar.org/publications/human_rights_magazine_home/human_rights_vol38_2011/human_rights_winter2011/privacy_and_surveillance_post_9-11.html.

Siebert, Horst. 2005. *The Germany Economy: Beyond the Social Market.* Princeton, NJ: Princeton University Press.

Sikkink, Kathryn. 1993. "Human Rights, Principled Issue-Networks, and Sovereignty in Latin America." *International Organization* 47 (3): 411-441.

Sikkink, Kathryn. 2005. "Patterns of Dynamic Multilevel Governance and the Insider-Outsider Coalition." In *Transnational Protest and Global Activism*, edited by Sidney G. Tarrow and Donatella Della Porta, 151-173. Rowman & Littlefield Publishing.

Simitis, Spiros. 1971. "Chancen und Gefahren der elektronischen Datenverarbeitung." *Neue Juristische Wochenschrift.*

Simitis, Spiros. 1978. "Datenschutz – Notwendigheit und Voraussetzungen einer gesetzlichen Regelung." In *Informatik - Fachberichte: Herausgegeben von W. Brauer im Auftrag Der Gesellschaft für Informatik (GI)*, by Wilhelm Steinmüller, Leonhard Ermer and Wolfgang Schimmel. Berlin: Springer-Verlag.

Simitis, Spiros. 1976. *Establishing Institutional Structures to Monitor and Enforce Data Protection.* Policy Issues in Data Protection and Privacy, Paris, FR: Organization for Economic Cooperation and Development.

Singer, P.W., and Allan Friedman. 2014. *Cybersecurity and Cyberwar: What Everyone Needs to Know.* New York, NY: Oxford University Press.

Skinner, Christina Parajon. 2014. "An International Law Response to Economic Cyber Espionage." *Connecticut Law Review* 46 (4): 1165- 1207.

Skocpol, Theda. 1994. *States and Social Revolutions in the Modern World.* London: Cambridge University Press.

Skocpol, Theda, and John Coggin. 2011. "The Tea Party and the Remaking of Republican Conservatism." *Perspectives in Politics* 9 (1): 25-43.

Stone, Deborah A. 2012. *Policy Paradox: The Art of Political Decision Making.* New York, NY: W.W. Norton & Company.

Stroup, Sarah S., and Amanda Murdie. 2012. "There's no place like home: Explaining international NGO advocacy." *The Review of International Organizations* 7 (4): 425-448.

Sweden, Government of. 1972. *Computers and Privacy.* Royal Commission, Stockholm: Commission on Publicity and Secrecy of Official Documents.

Swedish Ministry of Justice. 1996. *Swedish position concerning openness in the European institutions.* Stockholm: Government of Sweden.

Tanner, Henry. 1977. *German Troops Free Hostages on Hijacked Plane in Somalia; Four Terrorists Killed In Raid.* October 18. Accessed December 19, 2018.

https://www.nytimes.com/1977/10/18/archives/german-troops-free-hostages-on-hijacked-plane-in-somalia-four.html.

Tarrow, Sidney. 1994. *Power in Movement: Social Movements and Contentious Politics.* Cambridge: Cambridge University Press.

Taylor, Mark Zachary. 2016. *The Politics of Innovation: Why Some Countries are Better than Others at Science & Technology.* New York, NY: Oxford University Press.

2014. *The Cambridge Economic History of Modern Britain, Volume 2.* Cambridge: Cambridge University Press.

The Guardian News. 2011. *Activate 2011: Robert Kirkpatrick, director, UN Global Pulse.* April 26. Accessed March 10, 2019. https://www.theguardian.com/activate/video/activate-robert-kirkpatrick.

The Herald. 1997. *Lord Ross warns that judges should stay out of politics; unease over crime speech.* February 12. Accessed October 2018, 3 . https://www.heraldscotland.com/news/12077997.Lord_Ross_warns_that_judges__should_stay_out_of_politics_Unease_over_crime_speech/ .

The Privacy Rights Clearinghouse. 2018. *Data Breaches.* March. Accessed March 27, 2018. https://www.privacyrights.org/data-breaches.

The World Bank. 2006. *2006: Information and Communications for Development: Global Trends and Policies.* Washington, DC: The World Bank.

Thorn, Gaston. 1981 (12 January). "Address by Mr. Gaston Thorn, President of the Commission of the European Communities, to the European Parliament." Strasbourg: European Union.

—. 1984 (15 February). "Address by Mr. Gaston Thorn, President of the Commission of the European Communities, to the European Parliament." Strasbourg: European Union.

Tilly, Charles, and Sidney Tarrow. 2005. "How Political Identities Work." *Prepared for publication in Hellenic Political Science Review, sometime in 2006.* Columbia University, Cornell University, December 14.

Tolbert, Caroline J., and Ramona S. McNeal. 2003. "Unraveling the Effects of the Internet on Political Participation." *Political Research Quarterly* 56 (2): 175-185.

Treacy, Bridget. 2013. "How Safe is the U.S-EU Safe Harbour?" Thomas Reuters, September 9.

Treib, Oliver. 2006. "Implementing and Complying with EU Governance Outputs." *Living Reviews In European Governance.*

Tsebelis, George. 1990. *Nested Games: Rational Choice in Comparative Politics.* Berkeley, CA: University of California Press.

Tsutsui, Kiyoteru, and Chirstine Min Wotipka. 2004. "Global Civil Society and the International Human Rights Movement: Citizen Participation in Human Rights International Nongovernmental Organizations." *Social Forces* 83 (2): 587-620.

Tzanou, Maria. 2013. "Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right." *International Data Privacy Law* 3 (2): 88-99.

UK Parliament. n.d. *The work of the Information Commissioner: appointment of a new Commissioner - Justice Committee.* https://publications.parliament.uk/pa/cm200809/cmselect/cmjust/146/14604.htm.

United Nations. 2019. *About Global Pulse.* Accessed March 10, 2019. https://www.unglobalpulse.org/about-new.

United Nations. 2013. *Resolution adopted by the General Assembly on 18 December 2013.* Third Committee, New York, USA: General Assembly of the United Nations.

Utterback, James M, Marc Meyer, Edward Roberts, and Loren Reitberger. 1988. "Technology and industrial innovation in Sweden: A Study of tech firms formed between 1965 and 1980." *Research Policy* 17: 15-26.

van Ark, Bart, Johanna Melka, Nanno Mulder, Marcel TImmer, and Gerard Ypma. September 2002. *ICT Investment and Growth Accounts for the European Union, 1980-2000.* Final Report on ICT and Growth Accounting, for the DG Economics and Finance of the European Commission, University of Groningen & the Conference Board, Brussels; Centre d'études prospectives et d'informations internationales (CEPII), Paris, Brussels: EU Commission.

Voss, W. Gregory. 2016. "The Future of Transatlantic Data Flows: Privacy Shield or Bust?" *Journal of Internet Law* 19 (11): 8-19.

Wallace, Helen, Mark A. Pollack, and Alasdair R. Young. 2015. *Policy-Making in the European Union.* Oxford: Oxford University Press.

Warren, Adam, and James Dearnley. 2005. "Data Protection Legislation in the United Kingdom." *Information, Communication & Society* 8 (2): 238-263.

Weiss, Thomas G. 2013. *Global Governance - Why? What? Whither?* Cambridge: Polity Press.

Wendt, Alexander. 1992. "Anarchy is What States Make of It: The Social Construction of Power Politics." *International Organization* 46 (2): 391-425.

Wicker, Stephen B., and Stephanie M. Santosa. 2013. "Access to the Internet is a Human Right." *Communications of the ACM* 56 (6): 43-46.

Wicklein, John. 1982. *Electronic nightmare : the home communications set and your freedom.* Boston, MA: Beacon Press.

Wolfsfeld, Gadi, Elad Segev, and Tamir Sheafer. 2013. "Social Media and the Arab Spring: Politics Comes First." *International Journal of Press/Politics* 18 (2): 115-137.

Wood, Elisabeth Jean. 2007. *Forging Democracy from Below: Insurgent Transitions in South Africa and El Salvador.* Cambridge, NJ: Cambridge University Press.

Yoedemi, Toks. 2015. "Internet Access as Citizen's Right? Citizenship in the Digital Age." *Citizenship Studies* 19 (3-4): 450-464.

Young, Lori, and Stuart Soroka. 2012. "Affective News: The Automatic Coding of Sentiment in Political Texts." *Political Communication* 29: 205-231.

Younge, Gary. 1999. "Car bombs Explode Sweden's Self-image." *Guardian Weekly.*

Zaller, John. 1992. *The nature and origins of mass opinion.* Cambridge : Cambridge University Press.

Zuboff, Shoshana. 2015. "Big other: surveillance capitalism and the prospects of an information civilization." *Journal of Information Technology* 30: 75-89.

Zwingel, Susanne. 2012. "How Do Norms Travel? Theorizing International Women's Rights in Transnational Perspective." *International Studies Quarterly* 56: 115-129.