

Explaining Policy Change in Governing Digital Technology Risks

*Longitudinal Analysis of US and EU Cybersecurity and Privacy Policy
Regimes*

Thesis for the degree of “Doctor of Philosophy”
By Ido Sivan-Sevilla

Re-submitted to the Senate of the Hebrew University of Jerusalem
October 2019

Explaining Policy Change in Governing Digital Technology Risks

*Longitudinal Analysis of US and EU Cybersecurity and Privacy Policy
Regimes*

Thesis for the degree of “Doctor of Philosophy”
By Ido Sivan-Sevilla

Re-submitted to the Senate of the Hebrew University of Jerusalem
October 2019

This work was carried out under the supervision of
Prof. David Levi-Faur

ACKNOWLEDGEMENTS

The completion of this dissertation was made possible due to the help, guidance and support of numerous mentors, colleagues, friends and family members. First of all, I would like to thank my advisor, Professor David Levi-Faur, for being an incredible source of inspiration, support and intellectual curiosity. For four and a half years, David has dispensed excellent advice, and supported me wholeheartedly without holding back neither praise nor criticism, all while letting me walk my own scholarly paths, forming my own intellectual style, and learn from my mistakes. His professionalism and work ethics pushed me to consistently demand more from myself, and always strive to be better and influential in my academic community. Words cannot express how much I learnt from him throughout this significant period. His supervision had a substantial impact on my life and enabled me to develop as an academic, an intellectual, and a person, stimulating my passion to create a better world.

I wish to thank Professor Martin Lodge, Professor Charles Raab, and Professor Alon Peled, who served as my committee members. I am grateful for their time, attention, and valuable insights throughout the process. I am particularly thankful to Prof. Charles Raab for his personal guidance and feedback which have been extremely valuable for the accomplishment of my first article.

I am grateful for the mentorship, help, and support of Prof. Sharon Gilad, Dr. Tehilla Shwartz-Altshuler, Dr. Elyakim Kislev, Dr. Limor Samimian-Darash, and Dr. Dmitry Epstein from the Federmann School of Public Policy and Government. They all greatly contributed to my research as well as to my professional and intellectual development. I am especially thankful to Prof. Gilad for her time and advice. As her teaching assistant for one year, I was amazed and motivated not only by her passion for producing high quality research, but also from her perception of her social role as a social scientist in Israel.

I am also grateful for numerous scholars and colleagues outside the Federmann School who viewed early versions of the research design, results, and papers, and gave significant remarks: Prof. Avishai Benish, Prof. Michael Birnhack, Dr. Caelesta Braun, Prof. Ben Cashore, Dr. Hartmut Eden, Prof. Jacint Jordana, Dr. David Kamerer, Prof. Bing-Yan Lu, Dr. Hamish van der Van, and Dr. Kai Wegrich.

I wish to also thank several faculty members at the Hebrew University of Jerusalem for serving as intellectual mentors from which I learned the art of becoming a researcher: Prof. Roi Baer, Prof. Pazit Ben-Nun Bloom, Dr. Yotam Benziman, Prof. Gili Drori, Prof. Avraham Kluger, Dr. Tammy Oren, and Prof. Amalya Oliver.

I would also like to thank to the three anonymous reviewers of the first paper for their extremely valuable suggestions and comments, which helped me not only to improve this paper, but also to further expand my theoretical perspective and thinking with regard to the relevance of the entire project.

A special thank you to Mirit Kisner, for her patience, guidance, and unbelievable support in proof-reading my second and third papers. I would also like to thank Michelle Spektor for her great editing assistance in the first paper.

I am thankful to the Federmann School's administrative staff – Ofra Toren Commere, Meital Shtain, Oudelia Iluz-Levy, and Roni Sdikler-Cohen – for their support throughout the PhD program with everything I had ever asked for. A special thank you goes to all the MA

students I taught throughout the years. They challenged me intellectually and were able to diffuse their passion to public service across the School's halls.

A great sense of appreciation goes to my mentors and colleagues from the Institute for National Security Studies (INSS) at the Tel Aviv University. I want to thank Gabi Siboni for his mentorship, support, and advice throughout my PhD program, Meir Elran for his continuous support, and Amos Yadlin who devoted time for opening new opportunities for personal development. I want to thank my colleagues at INSS who constantly encouraged me during the research process – Hadas Klein, Gal Perl-Finkel, Liran Antebi, Mor Ben-Kalifa, Doron Ella, Michal Hatuel-Radoshitzky, Adi Kantor, Aviad Mandelboim, Vera Michlin-Shapir, Carmit Padan, Khader Sawaed, Pnina Shuker, David Siman-Tov, and Carmit Valensi.

I am extremely thankful to my MA program mentor at the University of Minnesota – Prof. Morris Kleiner – and his beloved family. Morris taught me the basics of becoming an academic and I will always cherish how his family made me feel at home, ten time zones away, at the beginning of my academic journey.

A warm thank you goes to my colleagues at the Regulation & Governance IL group: Inbar Mizrahi, Nir Kosti, Guy Mor, Rotem Medzini, Ayelet Metzger, Yair Ashuruv, Yael Kariv, Libby Maman, Keren Bornstein, Hanan Haber, Yair Hakak, Debby Sadeh, Daniel Hirsch, and Eilat Navon who helped me with the development of my theoretical arguments, empirical designs and analyses, as well as with their emotional support and friendship.

This project would not have been completed without the financial support I have received from the Azrieli Foundation and the Harry and Sylvia Hoffman Leadership and Responsibility Program. These programs were supportive above and beyond my expectations, allowing me to focus on my research while thinking and shaping my social role as a social scientist in Israel.

I also want to thank the Wizo Jerusalem community, with whom I have been doing voluntary work throughout the period of my research, for their flexibility with my schedule and their supportive environment. I am also grateful to Rashut Harabim, a Jewish pluralist non-profit, from which I was renting an office space in the past two years. They had provided a wonderful facility and company for writing my dissertation.

Lastly, throughout the entire way I have been supported by my family, who has been patient and encouraging, for which I am extremely grateful. I would like to thank my beloved partner, Anat, whose love and caring were an endless source of strength and motivation for me. To my parents, Hagit and Jacob, who have raised me with the thirst for knowledge, the aspiration for excellence, and the deep belief that I can accomplish whatever goal I set my mind to. To my parents-in-law, Rivka and Gabriel, thank you for your unconditional support, encouragement, and for providing such a warm and welcoming atmosphere to my PhD aspirations. To my two children, Tomer and Gili, who were born and grew up during my graduate studies – thank you for being such an inspiration and for bringing me so much joy. I am so lucky to be your parent.

ABSTRACT

It is hard to overstate the social, economic, and national importance of governing risks that arise from digital technologies. The use of digital devices encompasses half of the world's population, and digital practices are deployed across all industrial sectors, in every dimension of the production process. On the one hand, digital technologies enable unprecedented computation powers, global information flows, essential services, and growth of innovations. On the other hand, the emergence of risks and vulnerabilities that threaten the integrity, confidentiality, and availability of digital systems is incident to reliance on digital technologies.

Regardless of policymakers' attempts to mitigate cyber risks, the number of cybersecurity incidents is on the rise. Criminals exploit cyberspace for profit, intellectual property is regularly stolen, and national infrastructures are targeted. In addition, the proliferation of digital technologies jeopardizes privacy. The massive flows of information ease the unauthorized collection, processing, and usage of personal information by commercial and state actors. Since privacy is an enabler of other rights, such threats gnaw at other fundamental values such as anonymity, liberty, and freedom of speech.

Public policy research has barely addressed these policy problems. Empirical understanding of how these policies are organized and change over time is wanting; we do not know who the influential actors in those policy processes are, and what drives policy changes. Scholars who do study these problems only address specific policies in certain time frames, and do not employ a policy regime perspective to consider how the interplay of ideas, interests, and institutional arrangements shape cybersecurity and privacy governance. The regime lens is especially appealing for these problems because policymaking in that terrain is often fragmented and disjointed, taking place in multiple levels of governance.

This dissertation aims to bridge this gap by asking *how and why the governance of cybersecurity and privacy develops over time and across sectors in the US and EU?* The goals of this research are *first*, to handle difficult-to-capture dependent variables on the development of policy regimes for cybersecurity and privacy in two central political systems. *Second*, to identify the micro-mechanisms that lead to certain policy outcomes across political systems. *Third*, to generate new research questions based on the captured variables to explain contemporary governance arrangements in the age of continuous technological progress. The three papers study how these policy regimes were constructed, examine the actors, measures, and developments in time, and investigate what leads to policy change across contexts.

The first paper, entitled *complementaries and contradictions: national security and privacy risks in U.S. federal policy [1968-2018]* (Sivan-Sevilla, *Policy & Internet*, 2018) explores how the U.S. balances between national security and privacy in light of advancements in digital technologies in the past five decades. The paper analyzes (N=63) federal policies across three policy arenas based on a novel analytical framework, to determine how and why policy processes harm, compromise, or complement privacy and national security. The results of this study demonstrate how privacy has been eroded for the sake of national security, stressing the importance of different policy arenas, the characteristics of the policy process, and the variety of actors involved to the construction of national security and privacy dynamics.

The second paper, entitled *Framing and Governing Cyber Risks: Comparative Analysis of U.S. Federal Policies [1996-2018]* (approved for publication at *The Journal of Risk Research*), analyzes how U.S. federal cybersecurity policies frame cyber risks and consequently construct risk governance frameworks. Based on a systematic text analysis and a novel typology, this paper scrutinizes thirty federal policies from the past two decades from which (N=463) key sentences were coded. The paper finds that cyber risk governance frameworks vary across sectors and over time. It also reveals how policy outputs are loosely connected to policymakers' alarming framing of the problem, and are based on decision-making structures that were institutionalized early on.

The third paper, entitled *EU publicization of private certifiers for cybersecurity: explaining public-private interactions through the context of institutional change* (under review at the *Journal of Public Policy*), studies a rather unexplored interaction between public and private authorities in EU's cybersecurity governance arrangements. The study features a comparative analysis of the institutional frameworks for cybersecurity certification in the past two decades based on policy documents (N=40) and interviews (N=18), to reveal how and why private certification bodies were elevated and controlled by public authorities. The results of this study reveal political conflicts between EU and Member States in this arena and question the dichotomous portrayal of the shift from government to governance.

Altogether, the three papers illuminate the patchy nature and the political context of the development of policy regimes for cybersecurity and privacy. The papers demonstrate alarming contextual patterns of privacy erosion in favor of national security, stagnation of policy development despite the dynamic landscape of cyber threats, and the significance of old institutional patterns when it comes to the implementation of new policy solutions. This creates an important connection between public policy research and technological progress.



האוניברסיטה העברית בירושלים
THE HEBREW UNIVERSITY OF JERUSALEM

Ido Sivan-Sevilla, PhD candidate
The Federmann School of Public Policy and Government
The Hebrew University of Jerusalem
Mt. Scopus, Jerusalem 91905, Israel
ido.sivan@mail.huji.ac.il

October 13th, 2019

A statement on authorship and dissertation components

Dear committee members,

I hereby declare that my doctoral dissertation entitled “Explaining Policy Change in Governing Digital Technology Risks: Longitudinal Analysis of US and EU Cybersecurity and Privacy Policy Regimes,” is written in the form of compilation of articles (ASSUFA).

All three articles of the dissertation were written without any co-authors. The first article, entitled “Complementaries and Contradictions: National Security and Privacy Risks in U.S. Federal Policy, 1968-2018,” was published in the peer-review journal *Policy & Internet*. The second article, entitled “Framing and Governing Cyber Risks Comparative Analysis of U.S. Federal Policies [1996-2018],” was accepted for publication to the peer-review *Journal of Risk Research*. The third article, entitled “Publicization of Private Certifiers for Cybersecurity: Explaining Public-Private Interactions Through the Context of Institutional Change,” is currently under review in the peer-reviewed *Journal of Public Policy*. In all papers, I developed the theoretical models and the research design, managed the collection of data, conducted the empirical analyses and wrote the manuscripts. Prof. Levi-Faur has assisted throughout all these stages by providing me with critical comments.

The three articles are accompanied by an introductory chapter in which I lay down the motivation and aims of the dissertation, explain the relationship between the abovementioned three chapters, position them in the broader context of the public policy literature, and discuss their methodological approach. The dissertation also includes a concluding chapter in which I summarize the main findings and contributions of the dissertation.

Sincerely,

Ido Sivan-Sevilla

TABLE OF CONTENTS

Introduction	1
A Policy Regime Perspective to Study Policy Problems	5
The Empirical Approach for Studying Variance in Policy Regimes	9
Chapters' Summary	16
Bibliography	23
1. Complementaries and Contradictions: National Security and Privacy Risks in US Federal Policy, 1968-2018.....	25
Introduction	27
Literature Review.....	29
Conceptual Clarifications: National Security and Privacy.....	30
Analytical Framework and Methodology.....	31
Analysis over Time.....	34
Analysis across Policy Arenas	45
Discussion and Conclusion	53
References	59
Appendix: Methodological Annex.....	62
2. Framing and Governing Cyber Risks: Comparative Analysis of US Federal Policies [1996-2018].....	69
Introduction.....	71
Literature Review: The Role of Risk Frames in Risk Governance Across Sectors.....	73
Analytical Framework & Methodology.....	79
US Federal Policy Frameworks for Cyber Risk Governance.....	82
Comparative Analysis	98
Discussion and Conclusion.....	101
References	105
Supplementary appendix	108
Tables & Figures	110
3. EU Publicization of Private Certifiers for Cybersecurity: Explaining Public-Private Interactions through the Context of Institutional Change	117
Introduction.....	119
Literature Review.....	121
Research Hypotheses	123
Methodology	127
Current and Proposed Regimes for EU Cybersecurity Certification	128
Hypotheses Testing	136
Discussion & Conclusion.....	142
References	146
Tables and Figures.....	148
Supplementary appendix	151

Conclusion	155
Summary of the Research Project and Work Process.....	155
Going Back to the Dissertation Objectives.....	159
The Contribution of the Dissertation to Existing Public Policy Research.....	160
The Implications of the Dissertation for Other Audiences.....	162
Proposed Directions for Future Research.....	163
Bibliography.....	165

INTRODUCTION

Our world has been reorganized by the information revolution. Microscopic semiconductors have given billions of people information processing power that was literally unimaginable a century earlier, and networked connections have linked those billions to one another via nearly instant and global communications. This made digital technologies central to daily life, economic vitality, personal welfare, and national security, as nearly half of the world's population is already connected (Nye, 2017). But while the pervasiveness of cyberspace is consistently rising (Choucri, 2012), the spread of digital technologies has been accompanied by expansions of risks, vulnerabilities and uncertainties that threaten the security of cyber-based systems and the privacy of connected individuals (Warner, 2012; OECD, 2015).

Despite efforts and investments by policymakers in an attempt to mitigate these risks, cyber incidents are on the rise. Criminals efficiently exploit cyberspace for profit, intellectual property is regularly stolen, and national infrastructures are targeted. Since 2005, we have been witnessing a rise in the quantity and quality of data breaches. More than 4,500 breaches have been made public and more than 816 million individual records were stolen (De Groot, 2019). In addition, there is a constant increase in the number of incidents reported by US federal agencies - from a few thousands in 2006 to almost eighty thousand in 2015 (GAO, 2017). Some of the major breaches and incidents include the 2013 Target breach with data of more than 110 million data records stolen (Myers, 2018), the 2015 hack to a Ukrainian power station that left nearly a quarter of a million residents in the dark (Zetter, 2016), the 2017 cyber-attacks that struck more than 40 British hospitals (Woollaston, 2017), the 2017 data breach in Equifax that resulted in data loss of more than 143 million Americans (FTC, 2017), and the 2018 hack to Marriot International with 500 million customers losing their data (O'Flaherty, 2019).

In addition to risks from malicious actors, the proliferation of digital technologies led to threats on individuals' privacy from state and commercial entities. Individuals lost their ability to control how their personal information is collected, accessed, and used, often without their knowledge. The progress in computer processing, networking, and storage capacities removed most technical barriers to information collection. Instead of hand-picking their surveillance targets, governments can easily spy on large portions of the population on a regular basis, and commercial actors can tailor their campaigns based on accurate profiling techniques. By integrating distinct pieces of information, capable actors can reveal one's intimate habits,

interests, concerns, and passions (Granick, 2017; Solove, 2011). This intensive information collection creates forms of social control and disempowers individuals. Moreover, such privacy losses lead to an erosion of other values like anonymity, liberty, and freedom of speech and association (Raab, 2014; Solove, 2011; Waldron, 2003).

Thus, the promise of digital technologies comes with risks to the availability and integrity of essential economic and national infrastructures and to fundamental social values. These risks have increasingly occupied policymakers across nations (OECD, 2012), but surprisingly, policy scholars have devoted only little attention to study these policy problems. We lack an empirical understanding of how these policies are organized and alter over time, who are the influential actors in those policy processes, what are the drivers for policy changes in these policy spaces, and what can be learned about public policy from studying these policy problems. Scholars who do study these problems only address specific policies during certain time frames, without employing a policy regime perspective to consider how the interplay of ideas, interests, and institutional arrangements shape cybersecurity and privacy governance.

Moreover, the cybersecurity and privacy policy spaces, that were selected for analysis in this dissertation, are interesting policy areas not only due to the scarcity of works on these issues in the public policy literature, but also because of the characteristics of these policy spaces, that allows to generalize the findings to other policy domains. Specifically, findings are likely to ‘travel’ to other policy spaces that are fragmented, patchy, and operate in a multi-level nature with a variety of government agencies and institutional structures involved over time. Also, findings can be generalizable to policy spaces that are close to state’s power and sovereignty (Genschel and Jachtenfuchs, 2013), or experience a continuous technological change as a significant policy context over time.

Prior to in-depth analysis of how public policies address privacy, cybersecurity, and national security implications of digital technologies, it is important to provide conceptual clarifications for each of these terms: *Privacy* risks refer to risks to the control and knowledge that individuals have over collection, processing, and other uses of their personal information (Fried, 1968; Laudon, 1996; Lesig, 1999; Rachels, 1975; Westin, 1967). Such risks undermine the levels of autonomy, dignity, and self-determination that individuals can enjoy (Benn, 1971; Fried, 1968, Gavison, 1980; Rachels, 1975). *Cybersecurity* risks address the confidentiality, integrity, and availability of digital infrastructures and their associated information (Dunn Cavelty, 2010). These risks directly address vulnerabilities in digital infrastructures and their

implications. *National Security* risks are defined as risks to the nation which originate in foreign states or within the nation's border (Diffie & Landau, 2007). It is perceived in the dissertation as a form of collective security (Waldron, 2006) and can relate to almost any security issue, including cyber-related issues, that is understood as a form of severe crime that threatens the whole nation (Solove, 2011).

This dissertation aims to fulfill gaps in the public policy literature on cybersecurity and privacy risk governance by adhering to Hood's et al. (2001) and May & Jochim's (2013) conceptualizations of a policy regime, to capture the overall way cybersecurity and privacy risks are governed in two central political systems – the US and the EU. The focus of this dissertation on these two central polities stems from the fact that these are the main arenas for promoting public policy over issues of cybersecurity and privacy. The Privacy Act was enacted in the US already in 1974, and cybersecurity issues were addressed by federal policymakers as early as 1972 through the Brooks Act. In the EU, privacy is a fundamental right (e.g. Whitman, 2004) that is regulated since 1995 at the EU level (95/48/EC), and cybersecurity is promoted by the Union since 1992 (EU Council Decision 92/242/EEC). Ever since, these polities have produced public policies to promote cybersecurity and privacy governance, leading the world in addressing these issues. Beyond the rich seam of cybersecurity and privacy policies in these polities, studying these cases would allow both an understanding of the politics behind the design of investigated policy regimes, and also the generalization of findings to additional national contexts. Since these policy domains are heavily influenced by the context of technological change, the closeness to state's sovereignty issues, and introduce complex institutional structures that represent commercial, individual, and security-oriented stakeholders, other nations are likely to experience similar dynamics and policy patterns when wrestling with the same global cybersecurity and privacy risks.

In terms of data collection, the policy regime approach enables a backward mapping of governing arrangements for a given policy problem while shedding light on the link between politics of the policy process and policy outcomes (May and Jochim, 2013). It considers institutional structures, rules, and actors that are associated with governing specific problems (Hood et al., 2001), and helps to illuminate the multiple dimensions of how a given problem is addressed over time. While this approach has been fruitful for studying changes in other policy domains such as welfare, employment, and pensions (Gosta Esping-Andersen, 1990;

Jacobsson, 2004; Béland and Shinkawa, 2007), it was yet to be used in studying the somewhat terra incognita of policy problems related to cyber insecurity and threats on privacy.

Policymaking in the cybersecurity and privacy landscape is often fragmented and disjointed, taking place in multiple levels of governance, historically developed in different points in time, with a variety of government agencies involved, and in a variety of policy contexts. The regime lens addresses these analytical challenges and allows an understanding of the temporal variance in the different components that have jointly governed cybersecurity and privacy risks within national contexts.

Current gaps in the empirical and theoretical understanding of cybersecurity and privacy governance are alarming. Continuous reporting on significant cyber breaches erodes the trust in digital technologies and threatens the well-being of societies. Moreover, significant privacy infringements by the U.S. intelligence community (Macaskill and Dance, 2013) and privacy scandals by powerful private monopolies (Wong, 2019) emphasize the urgency to better understand policy development and drivers for policy change in light of increased state and commercial capacities to collect personal information.

Therefore, the main goal of this doctoral project is to fulfill the empirical and theoretical gaps in the public policy literature with respect to cybersecurity and privacy governance. By adopting a policy regime perspective, this dissertation aims to *first* handle difficult-to-capture dependent variables and analyze how policy regimes for cybersecurity and privacy have developed in the past decades in two central political systems. *Second*, identify the micro-mechanisms that lead to certain policy outcomes in certain points in time and advance theory of policy change. And *third*, generate new research questions based on the dependent and independent variables captured in this dissertation to further develop public policy theories based on under-studied policy domains to advance the study of contemporary governance frameworks in the era of continuous technological change.

The main driving force behind this project is to assess how security, well-being, and fundamental rights in society are preserved in the age of digital technologies. As the first generation to become ‘all-digital,’ these policy systems are likely to design the ways risks from technology will be governed in the future, and it is crucial for us to understand how and why policymakers decide on these issues and construct the ways that risks from digital technologies are governed.

The dissertation consists of three separate papers that embrace a policy regime approach and study cybersecurity and privacy governance over time in the US and EU. The *first* paper explores how the U.S. balances between national security and privacy over five decades of advancements in digital technologies. Based on a novel analytical framework, this paper qualitatively analyzes (N=63) federal policies across three policy arenas to determine how policy processes harm, compromise, or complement privacy and national security. The *second* paper studies how U.S. federal cybersecurity policies frame cyber risks and consequently construct risk governance frameworks. Based on a systematic text analysis and a novel typology, this paper analyzes thirty federal policies from the past two decades from which (N=463) key sentences had been singled out and then coded to ten risk governance categories. It tracks and explains variance across sectors and over time in the way the U.S. government has responded to cyber threats as well as the link between cyber risk framings and policy outputs. The *third* paper examines a rather unexplored interaction between public and private authorities demonstrated by EU's cybersecurity governance arrangements. Based on a process-tracing analysis of the institutional frameworks for cybersecurity certification in the past two decades by using policy documents (N=40) and interviews (N=18), this paper reveals how and why private certification bodies became elevated and controlled by public authorities, questioning the dichotomous portrayal of the shift from government to governance.

In the following sections, I present the conceptualization of the policy regime perspective and its promise for analyzing the cybersecurity and privacy policies spaces, elaborate on the empirical approach that was used across the three dissertation papers, and overview the three papers including the gaps they fulfill in the current literature.

A policy regime perspective to study policy problems

Policymaking is a political enterprise whereby policies are shaped in an attempt to govern policy problems. Still, the role of policies as governing instruments driven by political factors is hard to capture, especially for complex policy problems that are governed by a patchwork of laws and regulations, transpiring in frameworks that develop over time or across sectors, through the involvement of various government agencies, and by the usage of different institutional structures.

Through the policy regime lens that had initially emerged in the field of international relations (Martin and Simmons, 1998), and was later on conceptualized by May and Jochim (2013) as the overall governing arrangements for addressing policy problems, we can construct a conceptual map that considers all the individual components composing the governance over a policy problem over time. Rather than starting with a policy measure, the unit of analysis is a policy problem for which the combinations of multiple laws, rules, and administrative actions give rise to relevant governance arrangements. These usually include authoritative components such as executive orders and presidential directives in the US, or directives and regulations when it comes to the EU. The breadth of a policy regime is determined by the boundaries that circumscribe the analyzed policy problem. The regime perspective can apply to different levels of international, national, and private governance arrangements, and policy regimes can be narrowly or broadly constructed.

The added value of the regime lens approach to the cybersecurity and privacy policy spaces is both descriptive and analytical. It paves the way for a backward mapping of governance arrangements for a given policy problem and highlights how the politics of the policy process are constructed to design specific policy outcomes by taking into account the institutional arrangements, interests alignments, and shared ideas in regard to a certain policy problem over time.

Other possible analytical frameworks such as the ‘Agenda-Setting’ framework (Kingdon, 1984; Howlett and Ramesh, 2003), or the ‘Advocacy Coalition Framework’ (Sabatier, 1988; Fischer, 2014) are less suitable for analyzing the cybersecurity and privacy policy spaces. *First*, the ‘Agenda Setting’ framework, is focused on understanding how issues reach the agenda and become debated by policymakers. This framework highlights the varying conditions for introducing new issues to the policymaking agenda, and therefore restricts our understanding to specific independent variables that influence the introduction of privacy and cybersecurity issues to the agenda. These can include focusing events such as 9/11, or the growing threat landscape from digital technologies. This framework also highlights the importance of political conditions for introducing issues to the agenda (Kingdon, 1984). These can be the establishment of new government agencies, political coalitions from left and right that are formed after certain public outcries, or energetic ‘policy entrepreneurs’ that constantly push for policy change in the investigated policy spaces. While the examination of these independent variables is important and can be fruitful for analyzing the cybersecurity and

privacy policy spaces, the ‘Agenda Setting’ framework mostly ignores the content of the proposed policies and the different ways these policies mediate between values or govern risks from digital technologies. In contrast, the Policy Regime framework allows to take all this into consideration. It allows for the account of both policy content and context in the process of policy regime building. Also, in the cybersecurity and privacy policy spaces, many of the policy measures were introduced over time, with a variety of actors involved, and no single policy entrepreneur to follow. This stresses the significance of temporal variance in these policy spaces, which can only loosely be explained by studying micro dynamics around every policy event as suggested by the ‘Agenda-Setting’ framework. The Policy Regime perspective does highlight important drivers and contexts for the introduction of new policies but allows to study them as components in a broader effort to govern cybersecurity and privacy risks, and thus, advance our understanding on the drivers for the policy structures that were created to govern these policy problems.

Another competing framework is the ‘Advocacy Coalition Framework’ that suggests that policy change is the consequence of changes in advocacy coalition structures within policy subsystems (Sabatier, 1988; Fischer, 2014). Such coalition change occurs because of individual actors’ belief changes and actors seek to translate these beliefs into policies through coordinated action within advocacy coalitions (Weibe et al., 2011). Exogenous factors are specifically identified as important factors for belief change, and this analytical framework is focused on defining and describing coalitions constellations at a given point in time. Whereas this framework is useful for understanding the different groups that advance policy change in the cybersecurity and privacy policy spaces, and especially would allow a differentiation between different types of commercial interests that influence these policy spaces, it would only capture certain parts of drivers for change in these spaces. In contrast, the Policy Regime perspective would allow a broader understanding of the change in the content of these policies as well as changing roles of certain policy actors and coalition groups over policy issues over time. While changes in coalition groups seem important for the policy spaces under study, they uncover only parts of the temporal and sectoral variance that is observed. Other independent variables such as institutional settings and structures, or the capturing of intriguing dependent variables based on changes in policy content in these policy spaces, cannot be fully observed by using the Advocacy Coalition Framework.

Moreover, the policy regime perspective was already successfully embraced by policy scholars who study welfare, employment, pensions, and so forth. For instance, Gosta Esping-Andersen (1990) traced the development of policy regimes of welfare state arrangements in several nations. Conceptualized three different types of regimes based on their policy content, he was able to discover new explanatory factors to different types of welfare states. In addition, Jacobsson (2004) studied the development of employment policies in the EU. He traced three decades of soft employment policies to realize how a soft system of governance is designed at the EU level and can transform practices in Member States. Another example is Béland and Shinkawa's (2007) comparative study on pension policies in four nations. These scholars were able to characterize national pension regimes and bring several theories together to explain variance in these regimes through historical institutional arrangements, shared ideas, and interest groups' influence. The embracement of the Policy Regime framework by these scholars allowed them to devote their attention to changes in the content of policies over the studied policy problems, recognize unexplored dependent variables, while also tracing causes for policy change that are connected to the structure of the designed policy regimes and the contextual factors of policy regime building.

Thus, in each of these examples, the policy regime perspective captured new dependent variables based on national or temporal variance in newly characterized policy regimes. In addition, the regime perspective led to the discovery of independent variables to account for such variance and unravel the drivers and influential actors that are associated with the development of each regime. This has been conducive to theory by explaining how the politics of the policy process yield varying policy outcomes within and across policy regimes.

Therefore, I argue that the policy scholarship can benefit from applying a regime perspective to cybersecurity and privacy governance. It provides new insights for studying policy development and understanding the governing role of policies. While applying the perspective itself does not provide explanatory power, it helps highlight the realities of how policymakers address policy problems and what are the political dynamics these realities engender. It emphasizes the constellation of political and institutional forces operating in the case of a certain problem, identifying possible explanatory factors and micro mechanisms underlying policy outcomes within a policy regime. It complements policy theories by allowing us to consider how they operate on specific problems and through political processes, thereby advancing the understanding of the politics of policy regime construction.

The empirical approach for studying variance in policy regimes

In order to properly capture the different components of a policy regime methodologically, there is a need to conduct a backward mapping of the governing arrangements and have a firm understanding of the issues and relevant policies that govern a given problem (May and Jochim, 2013). Acknowledging the relevant interests and different stakeholders' positions in a policy regime requires a close reading of the relevant debates at the time of policy enactment while considering how given policies affect different interest groups and are influenced by institutional structures and certain paradigms.

Thus, to empirically understand how public policies govern cybersecurity and privacy-related problems in the US and EU over time, I chose to use the (1) *process-tracing methodology* for the first and third chapters, and (2) a systemic *inductive and deductive text analysis* for the second chapter.

The process-tracing analysis methodology is defined as 'the analysis of evidence on processes, sequences, and conjunctures of events within a case for the purposes of either developing or testing hypotheses about causal mechanisms that might causally explain the case.' (Bennet and Checkel, 2015, p.7). This methodology was chosen because of its qualities as a within-case analysis methodology for studying cases for the first time (Bennet and Checkel, 2015) and its ability to tackle the 'dependent variable problem' in policy studies (Kay and Baker, 2015): Addressing policy as variables displays various spatial, temporal, and complexity characteristics that make it difficult to trace causally. A policy change can occur across a nested hierarchy of layers, levels, or orders of abstraction. Mechanisms underpinning policy change can thereby operate at the micro (individual behavior), meso (the actions of policy communities and networks), and macro (institutional or social systems that structure political interaction) levels – all three levels can be important in determining or constituting a given policy process. A careful implementation of the process tracing methodology allows to capture that and uncover new dependent variables while how certain independent variables interact with them.

The methodology had enabled me to develop an in-depth understanding of elements of cybersecurity and privacy policy regimes that are part of a pattern of meanings within the cases under study. I was able to reveal elements of the policy process such as the levels of transparency or the framing of issues through technological contexts within US policy systems

in the first chapter, as well as the significant influence of European Member States in the cybersecurity certification regime and EU's supranational aspirations for policy change in the third chapter. These findings may be otherwise overlooked because identifying common themes across cases in cross-case analysis may dilute the findings of individual cases. The methodology was also helpful in capturing the structure of the policy regimes under study. This can lead other researchers to new insights that determine the later analysis of other cases, or provoke new questions (Bennet and Checkel, 2015).

Since this dissertation aimed to comprehensively study these policy spaces in US and EU national contexts for the first time, this methodology was the most appropriate one to appreciate the uniqueness of each case and enabled me to be thoroughly immersed in the data within each context, fostering the emergence of the unique attributes and patterns in each case, before a possible next step of attempting to locate general patterns and themes that exist in parallel domains in the literature.

In practice, the process tracing methodology allowed to advance typology development, hypothesis generation, and theory building around the cases of cybersecurity and privacy governance, with no clear prior theory to derive research expectations from (Bennet and Checkel, 2015). Such portrayals of the cases under study were necessary as a data reduction strategy to deal with the daunting amount of data that case studies had generated. It was also a useful way of organizing the data that allowed for conclusions to be drawn in ways that might be appealing for other policy spaces or in different national contexts. The methodology led to research outcomes that directly address the dissertation's goals. It allowed to identify commonalities and differences in the case data, capture new dependent variables, explain the mechanisms behind them, and generate new research questions.

I had collected all the relevant policy documents and mapped the actors, interest groups, institutional structures, and shared ideas to trace their development over time in the US and EU cybersecurity and privacy policy spaces. In the *first chapter*, for capturing the US policy regime that governs the relationships between national security and privacy over time, I analyzed three sub-regimes of information collection: for criminal investigations, foreign intelligence gathering, and cybersecurity protections for vital information systems. These regimes evolved in tandem with the expansion of digital technologies over the last five decades, constructing plural types of relationships between privacy and national security.

To measure how these policies address privacy risks over time, the first chapter adopted a working definition for privacy according to certain conceptualizations of a privacy harm. Privacy harms in this paper are understood as actions that undermine individual's autonomy, dignity, and self-determination, by threatening individuals' ability to control how their personal information is collected, accessed, and used, often without their knowledge. The paper gathers that such threats increase when privacy oversight and scrutiny procedures for information collection are relaxed by policymakers. Thus, instead of understanding privacy in terms of noninterference in individuals' private space (Warren & Brandies, 1890), the paper adopts a definition of privacy as control and knowledge individuals have over collections, processing, and other uses of their personal information and therefore study policies that either protect or relax oversight over such practices. Thus, it attaches privacy harms to personal information, and not necessarily limits it to personal space, in order to grasp a broad understanding of how privacy is protected or abused by policymakers through public policies.

An original data set was created, featuring policy events (N=63) from the years 1968–2018 that delineate the three sub-regimes under study. Each policy event was classified into one of three possible categories according to its effect on the relationships between privacy and national security. These categories include: (i) detriment to privacy for the sake of national security; (ii) creating a compromise between the two; or (iii) advancing complementary relationships that enhance both. Then, I was able to recognize the dependent variable of this research and explain variance in privacy and national security dynamics over time and across policy arenas based on characteristics of the policy process, commercial interests, and leading actors in each sub-regime.

Specifically, three of the four examined policy characteristics in these policy processes were chosen according to the literature on the appropriate norms for administrative law (Haque, 2001; Benish and Levi-Faur, 2012) and include the openness and transparency of the process, the involvement of commercial interest in the policy process, equal representation of the different stakeholders in the process. I also borrowed from the literature on agenda-setting to study the context in which those policies were introduced (Kingdon, 1984; Howlett and Ramesh, 2003).

Process-tracing was also used for the *third chapter*, to capture the EU certification policy regime that governs the policy problem of cyber risks in connected devices and supply chain processes. I traced how the institutional frameworks for cybersecurity certification have

changed over the course of two decades through the collection and analysis of 40 relevant policy documents and reports and 18 interview transcripts with key stakeholders in the field. In those interviews, I asked for insights about the current and proposed certification regime, the public-private interactions in both regimes, and main compromises that were made during the policy process. By doing so I was able to recognize the dependent variable of this research – the temporal variance of institutional paths for cybersecurity certification in the EU, namely the publicization of private certifiers for cybersecurity by the EU. Tracing the links between possible causes for the publicization of private certification bodies and observed outcomes, I centered on sequential processes within the legislative process.

Bringing the political context of this regime change into play, I tested my hypotheses as follows: to measure the influence of Member States, I traced stated positions by national authorities, the veto powers that Member States gained in the process, and the changes that Member States were able to incorporate in the text. To measure the influence of EU's supranational aspirations, I traced the significance of the proposed change to EU's policy standing in the field, and the battles that the Commission chose during the legislative process. Finally, to measure the influence of private interests, I traced all the arguments in the collected position papers, realizing how significant was the addition of new institutional paths for certification to private groups, even if the price private certification bodies had to pay was increased control over their operations.

One of the main challenges to the process-tracing methodology is that researchers will use it unsystematically with potential inferential errors (Bennet and Checkel, 2015). In order to cope with that, I've used some methodological safeguards that include: (1) Justifiable decisions on where to start and end data collection efforts. For the first and third papers, I chose that starting points of data collection based on critical junctures at which a governance practice was contingent to alternative paths, and the actors involved determined which path it would take. In the first dissertation chapter, the decision to regulate information collection for the first time in 1967 through the Wiretap Act was a crucial starting point in the development of the policy regime under study. In the third dissertation chapter, the 1997 mutual recognition agreement regarding security certificates between European nations was the first mutually agreed certification mechanism in Europe, that was produced in response to EU Council Decision from 1992 (92/242/EEC) and a subsequent Council recommendation from 1995 (1995/144/EC) on common information technology security evaluation criteria. Reviewing these two starting

points in each chapter in retrospect highlighted their key role in the development of the policy regimes under investigation in those chapters.

Another methodological safeguard is in (2) the decision when to stop – In both process-tracing based chapters, I decided to stop pursuing one stream of evidence when it became so repetitive that gathering more of that same kind of evidence had a low probability of revising my estimate of the likely accuracy of alternative explanations. For the first chapter, data collection ended when additional sources did not highlight new trends regarding decision-making processes over each policy event under study. For the third chapter, in addition to that logic, no more interviews were conducted once I realized that the framing of the dependent variable and the explanations for its evolvement are starting to repeat themselves.

Another challenge in process tracing is the risk of incorporating potential bias of evidentiary sources (Bennet and Checkel, 2015). To cope with that, I have (3) considered a wide range of primary and secondary sources in both process-tracing based chapters of the dissertation. For the first chapter, I have investigated different types of policy measures and consequently different types documents that surrounded their establishment. In addition, I relied on secondary sources – works of scholars from a variety of disciplines that include law, national security, criminologists, and military studies – to bring together contending historiographical schools and explanations. For the third chapter, I had gathered policy documents from all EU institutions, a variety of private stakeholders in the certification regime, and relied on interviewees from EU institutions, agencies, and different types of private stakeholders – certification bodies, evaluation laboratories, product manufactures, digital service providers, and industry associations.

A final significant challenge in the process-tracing methodology is the missing data challenge. Given the critical importance of analyzing data on every ‘step’ of the process for process tracing to be robust, I had to cope with the problem of limited data in certain points in time regarding the policy regimes under study. Therefore, during the analysis process, beyond relying on diverse streams of evidence, I was able to (4) locate data points that were more valuable than others, and cover for missing data in specific segments. I found that a single meeting or memo may prove to be the crucial piece of evidence that instantiates one explanation or undermines another. This follows Bennet and Checkel’s (2015) observation according to which what matters is not the amount of evidence, but its contribution to adjudicating among alternative hypotheses, stressing the relationships between the evidence

and the hypotheses, and not the number of pieces of evidence. For instance, in the first chapter, I was able to find various secondary sources that directly quote policymakers on the way they frame policy problems in light of technological changes. This was a direct demonstration of my hypothesis about the different instrumental use of technological change over time. Another significant source of evidence in the first chapter was classified documents that were publicized by whistleblowers and verified policy patterns in time frames for which I had limited data about. These unclassified documents provided strong confirmatory evidence (Bennet and Checkel, 2015) that my hypotheses about policy trends in the policy regime under study were indeed happening ‘on the ground.’ In the third paper, pieces of evidence that significantly contributed to my understanding of the relationships between my hypotheses and reality were interviews with policymakers and industry stakeholders who anonymously pointed out to the strong influence of Member States on the policy process, while also addressing EU Commission’s supranational aims in the field of cybersecurity. The limited access to official documents about these standings became less crucial once several interviewees from different segments agreed to clearly state these trends, thus providing confirmatory evidence to what was happening in this policy space behind ‘closed doors.’

Another helpful strategy to cope with missing data was to (5) use a comparative case study analysis within the same case over different periods of time. Temporal differences were identified in each of these chapters and were explained through the examined research hypotheses, turning the focus to differences in different points in time, and emphasizing the importance of having convincing unbiased evidence from each time frame under comparison, rather than having ‘enough’ evidence on every step of the way. In the first paper, the comparison between the three time periods of policy trends in national security and privacy policies, as well as the comparison between the different policy arenas, highlighted the significance of evidence that was gathered to explain differences and similarities in these two comparisons. In the third paper, the comparison between the two policy regime periods – before and after the enactment of the Cybersecurity Act – allowed to emphasize the role of Member States, interest groups, and EU aspirations in this policy process, providing great emphasis to evidence that was gathered through interviews and documents’ analysis.

Moreover, an important strategy for missing information in the third paper was the (6) particular operationalization of the three hypotheses under examination and their adaption to

specific processes predicted in the particular case. This was helpful in clarifying as much as possible the facts and sequences that should be true if each of the alternative hypothesized explanations of the case were true (Bennet and Checkel, 2015). In the beginning of the research process, and as described in chapter 3, I had clearly stated the indicators for each tested hypothesis and looked for its possible appearance in the collected data. This provided focus to the data analysis process and helped cope with missing data in certain time frames with the policy regime.

By and large, keeping these limitations and the way they were remediated in mind, I believe that the methodological approach taken by these studies yields reliable results that can be carefully generalized based on the characteristics of the cybersecurity and privacy policy spaces, also serving as a point of reference for studying similar policy problems in additional political systems. The novel analytical framework for studying the dynamics between national security and privacy in the first chapter and the novel understanding of the EU cybersecurity certification regime in the third chapter can be fruitful for studying additional policy regimes, not only across nations, but also across issues, explicating how policymakers govern risks for society.

For the second chapter, I used a different methodology of *systemic inductive and deductive text analysis* for capturing the US policy regime that governs the policy problem of mitigating cyber risks across private sectors. I used qualitative research methods to examine, in a systematic way, a corpus of thirty federal cybersecurity policies that includes statutes, executive orders, policy strategies, and secondary legislation of federal agencies between the years of 1996 and 2018. I chose the US federal cybersecurity policy arena as my case study because it has been evolving for the past 22 years, something which allowed me to mine the rich seam of cyber risk frameworks and governance practices.

I analyzed federal policy texts in two phases. In the *first* step, I had signaled out key sentences and afterwards, assigned code or several codes per sentence, representing its principal content or theme. After removing redundancies and duplicate codes, seven codes that uncover different categories of cyber risk-management emerged. In the *second* step, I conducted a deductive analysis based on pre-defined categories derived from Renn's study (2008) on the early phases of risk governance – pre-assessment, assessment, characterization and evaluation. My goal was to deductively detect additional categories in the policy texts and understand how policymakers frame, assess, characterize and evaluate cyber risks.

Within the thirty policy texts, (N=463) key sentences were identified. The two phases of the text analysis had yielded a typology of ten categories that was then used to classify key sentences in each federal policy into a risk governance phase of pre-assessment, assessment, characterization and evaluation, or risk management. I drew on secondary sources of information to further understand how federal policies shape cyber risk governance frameworks for each sector. Following the analysis, three sub-regimes that differently govern the policy problem of cyber insecurity in the private sector have emerged, and I was able to frame the dependent variable of the research and explain its evolvement through shared ideas and early institutional practices in each sub-regime.

To summarize, in all three papers, the analysis of the various sources of information from different periods in each regime allowed me to capture the dependent variables that demonstrated temporal, sectoral, and contextual variance in each captured policy regime. Subsequently, I tested possible research hypotheses based on the existent literature, relying on the same or additional information sources to explain the dependent variable in each paper.

Summary of papers

The three dissertation papers conceptualize and study policy regimes in two central political systems – the US and EU - over three policy problems that are related to emerging risks from digital technologies. They explore how and why US policies have constructed the relationships between national security and privacy (first paper), the US cyber risk governance regime has been emerging across sectors (second paper), and how EU's institutional frameworks for cybersecurity certification has been changing to incorporate private governance actors (third paper).

1. Complementaries and Contradictions: National Security and Privacy Risks in U.S. Federal Policy, 1968–2018

The first dissertation paper was published as an article in 2018 in *Policy & Internet*. It addresses gaps in the current literature that mostly brings forth theoretical rather than empirical studies about the relationships between national security and privacy, and does not consider how policymakers de-facto set these dynamics in the age of digital technologies. Moreover, scholars who conduct empirical work on these dynamics mostly consider contradictory rather

than complementary dynamics between the two goals, and study only short periods. They do not address the plurality of dimensions for these relationships, nor do they assess their development over five decades. Thus, they set forth rather limited regime boundaries for studying this policy problem.

In contrast, this paper broadens current regime boundaries in the literature, examining various dimensions in the dynamics between privacy and national security in US federal policymaking. Through a comparative process-tracing analysis of three policy arenas—criminal investigations, foreign intelligence, and cybersecurity—over five decades, this study shows how national security efforts enhance or infringe upon privacy safeguards. It classifies policies into three categories: (1) policies that impinge on privacy in favor of national security; (2) policies that create a compromise between privacy and national security; and (3) policies that complement privacy and national security, and considers how these relationships have changed over time, across different stages of the policymaking process, and in various policy contexts.

The paper finds that US federal decision-making regarding privacy and national security has been made out of a patchwork of laws and regulations that changes over time and across the three policy arenas. Instead of a single equilibrium between the two goals, this study finds that they are mediated by a plurality of contexts, interests, and policy arenas, underscoring the value of applying a policy regime perspective to this policy problem.

As in previous scholarly works, an overall erosion of privacy over time is indeed revealed by this study. This is not only reflected quantitatively (out of 38 policies of contradictory dynamics, 21 impinged on privacy for the sake of national security), but also qualitatively, setting unprecedented expansions in surveillance authorities. Once a policy that can potentially encroach on privacy is introduced, it is unlikely to be fully reversed.

Still, there are multiple policy trends to follow, ones that are shaped by different actors and policy processes. To better understand the balance between privacy and national security, we need to assess the context of power relationships between Congress, the executive branch, and commercial interests, and pay close attention to problem framing and types of policy processes mediated by these actors, including the different levels of transparency and the motley variety of actors allowed into the policy process.

By considering the full spectrum of policy relationships between privacy and national security, this paper provides a well-rounded picture of the factors that drive change and the ways the goals are balanced. Government can be a source of both problems and solutions for guarding citizens' privacy. Convergence of interests between commercial companies and intelligence agencies is revealed across arenas, as both parties push for lax privacy protections in the foreign intelligence and the cybersecurity policy arenas. Moreover, tracing the roles of Congress and businesses over time also displays an alarming pattern. While both actors have been facilitating a transparent policy process and had pushed back against the executive branch's attempts to expand surveillance in the 1980s and 1990s, their efforts in that direction were considerably less effective following the 9/11 attacks. Instead of holding the executive branch accountable, Congress provided supportive legislation and passed measures without meaningful debates.

2. Framing and Governing Cyber Risks: comparative analysis of US federal policies [1996-2018]

The second dissertation paper was accepted for publication at the *Journal of Risk Research*. It addresses gaps in the existent literature on cybersecurity governance, as current writings consider only specific policy measures at certain points in time, and do not investigate the link between policymakers' risk framings and chosen policy paths.

Contrarily, this paper adopts a policy regime perspective in an original manner for studying how cybersecurity governance arrangements develop over time and change across sectors. It also traces distinct shared ideas and risk framings within the regime, showing how cybersecurity is perceived by policymakers as a public/private infrastructure concern, a data protection problem, or a tool to safeguard financial interests. This reveals three different sub-regimes that vary across critical infrastructures, health and financial service providers, and the broader digital economy, putting forth different objects to protect, threats to consider, and roles for the actors involved.

To comparatively analyze the three sub-regimes, the paper conducts a text analysis of thirty US federal cybersecurity policies between the years of 1996 and 2018, extracted (N=463) key sentences in these texts, and suggested a typology for translating federal policies into risk governance frameworks. Then, based on the characterizations of cyber risks in these texts, and

the initial decision-making structures they have created, it explains the extent to which frameworks of cyber risk governance have changed across sectors and over time.

The paper found variance across sectors in the role of the government and the extent to which it dictates coercive risk management steps. It also discovered variance over time, that is, on the ways in which the government has responded to cyber threats. Across sectors, policymakers were bound to certain framings, assessments, and evaluations of cyber risks that informed their risk management policy decisions. The role of the government and the extent to which it has dictated coercive risk management steps were only loosely attached to the way these risks were framed by policymakers in the same policy texts. Over time, it seems that the government has been responding to the dynamic cyber threat landscape, but within the boundaries and paradigms of the decision-making structures stipulated during early regime development. For each regime, the government tried to improve risk management practices without diverging from previous policy paths considerably: the private sector still enjoys significant discretion in decisions pertaining to the protection of critical infrastructures, whereas health and financial industries encounter the increasing monitoring and enforcement capacities of top-down regulators. Non-critical sectors are still governed based on incentives and completely self-regulatory models, regardless of evidence-based hazard estimations and the perceived seriousness of the risk. Each regime has had its own punctuation points in time. The protection of critical infrastructures and health and financial service providers has remained stable over time, whereas the protection of non-critical sectors seems to be more dynamic and open to prospective changes.

Unsurprisingly, increased sophistication of cyber threats over time has led the federal government to respond, albeit in ways that mirrored existing paradigms and did not diverge from two-decade old decision-making structures.

By tracing the governance of cyber risks and the link between policymakers' risk perceptions and actions, this paper demonstrates how seemingly technical decisions of cybersecurity governance can be social and political issues that are contingent early policy decisions rather than problem framing.

3. EU Publicization of Private Certifiers for Cybersecurity: explaining public-private interactions through the context of institutional change

The third dissertation paper is completed and ready to be sent for first review to *Governance*. It addresses gaps in understanding how public authorities interact with private governance actors in indirect governance arrangements. While this strategy has been gaining traction across sectors and political systems, we lack an understanding of how public-private interactions emerge in cybersecurity policy regimes, and do not know whether these interactions can advance our theoretical understanding about private authorities in contemporary governance arrangements.

Notably, a recent innovation in EU cybersecurity governance suggests a rather unexplored type of public-private interaction in indirect governance arrangements. Through the establishment of the EU Framework for Cybersecurity Certification, policymakers have elevated the role of private certification bodies to issue certificates on behalf of the EU while increasing public control over their operations. In contrast to full public control in delegation dynamics or the lack of control in orchestration interactions, this interaction suggests a different type of dynamic for private actors who voluntarily enlist themselves for governing on behalf of public authorities, becoming subordinate to their supervision. This intriguing dynamic begs the questions: how and why has such public-private interaction evolved?

The literature provides little attention to this type of interaction and does not take into account the politics of governing certification bodies. Scholars of private governance mostly address the emergence of private regulators due to states' inaction. When the government becomes involved, public-private interactions usually take one of two forms: (1) top-down interactions in the form *delegation*, outsourcing specific regulatory tasks to private actors under strict public control, or (2) non-hierarchical interactions in the form of *orchestration*, exchanging private regulatory capacities for public material support.

Nonetheless, in the policy regime for EU cybersecurity certification, a third public-private dynamic of increased state control over the operation of voluntary enlisted private regulators has been emerging. The paper frames this dynamic as 'publicization' and argues that we should appreciate its institutional context in order to explain its evolvement. It explains the political drivers for publicization by highlighting the importance of its institutional context. It considers public control over private regulators as a component in a broader institutional change, finding that despite promises by EU policymakers to 'completely replace' and 'fundamentally change' the ecosystem for certification, new institutional paths are established

in addition, rather than instead of existing frameworks. Consequently, public-private interactions have diffused from the current certification regime.

Markedly, scholars of endogenous institutional change mostly ignore the public or private nature of institutional frameworks and do not link modes of change with the distribution of public or private authorities. This paper, nonetheless, argues that causes for institutional change can shed light into why policymakers choose certain public-private interactions when designing institutional changes.

To capture the change in EU cybersecurity certification, the paper embraces a policy regime perspective for studying institutional frameworks for EU cybersecurity certification in the past two decades. Based on May and Jochim (2013) conceptualization of policy regimes, I expect the regime perspective to be highly adaptable to multi-level governance. Thus, through a qualitative process-tracing analysis based on 40 policy documents and 18 interviews, the paper traces the elevation and the extra public control imposed on private certification bodies in the new institutional frameworks. It recognizes this temporal variance by broaching the multiple levels of governance in these arrangements.

To explain these public-private interactions, the paper tests three hypotheses that consider: (1) Member States' powerful influence in this policy space, (2) EU's supranational aspirations, and (3) The significant benefits to private interest groups in the new framework. Testing these hypotheses reveals how Member States were able to pose on the EU a policy compromise that prevented a significant divergence from current institutional paths. It also discovers that the EU was able to strategically improve its standing in the cybersecurity policy arena and secure a long-term EU interest, in the price of allowing Member States to increase their control over private certification bodies and maintain existing institutional frameworks. Finally, it stresses how industry groups that benefited from the new framework posed no opposition to enhanced national control over private certification bodies.

Thus, the publicization of private governance actors was a political compromise led by actors with strong veto powers and low discretion capacities, who were able to diffuse current public control practices over private governance actors to the prospective framework. This highlights a rather unexplored link between private governance and the institutional change literature, demonstrating how the reasons behind modes of institutional change hold

explanatory powers for understanding why certain types of public-private interactions have emerged.

This study is conducive to our understanding of political battles in the cybersecurity policy arena. On the one hand, the paper found that Member States pushed for layering practices in order to increase the stability and legitimacy of current, nationally dominant, institutional frameworks for certification. The EU, on the other hand, was also successful in promoting the link between cybersecurity issues and its Single Market approach, further legitimizing its intervention in this policy field.

By studying a rather new and unexplored type of public-private interaction and capturing the transformation of private certification practices within the policy regime, this paper underlines how public authorities take center stage in the operation of private ones. Throwing light on a hybrid form of governance, this study adds to our understanding of the political considerations taking place at the often-overlooked phase of standards' implementation. This undertaking creates a novel link between patterns of endogenous institutional change and public-private interactions, expounding the political context of a new form of intervention by the state - one that calls into question the dichotomous portrayal of the shift from government to governance and comes to pass through the publicization of market-driven governance practices.

Bibliography

- Béland, D. and Shinkawa, T. 2007. "Public and Private Policy Change: Pension Reform in Four Countries." *The Policy Studies Journal* 35(3): 349-71
- Benish A., and D. Levi-Faur. 2012. "New Forms of Administrative Law in the Age of Third Party Government." *Public Administration* 90 (4): 886-900
- Benn, S.I. 1971. "Privacy, Freedom, and Respect for Persons." In *Privacy*, eds. J.R. Pennock and J.W. Chapman. New York: Atherton Press, 1-26.
- Bennet A., and J. T. Checkel. 2015. *Process Tracing: From Metaphor to Analytic Tool*. Cambridge: Cambridge University Press
- Choucri, N. 2012. "Cyberpolitics in international relations." Cambridge, MA: MIT Press.
- De Groot, J. 2019. "The History of Data Breaches." *Digital Guardian*. Available here: <https://digitalguardian.com/blog/history-data-breaches>
- Diffie, W., and S. Landau. 2007. *Privacy on the Line: The Politics of Wiretapping and Encryption. Updated and Expanded Edition*. Cambridge: MIT Press.
- Dunn Cavelty, M. 2010. "Cyber-Security." In *The Routledge Handbook of New Security Studies*, ed. P.J. Burgess. Oxford: Taylor and Francis, 154-62.
- Esping-Andersen, G. 1990. "The Three Political Economies of the Welfare State." *International Journal of Sociology* 20(3): 92-123.
- The Federal Trade Commission (FTC). 2017. "The Equifax Breach." *FTC.gov*. Available here: <https://www.ftc.gov/equifax-data-breach>
- Fischer, Manuel. 2014. "Coalition Structures and Policy Change in a Consensus Democracy." *Policy Studies Journal* 42(3): 344-366.
- Fried, C. 1968. "Privacy." *Yale Law Journal* 77: 475-93.
- Gavison, R. 1980. "Privacy and the Limits of Law." *Yale Law Journal* 89: 421-71.
- U.S. Government Accountability Office (GAO). 2017. "Cybersecurity: Actions Needed to Strengthen U.S. Capabilities". *Testimony before the Subcommittee on Research and Technology, Committee on Science, Space, and Technology, House of Representatives*.
- Genschel P., and M. Jachtenfuchs. 2013. *Beyond the Regulatory Polity?: The European Integration of Core State Powers*. New York: Oxford University Press.
- George, A. L., & Bennett, A. 2005. *Case studies and theory development in the social sciences*. Cambridge: MIT Press.
- Granick, J. 2017. *American Spies: Modern Surveillance, Why Should You Care, and What to Do About It*. Cambridge: Cambridge University Press.
- Haque M. S. 2001. "The Diminishing Publicness of Public Sector Under the Current Mode of Governance." *Public Administration Review*. Vol 61(1): 65-82.
- Hood C., Rothstein H., Baldwin R. 2001. *The Government of Risk: Understanding Risk Regulation Regimes*. Oxford, Oxford University Press.
- Howlett M., and M. Ramesh. 2003. *Studying public policy: Policy cycles and policy subsystems*. OUP: Canada.
- Jacobsson, K. 2004. "Soft Regulation and the Subtle Transformation of States: The Case of EU Employment Policy." *Journal of European Social Policy* 14(4): 355-70
- Kay A., and P. Baker. 2015. "What Can Causal Process Tracing Offer to Policy Studies? A Review of the Literature." *Policy Studies Journal* 43(1): 1 - 21.
- Kingdon, J. W. 1984. *Agendas, alternatives and public policies*. Boston: Little Brown.
- Laudon, K.C. 1996. "Markets and Privacy." *Communications of the ACM* 39(9): 92-104.
- Lessig, L. 1999. *Code and Other Laws of Cyberspace*. New York: Basic Books.

- Macaskill, E. and Dance, G. 2013. "NSA Files: Decoded. What the Revelations Mean to You." *The Guardian*. Available here: <https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded>
- Martin, L. and Simmons, B. 1998. "Theories and Empirical Studies of International Institutions." *International Organization* 52 (4): 729–57.
- May, P. and Jochim A. 2013. "Policy Regime Perspectives: Policies, Politics, and Governing." *Policy Studies Journal* 41(3): 426-452.
- Myers, L. 2018. "Target targeted: Five Years on from a Breach that shook the Cybersecurity Industry." *Welivesecurity.com*. Available here: <https://www.welivesecurity.com/2018/12/18/target-targeted-five-years-breach-shook-cybersecurity/>
- Nye, J. S. 2017. "Deterrence and dissuasion in cyberspace." *International Security* 41(3): 44–71.
- Organization for Economic Co-operation and Development (OECD). 2012. "Cybersecurity Policymaking at a Turning Point." *OECD Report on the Digital Economy*. Available here: <https://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf>
- Organization for Economic Co-operation and Development (OECD). 2015. "Digital Security Risk Management for Economic and Social Prosperity." *OECD Recommendation and Companion Document*. Paris: OECD Publication. Available here: https://read.oecd-ilibrary.org/science-and-technology/digital-security-risk-management-for-economic-and-social-prosperity_9789264245471-en
- O’Flaherty, K. 2019. "Marriott CEO Reveals New Details About Mega Breach." *Forbes.com*. Available here: <https://www.forbes.com/sites/kateoflahertyuk/2019/03/11/marriott-ceo-reveals-new-details-about-mega-breach/#2b4c88fa155c>
- Raab, C. 2014. "Privacy as a Security Value." In *Jon Bing: En Hyllest/A Tribute*, eds. J. Bing, D.W. Schartum, L.A. Bygrave, and A.G.B. Bekken. Copenhagen, Denmark: Gyldendal, 39–58.
- Rachels, J. 1975. "Why Privacy Is Important." *Philosophy & Public Affairs* 4(4): 323–33.
- Renn, O. 2008. *Risk Governance: Coping with Uncertainty in a Complex World*. Earthscan, London: UK.
- Sabatier, Paul A. 1988. "An Advocacy Coalition Framework of Policy Change and the Role of Policy-Oriented Learning Therein." *Policy Sciences* 21 (2): 129–68.
- Solove, D. 2011. *Nothing to Hide: The False Tradeoff Between Privacy and Security*. New Haven: Yale: University Press.
- Waldron, J. 2003. "Security and Liberty: The Image of Balance." *Journal of Political Philosophy* 11 (2): 191–210.
- Waldron, J. 2006. "Safety and Security." *Nebraska Law Review* 85: 454–507.
- Warner, M. 2012. "Cyber Security: A Pre-History." *Intelligence and National Security* 27 (5): 781–99.
- Warren, S.D., and L.D. Brandeis. 1890. "The Right to Privacy." *Harvard Law Review* 4: 193–220.
- Weible, C. M., Sabatier, P. A., Jenkins-Smith, H. C., Nohrstedt, D., Henry, A. D., & deLeon, P. 2011. "A quarter century of the advocacy coalition framework: An introduction to the special issue." *Policy Studies Journal*, 39(3): 349-360
- Westin, A. 1967. *Privacy and Freedom*. New York: Atheneum.
- Whitman, J. Q. 2004. "The Two Western Cultures of Privacy: Dignity versus Liberty." *Yale Law Journal* 113: 1151-1222.
- Wong, J. 2019. "The Cambridge Analytica Scandal Changed the World – But it Didn’t Change Facebook." *Theguardian.com*. Available here: <https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook>
- Woollaston, V. 2017. "The NHS trusts and hospitals affected by the Wannacry cyberattack." *WIRED.com*. Available here: <http://www.wired.co.uk/article/nhs-trusts-affected-by-cyber-attack>
- Zetter, K. 2016. "Inside the cunning, unprecedented hack of Ukraine’s power grid." *WIRED.com*. Available here: <https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/>

CHAPTER 1

Complementaries and Contradictions: National Security and Privacy Risks in U.S. Federal Policy, 1968-2018

Sivan-Sevilla, Ido. 2018. “Complementaries and Contradictions: National Security and Privacy Risks in U.S. Federal Policy, 1968-2018”. *Policy & Internet*. DOI: <https://doi.org/10.1002/poi3.189>

Complementaries and Contradictions: National Security and Privacy Risks in U.S. Federal Policy, 1968–2018

Ido Sivan-Sevilla 

How does the U.S. balance privacy with national security? This article analyzes how the three regulatory regimes of information collection for criminal investigations, foreign intelligence gathering, and cybersecurity have balanced privacy with national security over a 50-year period. A longitudinal, arena-based analysis is conducted of policies (N=63) introduced between 1968 and 2018 to determine how policy processes harm, compromise, or complement privacy and national security. The study considers the roles of context, process, actor variance, and commercial interests in these policy constructions. Analysis over time reveals that policy actors' instrumental use of technological contexts and invocations of security crises and privacy scandals have influenced policy changes. Analysis across policy arenas shows that actor variance and levels of transparency in the process shape policy outcomes and highlights the conflicting roles of commercial interests in favor of and in opposition to privacy safeguards. While the existing literature does address these relationships, it mostly focuses on one of the three regulatory regimes over a limited period. Considering these regimes together, the article uses a comparative process-tracing analysis to show how and explain why policy processes dynamically construct different kinds of relationships across time and space.

KEY WORDS: national security, privacy, surveillance, cybersecurity, temporal policy trends, policy arenas

美国是如何平衡隐私和国家安全的？本文分析了三种监管信息收集体系（针对刑事侦查、外交情报收集和网络安全）如何在五十年间平衡隐私和国家安全。本文实施了一项基于政策舞台的纵向分析（其所包含的63项政策均在1968年到2018年之间提出），此分析用于确定政策过程如何对隐私和国家安全造成危害、损坏或补充。本文考量了背景、过程、行为者差异、以及商业利益在上述政策构建中产生的作用。长期的分析表明，政策行为者对技术背景的工具性使用，以及对安全危机和隐私丑闻的调用，已对政策变化产生了影响。跨政策舞台分析表明，政策过程中的行为者差异和透明度影响了政策结果，强调了商业利益所扮演的矛盾角色——既赞成又反对隐私保护。尽管现有文献的确研究了这些关系，但也主要聚焦于有限期间内上述三种监管体系中的其中一种。为了将这三种体系一同进行考量，本文使用一项比较过程追踪分析，以展示政策过程如何（以及为何）以一种动态的方式跨越时间和空间，建构不同关系。

关键词： 国家安全，隐私，监控，网络安全，临时政策趋势，政策舞台

¿Cómo equilibra los Estados Unidos la privacidad con la seguridad nacional? Este artículo analiza cómo los tres regímenes regulatorios de recopilación de información para investigaciones criminales, recopilación de inteligencia extranjera y ciberseguridad han equilibrado la privacidad con la seguridad nacional durante un período de 50 años. Se realiza un análisis longitudinal, basado en la arena, de las políticas (N=63) introducidas entre 1968 y 2018 para determinar cómo los procesos de políticas perjudican, comprometen o complementan la privacidad y la seguridad nacional. El estudio considera los roles del contexto, el proceso, la variación de los actores y los intereses comerciales en estas construcciones de políticas. El análisis a lo largo del tiempo revela que el uso instrumental de los contextos tecnológicos de los actores políticos y las invocaciones a las crisis de seguridad y los escándalos de privacidad han influido en los cambios de política. El análisis en todos los ámbitos de las políticas muestra que la varianza de los actores y los niveles de transparencia en el proceso moldean los resultados de las políticas y resalta los roles conflictivos de los intereses comerciales a favor y en oposición a las salvaguardas de la privacidad. Si bien la literatura existente aborda estas relaciones, se centra principalmente en uno de los tres regímenes reguladores durante un período limitado. Considerando estos regímenes juntos, el artículo utiliza un análisis comparativo de seguimiento de procesos para mostrar cómo y explicar por qué los procesos de políticas construyen dinámicamente diferentes tipos de relaciones a través del tiempo y el espacio.

PALABRAS CLAVES: seguridad nacional, privacidad, vigilancia, seguridad cibernética, tendencias de políticas temporales, arenas políticas

Introduction

Privacy and national security are two important goals in the U.S. federal arena. The extent to which these goals complement and contradict each other is dynamically determined by laws and regulations, through processes that take decades to unfold and contain various decision points (Diffie & Landau, 2007; Regan, 1995; Solove, 2011). The philosophy literature offers two perspectives on how to balance privacy and national security. Taking a utilitarian approach, Etzioni (1999, pp. 3–5) defines privacy as an individual right that should be balanced against national security concerns in times of crisis. When the crisis ends, security measures can gradually be rolled back (Etzioni, 1999, p. 25). In contrast, Waldron (2003, 2006), Zedner (2003), and Chandler (2009) argue that while security is the foundation of all other liberties, the public cost of advancing security at the expense of privacy weakens such security measures. According to Chandler (2009, pp. 132–138), privacy-invading security measures redistribute risks to minorities and create new patterns of vulnerability in digital infrastructures that undermine both security and privacy.¹ Privacy and national security, therefore, should be perceived as interdependent rather than mutually exclusive (Dworkin, 1977; Loader & Walker, 2007; Raab, 2014). According to Solove (2011), governments do not choose between privacy and national security but rather between the levels of privacy oversight within national security measures that prevents abuses of government power (Solove, 2011, p. 37).

Privacy proponents argue that privacy losses lead to an erosion of other values like anonymity, liberty, and freedom of speech and association (Raab, 2014; Solove, 2011; Waldron, 2003). Privacy demarcates between individuals'

personal and public lives (Raab, 2014, p. 40) as well as between public institutions and private citizens (Regan, 1995; Solove, 2008). As an enabler of other rights, privacy's incorporation into national security practices is therefore central to liberal society.

While the academic literature has theorized about the relationships between privacy and national security, an empirical study on how policymaking shapes these relationships has not been carried out. For instance, the role of commercial interests, which both undermine policy efforts to strengthen privacy safeguards and resist intrusive forms of government surveillance, has not been studied over time or across policy arenas. Furthermore, the effects of digital technologies on these relationships have not been fully explored. Even though technology increases governments' abilities to collect personal information (Diffie & Landau, 2007; Granick, 2017; Solove, 2011), the legal structure for protecting online privacy has not changed since 1986.² Although some uses of new technologies result in privacy infringements, others advance both privacy and national security. For example, cybersecurity policies enable governments to collect information but also protect personal information systems from external threats. Yet, this feature of cybersecurity has not been addressed by legal scholars and political scientists who study the relationship between the two goals.

This article examines this plurality of relationships between privacy and national security in U.S. federal policymaking. Through a comparative process-tracing analysis of three policy arenas—criminal investigations, foreign intelligence, and cybersecurity—over five decades, this study shows how the state's national security efforts enhance or infringe upon privacy safeguards. The literature provides insights into the processes that mediate the two goals, but usually views them as either contradictory or complementary and considers only short periods of time (e.g., Birnhack & Elkin-Koren, 2003; Diffie & Landau, 2007; Etzioni, 2011; Gidari, 2006; Newman & Bach, 2004; Regan, 1995; Solove, 2011; Warner, 2015).

This article extends these analyses by examining how federal statutes, executive orders, presidential directives, federal rules, policy guidelines, and court rulings constructed relationships between national security and privacy ($N = 63$) between the years of 1968 and 2018. It considers how these relationships have changed over time, across different stages of the policymaking process, and in various policy contexts. It classifies policies into three categories: (i) policies that harm privacy on behalf of national security; (ii) policies that create a compromise between privacy and national security; and (iii) policies that complement privacy and national security.

The article is organized into six sections. The first reviews the literature's approaches to the questions of how and why policies balance privacy and national security. The second defines the key concepts in the article—national security and privacy. The third presents the methods and analytical framework for studying the three regulatory regimes, and the fourth analyzes contradictory and complementary dynamics between privacy and national security over time in the United States. The fifth section presents this analysis across three policy

arenas (criminal investigations, foreign intelligence, and cybersecurity), while the final section concludes.

Literature Review

Longitudinal studies of privacy and national security policymaking in the U.S. federal arena conducted over the past decades have shown that legislators usually prioritize national security over privacy. Throughout the mid- to late twentieth century, privacy often appeared on the legislative agenda following technological changes that provided new kinds of access to personal information (Flaherty, 1989; Regan, 1995, p. 5). Despite a significant amount of congressional activity, only a few pro-privacy statutes were enacted during this period (Regan, 1995, p. 7). In these cases, legislation usually conformed to the following pattern: those who benefitted from privacy infringements framed the policy problem and faced opposition from a small community of privacy advocates. Then, in debates over privacy protections, the final legislation would include the most minimal possible protections (Regan, 1995, p. 22). Regan (1995, p. 23) explains this pattern as a factor of policymakers' perceptions of privacy as an individual value, rather than as a social value, which competes with collective goals like crime mitigation and government efficiency. In their study of privacy in criminal investigations and foreign intelligence policy debates, Diffie and Landau (2007) also find that privacy often loses to national security. However, they explain this as the result of the executive branch's powers to invade privacy in the name of national security (p. 169), which in some cases is resisted by commercial interests (pp. 236–248).

Solove's (2011) study of U.S. policymaking also finds a consistent pattern of privacy infringements in the name of national security, especially after the attacks of September 11, 2001. Like Diffie and Landau (2007), he acknowledges that this could be related to the executive branch's powers over foreign intelligence gathering (Solove, 2011, pp. 62–71) but also argues that it is largely due to the abstract nature of privacy interests, the consistent deference of legislatures and judges to security officials in times of crisis, and the consequent lack of meaningful evaluation of security measures (Solove, 2011, pp. 38–47, 55–62).

These studies reflect a pattern of expansions of national security at the expense of privacy. They all consider the technological context as a driver for policy change. Solove (2011) and Diffie and Landau (2007) also highlight how security crises have further harmed privacy in the name of national security after the 9/11 attacks. The studies, however, differ in their explanations of the causes for privacy harms. Whereas Regan (1995) addresses the inadequate framing of privacy as a public policy problem, Solove (2011) discusses the practice of deference to security officials and the lack of oversight over the executive branch as important sources of privacy harms. Diffie and Landau (2007) also highlight the influence of commercial companies which resisted privacy infringements on behalf of national security and insisted on strong encryption and privacy protections for their customers. Other scholars who study privacy and national

security in crime-related issues (Bevier, 1999; Dempsey, 1997; Gidari, 2006; Nylund, 2000; Soghoian, 2012) or in both the crime and foreign intelligence arenas (Birnhack & Elkin-Koren, 2003; Kleinig, Mameli, Miller, Salane, & Schqartz, 2011; Logan, 2009; Regan, 2004) also find detriments to privacy on behalf of national security, but they study a limited time frame and specific policy measures, and they do not provide additional explanations for the policy process.

Also, these studies do not address the plurality of dimensions in the relationships between privacy and national security, nor do they address government's multifaceted role in threatening but also enhancing privacy. Such complementary relations between privacy and national security are discussed in the information security policy literature. Scholars have highlighted the reluctance of the private sector to apply mandatory requirements (Chertoff, 2008; Etzioni, 2011; Hiller & Russel, 2013; Newman & Bach, 2004), the sectoral nature of these regulations (Regan, 2009; Schwartz & Janger, 2007; Thaw, 2014), and the ways in which policymakers' risk perceptions are constrained by private interests (Johnson, 2015; Quigley & Roy, 2012). Therefore, we can expect commercial interests to dominate the construction of these relations, while also aiming to understand when the information security policy arena introduces tensions with privacy.

In this article, these explanations are tested against variations in the balance between privacy and national security over time and across policy arenas. The literature's findings on the importance of policy framing, commercial interests, and the role of the executive branch are assessed, and I also show how technological developments and distinct characteristics of the policy process across policy arenas are essential factors in constructing the relations between privacy and national security.

Conceptual Clarifications: National Security and Privacy

The literature defines national security as the set of practices that protect the country from threats, which originate either in foreign states or within the nation's borders (Diffie & Landau, 2007; Reveron, Gvosdev, & Cloud, 2018; Romm, 1993; Solove, 2011). When the U.S. National Security Act of 1947 ushered the term into general use, it was often understood as protecting a country against internal subversion and external military attack. Since then, national security designations have been broadly and ambiguously used, while still referring to the nation rather than to individuals, subnations, or groups (Wolfers, 1952). Waldron (2006, pp. 459–460) defines national security as “collective security,” which is determined by the constraints individuals are willing to accept to secure the whole. Following the Cold War the term has been associated with nonmilitary threats (Romm, 1993),³ and in 2003, the frontier of national security was defined as “everywhere” (Zelikow, 2003). The concept can now relate to almost any security issue and is perceived as a form of severe crime (Solove, 2011, pp. 64–66).⁴

Diffie and Landau (2007, pp. 87–88) delineate five practices that characterize national security in the twenty-first century, and four of them are used here to

define national security practices as: procedures of intelligence gathering, foreign intelligence denial, enforcement of terrorism laws, and maintenance of national infrastructure.⁵ These national security practices are assessed in the paper in relation to privacy, for which there is no agreed-upon definition.⁶ Solove (2008, pp. 8–10) argues against searching for a single universal definition of privacy and asserts that privacy is a plural, context-dependent value that is best understood by studying practices that harm privacy. He provides two metaphors for privacy harms—the big brother state, which demonstrates how information collection creates new forms of social control, and the bureaucratic state, which disempowers individuals (Solove, 2011, pp. 25–26).⁷

Bygrave (2002) groups scholars' definitions of privacy into three categories. The first includes definitions of privacy in terms of noninterference in individuals' private space (Warren & Brandeis, 1890). The second includes definitions in terms of the levels of control and knowledge that individuals have over collections, processing, and other uses of their personal information (Fried, 1968; Laudon, 1996; Lessig, 1999; Rachels, 1975; Westin, 1967). The third understands privacy in terms of the values of autonomy, dignity, and self-determination as well as individuals' control over their own bodies, minds, and social relations (Benn, 1971; Fried, 1968; Gavison, 1980; Rachels, 1975; Reiman, 1976).

In this article, I adopt a working definition of privacy based on Bygrave's (2002) second and third groups, while embracing Solove's (2008) emphasis on defining privacy in terms of measures that infringe upon it. Privacy harms are therefore understood as actions that undermine individuals' autonomy, dignity, and self-determination by threatening their ability to control how their personal information is collected, accessed, and used, often without their knowledge.⁸ Such threats increase when privacy oversight and scrutiny procedures such as warrant requirements and minimization procedures for information collection are relaxed.

Following these definitions, the article examines how U.S. federal policies grant data subjects knowledge about and control over the collection of their personal information, and how they provide privacy protections in the national security practices of enforcement of terrorism laws, intelligence-gathering procedures, foreign intelligence denial, and the maintenance of vital national infrastructures.

Analytical Framework and Methodology

This article examines the U.S. federal regulatory regimes that govern: (i) information collection for criminal investigations; (ii) foreign intelligence gathering; and (iii) cybersecurity practices that protect vital information systems. These regimes evolved together with the expansion of digital technologies over the last five decades and construct plural types of relationships between privacy and national security.

The beginning of information collection oversight in criminal investigations can be identified as the Wiretap Act of 1968, which created a uniform procedure for domestic electronic surveillance and required investigators to obtain a warrant

based on a probable cause. Another inflection point in this regime was the 1986 Electronic Communications Privacy Act (ECPA). Since then, Congress has not reformed the regime, resulting in difficulties in applying privacy protections to new communication technologies. Moreover, an increasing number of criminal issues have become national security threats but are still governed by this regime.⁹

At the same time, a second regulatory regime for collecting personal information emerged with the enactment of the Foreign Intelligence Surveillance Act (FISA) of 1978, which regulated how intelligence services collect information on U.S. soil. The act followed the 1976 Church Committee's exposure of illegitimate government collections of personal information. Over time, new technologies and consistent attempts by the executive branch to expand its surveillance powers have challenged the regime's privacy protections.

The third regulatory regime under study, cybersecurity,¹⁰ involves policies that protect vital personal information networks, including those of the federal government and of health and financial service providers. The start of this regime can be pinpointed to the passage of the National Security Directive (NSD) #148 and the Comprehensive Crime Control Act of 1984, through which the government began sanctioning cyber-criminals and protecting federal networks. Most policies in this regime enhanced the protection of personal information in vital systems, but some introduced new threats to privacy.

To understand how and why public policies construct relationships between privacy and national security, I link laws and regulations enacted between 1968 and 2018 to these three regulatory regimes and study them through process-tracing and comparative analysis methods (Levi-Faur, 2006). The United States is an ideal case for studying privacy *vis-à-vis* national security in a liberal democracy, as policy records are complete and easily accessible. The study starts with 1968 because that is the year when regulation on information collection was initiated.

An original data set was created with policy events (N=63) from the years 1968–2018 that delineate the three regulatory regimes under study.¹¹ Each policy event is classified into one of three possible categories according to its effect on the relationships between privacy and national security. These categories include: (i) harming privacy for national security; (ii) creating a compromise between the two; or (iii) advancing complementary relationships that enhance both.

The effect of a policy event is assessed according to the policy's purpose and features. Policy purposes range from regulating the government's information collection to protecting the security and privacy of vital personal information systems. The former type of policy creates contradictory relations between privacy and national security, while the latter constructs complementary relations between the two goals. The features of each policy are also assessed to determine the extent of privacy oversight and scrutiny measures provided by policymakers to achieve the policy's purpose. Within contradictory dynamics, the focus on policy features allows to distinguish between policies that harm privacy for national security and policies that create a compromise between the two goals.

The first type of relationship, harming privacy for national security, is indicated by policies that regulate the government's information collection and relax oversight over privacy-harming components within these national security practices. For instance, the 2008 FISA Amendments Act (FAA), and specifically the newly added Section 702, authorized government surveillance over international communications without requiring the government to demonstrate probable cause that the surveillance targets are agents of a foreign power. This allowed the surveillance of Americans' international communications without any suspicion of wrongdoing. The act also limited the role of the judicial authority over surveillance authorizations of overseas targets. Rather than reviewing individualized surveillance applications, the judiciary was relegated to reviewing general targeting and minimization procedures for gathering international communications that can incidentally include U.S. citizens. In addition, the duration of warrantless surveillance was increased from 48 hours to seven days in case one of the parties to the communications is based overseas.

The second relationship, compromises between privacy and national security, is indicated by policies that regulate the government's information collection and incorporate privacy-protecting measures into these national security practices. For instance, the 1986 ECPA regulates information collection for criminal investigations. The statute requires government officials to justify their belief that the proposed surveillance will uncover evidence of a crime. It also requires investigators to minimize surveillance when innocents are involved and to explain why alternative investigation methods would not be effective. The subjects of surveillance are always informed at some point and are made aware in court about the data obtained. This policy allows the government to conduct surveillance but only through oversight and scrutiny mechanisms that limit privacy harms.

The third relationship, complementary, is denoted by policies aimed at protecting security and privacy in vital information systems in ways that carry no privacy-harming features. For instance, the 2002 Federal Information Security Management Act (FISMA) poses information security requirements on federal networks to increase the security of vital systems, shield against intelligence gathering by foreign states, and protect the personal information they process. This policy does not include privacy-harming components to achieve its purpose. While 25 out of 30 information security policies do not include privacy-harming features, five policies achieve their purpose through the creation of privacy infringements. In this case, such policies were classified according to their features rather than their purpose.¹² For instance, the 2015 Cyber Information Sharing Act (CISA) is aimed at increasing information security and privacy but achieves this goal through privacy-harming measures that authorize information collection without a court order and do not share with data subjects how information is accessed by the government. Therefore, such policies were classified as harming privacy for national security.

The methodological annex of this article provides additional details on the collection and classification of each policy measure in the data set (see the Appendix).

Analysis Over Time

Contradictory Relationships

The analysis of contradictory dynamics between privacy and national security included 38 policy events from 1968 to 2018. Twenty-one of the events reflected an expansion of national security at the expense of privacy, and 17 reflected a compromise between the goals.

First Period: 1968–89

Fifteen policy events were identified that constructed a compromise between the two goals, with several outliers. During this period, the three regulatory regimes under study were initiated. The Wiretap Act of 1968, which created privacy protections for information collected by criminal investigators, was the first information collection regulation enacted by Congress. It came one year after the Supreme Court ruled in *Katz v. United States* (1967) that the Fourth Amendment prohibits the government from using wiretapping without a warrant and probable cause (Regan, 1995, p. 122). It also required investigators to minimize collection, notify subjects once the gathering was concluded, and report the number of warrant applications to Congress, while providing that illegally obtained evidence cannot be used in court. Prior to this court ruling, Congress discussed numerous bills that would allow limited government wiretapping but was unable to pass such legislation (Regan, 1995, pp. 118–120).

Through the mid-1980s, new telecommunications technologies introduced new forms of information collection not addressed by the Wiretap Act. These included wireless phones and computer communications operated by new companies that did not have wiretapping agreements with the government. Several court rulings permitted the executive branch to use wiretaps without regulatory oversight (Regan, 1995, p. 130). Still, the Department of Justice (DOJ) was cautious in its use of new information collection technologies and wanted Congress to determine their regulatory status. In addition, industry and privacy advocates pushed for better privacy protections on new communication methods (Regan, 1995, pp. 133–134). Consequently, Congress amended the Wiretap Act by enacting the ECPA in 1986. The statute covered new communications methods¹³ and created a distinction between content, which is regulated by strict privacy protections, and metadata, which can be accessed with a judicial order instead of a warrant. Congress quickly passed the ECPA with industry's support. Following the Bell Systems breakup in 1982,¹⁴ businesses were eager to protect the privacy of their consumers and create alliances with civic groups to be competitive in the new market structure (Regan, 1995, pp. 135–136).

During the same period, Congress initiated a second regulatory regime for information collection. Through the 1978 FISA, Congress established privacy protections for foreign intelligence gathering for the first time, in the wake of scandals over government information collection on U.S. citizens. In 1972, the

Supreme Court unanimously ruled that the Fourth Amendment requires the government to use warrants when gathering foreign intelligence within U.S. borders,¹⁵ and urged Congress to provide regulations on the matter. Later, as public outcry over government surveillance peaked during the Watergate scandal,¹⁶ President Ford established the 1976 Church Committee to investigate government information collection practices.¹⁷ The committee determined that the government targeted some people solely because of their political beliefs, while justifying surveillance with national security concerns. It concluded that these actions undermined the democratic process and the government's duty to protect society.¹⁸

Presidents Ford and Carter responded with executive orders that prohibited the Central Intelligence Agency (CIA) and National Security Agency (NSA) from intercepting communications within the United States, unless approved by the attorney general. Congress responded with the 1978 enactment of FISA, which required that (i) the government obtain a warrant to conduct foreign intelligence gathering and (ii) Congress create a special judicial authority—FISA courts—to handle classified matters not previously considered under the law. FISA also includes reporting and minimization requirements on collected information. It created a regulatory separation of information collection for foreign intelligence and criminal investigations, also known as the “FISA wall.” This wall subjected criminal investigations to more rigorous rules and foreign intelligence gathering to laxer ones.¹⁹ Overall, FISA reflected a compromise between those who advocated for intelligence agencies' broad powers and those who advocated for privacy protections. Still, FISA did not address the president's authority to engage in surveillance outside U.S. borders.

In 1981, President Reagan addressed the issue in Executive Order (EO) #12333. He authorized the collection of information outside U.S. borders without congressional oversight or court warrants. While not considered harmful to privacy at the time, the order presents several harmful privacy implications today. John Tye, a former State Department official, revealed in 2014 that the order allowed intelligence agencies to incidentally collect U.S. citizens' communications, without proper oversight, for cases in which these communications are stored or routed outside U.S. jurisdictions.²⁰ The order also authorized the attorney general, rather than the courts, to approve minimization procedures in handling data.²¹

Another regulatory tool introduced in this period are National Security Letters (NSLs). These secret Federal Bureau of Investigation (FBI)-issued letters, meant to override privacy protections in emergency situations, required private sector companies to hand over certain data records. Over the years, however, this tool increasingly has been used to infringe upon privacy. The first authorization of NSLs took place through the 1978 Right to Financial Privacy Act (RFPA). The act was Congress's response to the Supreme Court's decision in *United States v. Miller* (1976), which ruled that bank records are not subject to constitutional privacy protections. According to the RFPA, the government must obtain a search warrant, subpoena, or formal written request reviewable in court to collect personal financial data. The act also established NSLs as a limited exception in the case of foreign intelligence emergencies (Nieland, 2007). During the 1980s,

telecommunications companies mostly led the resistance to the use of NSLs. The ECPA of 1986 limited the issuance of NSLs to the FBI director for acquiring metadata when the target is a foreign agent.

The third regulatory regime under study, cybersecurity, was also initiated during this period. President Reagan's 1984 NSD #145 granted the NSA responsibility over the information security of federal networks. The administration further extended this authority in a 1986 policy memo that expanded the NSA's jurisdiction to the entire federal government and related private sector networks.²² Congress, industry, and civil society expressed concerns about these developments; in response, Congress passed the 1987 Computer Security Act. The new statute assigned the information security of federal networks to the National Institute of Standards and Technology (NIST). In 1989, however, the NIST and NSA signed a memorandum of understanding that included the NSA in decision-making processes over federal networks' security.²³

Overall, policy events during this period created compromises between privacy and national security, with a few outliers. Privacy oversight mechanisms over national security practices were established, and Congress applied checks to the executive branch's power to collect personal information. The executive branch itself, however, reflected conflicting trends. While the Ford and Carter administrations limited privacy infringements, the Reagan administration expanded national security at the expense of privacy. During this period, the private sector also took an active role in advocating for consumers' privacy. Technology provided the context and driver for policymakers and judges to protect privacy against emerging threats. This status quo in privacy and national security relationships remained until 1993.²⁴

Second Period: 1993–2012

In the early 1990s, the DOJ expressed concerns about commercial sales of encrypted products and digital telephone switches (Diffie & Landau, 2007, pp. 205–206, 229–230). These technologies constrained the government's surveillance capabilities and marked the start of the second major period of expanding national security authorities at the expense of privacy.

In 1993, the government fought the use of encryption by imposing export controls on encrypted products and requiring breakable encryption standards for U.S. products through the Clipper Chip program.²⁵ AT&T started including it in their models, but by 1995, the Clipper Chip had become unpopular in the market and drew opposition from industry and civil society (Diffie & Landau, 2007, p. 240). Following public controversy over the program's constitutionality and technical difficulties in implementing the new encryption scheme,²⁶ an independent study by Congress recommended removing export limitations and implementing strong rather than breakable encryption standards in the market.²⁷ In 2000, seven years after the announcement of the Clipper Chip program, the export limitations were removed.

Another contested issue was the commercial use of digital telephone switches.²⁸ In 1994, Congress passed the 1994 Communications Assistance for

Law Enforcement Act (CALEA). The act ordered all telecommunications providers to produce “surveillance-friendly” infrastructures that would allow the government to silently participate in personal phone calls. Congress approved \$500 million to implement the act and allowed the use of subpoenas instead of search warrants to obtain telephone records. Despite disputes between industry and the FBI over privacy-intrusive implementation standards, the industry had to compromise and adopt most of the FBI’s requests. In 2006, under pressure from security agencies, the Federal Communications Commission (FCC) expanded the CALEA’s authority to include new methods of communication, like Voice-over-IP operators and Internet communications.²⁹

The 1990s also witnessed failed policy attempts to expand the legal authority over government information collection. Following the 1995 bombing of the Murrah Federal Office Building in Oklahoma City and the 1996 TWA flight explosion, the FBI and the Clinton administration pushed for expanded surveillance authorities, which Congress opposed.³⁰ It seems that the policy climate in the 1990s did not support the expansion of the government’s authority, beyond “adjustments” to the changing nature of communication technologies.³¹

In contrast, by the early 2000s, and especially after the 9/11 attacks, Congress broadly accepted the government’s expanded surveillance authorities. In 1998, the FISA was revised to allow surveillance on pen register and trap-and-trace devices,³² and to permit foreign intelligence investigations to access business records. A few weeks after 9/11, Congress passed the 2001 Patriot Act. In a tense and fearful atmosphere,³³ the act received little scrutiny in Congress or by the media, even though it incorporated provisions that Congress and the courts had previously rejected (Kerr, 2003, p. 637). The act amended almost every privacy statute,³⁴ including the 1986 ECPA, and allowed the government to collect new types of metadata like email headers, IP addresses, and URLs. Moreover, Section 218 of the act removed the “FISA wall” barrier for usages of collected information, which meant that criminal investigators could conduct surveillance under laxer privacy protections of the foreign intelligence regime (Solove, 2011, p. 74).

After 9/11, many argued that the crime/foreign intelligence distinction prevented critical information sharing between government agencies. Consequently, the Patriot Act’s expanded FISA authority had invoked this justification and permitted the government to rely on FISA protections in cases for which foreign intelligence gathering is only one of many goals.³⁵ Attorney General Ashcroft, in his 2002 guidelines, further eliminated the separation by allowing the government to apply loose privacy protections on domestic information collection.³⁶ These developments allowed the government to surveil citizens not suspected of wrongdoing, while the application of the secrecy characteristics of foreign intelligence practices to crime-mitigation efforts had eliminated the accountability of government agents (Solove, 2011, p. 77).

Section 215 of the Patriot Act also allowed the FBI to collect any tangible piece of information for foreign intelligence purposes as long as it did not directly relate to a U.S. citizen. Documents exposed by Edward Snowden revealed that since 2006, the NSA interpreted this section as permitting the direct bulk

collection of metadata from U.S. citizens' phone calls.³⁷ NSLs were addressed in the Patriot Act through Section 505, which amended the 1986 ECPA to relax restrictions on the type of data subject as well as the requirements for the FBI agent requesting a NSL.³⁸

Congress reauthorized the Patriot Act twice in the 2000s. In 2005, Congress amended Section 215 by limiting information collection to FISA court authorizations for which the government provides proof of relevance. In practice, however, the NSA broadly interpreted these court limitations to collect metadata from U.S. citizens' phone calls.³⁹ The reauthorization also prompted Congress to reach a compromise on the use of NSLs.⁴⁰ In 2011, Congress extended the act's sunset provisions without significant privacy limitations. The government could continue to use roving wiretaps and search for the business records of non-U.S. citizens without confirmed ties to terrorism.

The executive branch, however, was interested in additional information collection practices. Unsatisfied with the FISA's privacy barriers, the Bush administration secretly launched the President's Surveillance Program (PSP) from 2001 to 2007. This program allowed the NSA to conduct domestic surveillance without a FISA warrant or judicial oversight, possibly on U.S. citizens, if the domestic individual communicates with a foreign entity (Solove, 2011, p. 81). It circumvented existing regulations and created a new path for information collection on U.S. citizens.⁴¹

The program was never approved by Congress, but President Bush argued that the 2001 congressional resolution on the use of military force after 9/11 broadly authorized him to conduct surveillance without congressional approval (Solove, 2011, p. 83). Both the DOJ and FISA courts sided with the Bush administration. President Bush reauthorized the program and its classified status every 45 days without a court order and justified each reauthorization by citing a continued state of emergency. He said he would inform Congress about the nature of the program as soon as he ascertained that doing so would serve the national interest (Kleinig et al., 2011, p. 40).

The New York Times exposed these surveillance programs in 2005.⁴² In response, Attorney General Gonzales confirmed their existence and claimed that the government only conducted surveillance when it reasonably believed that at least one party to the communication was outside the United States and affiliated with a foreign agent. Whistleblower Mark Klein later refuted this claim and revealed that the NSA had full access to the communications of all AT&T subscribers based on the program.⁴³

In 2008, Congress passed the FAA and created Section 702 to authorize these surveillance programs. The section established separate procedures for targeting non-U.S. citizens outside the United States without a court order and gave the NSA the authority to acquire information on U.S. citizens that might be part of the gathered data.⁴⁴ This practice, also known as NSA's "about" collection, took place without proper privacy oversight and could be harmful to U.S. citizens' privacy.⁴⁵ The FAA also provided retroactive immunity to telecom companies that illegally collected information on behalf of the government between 2001 and

2007 (Solove, 2011, p. 89). In 2012, the FAA was reauthorized for an additional five years without any additional privacy protections. The statute authorized the NSA's PRISM program, which collects Internet communications from U.S. digital service providers such as Google and Yahoo and can unintentionally include the personal information of U.S. citizens.

Overall, the second period reflects the increasing harms of privacy on behalf of national security. The 14 policy events under analysis exhibited two temporal policy trends: (i) In the 1990s, the executive branch responded to technological developments that challenged the government's surveillance capabilities and (ii) in the 2000s, security crises allowed the expansion of the government's authority to collect information without oversight or scrutiny. During the 1990s–2000s, Congress's role shifted from providing a check against the expansion of the executive branch's surveillance authorities to deferring to security officials and supporting legislation that extended the government's surveillance authority. Fear after 9/11 was a decisive factor in Congress's retreat from oversight. The executive branch effectively used the sense of urgency to legitimize its expansion of surveillance authorities that undermined privacy. Technological developments also provided an important context for legislation that ultimately broadened surveillance authorities. Commercial interests in protecting privacy were also eroded during this time. In the 1990s, businesses effectively lobbied against limiting the exports of encryption technologies, opposed the Clipper Chip program, and fought against the FBI's implementation of the CALEA. But following the 9/11 attacks, commercial interests did not introduce privacy-related opposition to the expansion of national security authorities.

Third Period: 2013–18

After 20 years of significant harms to privacy for national security, the third period, with nine policy events, revealed conflicting trends of both harming privacy for national security and constructing compromises between the two goals. This period started in June 2013, with Edward Snowden's exposure of the U.S. government's wide-ranging surveillance practices. The disclosures led to public outcry, facilitated the formation of unlikely coalitions in Congress, and renewed technology companies' opposition to government surveillance (Wizner, 2017, p. 899). Although this period does not exhibit a clear trend toward one extreme or the other, prioritizations of privacy protections over national security during this period do suggest a reversal from a few decades of national security supremacy.

In 2014, President Obama published the Presidential Policy Directive (PPD) #28. It was the first time the White House published principles and protocols for foreign intelligence. The directive stated the importance of properly authorizing surveillance practices, required the minimization of information collected, and limited bulk collection practices in certain cases. It also protected the privacy of non-U.S. citizens, but with a long list of national security exceptions.⁴⁶ President Obama also called on Congress to declassify FISA Court decisions and appoint independent advisers for FISA Court cases.⁴⁷

In 2015, Congress passed the U.S. Freedom Act. This statute, enacted after the sunset of the Patriot Act's Section 2015, limited privacy-harming national security practices for the first time since 1978 by ending the direct bulk collection of phone call metadata.⁴⁸ It also required the appointment of external technical personnel to select FISA Courts, and publication of further rulings that set new surveillance authorization precedents. The Act required security agencies to be as specific as possible when issuing NSLs, noted that the disclosure of a letter request should not conclusively be treated as a danger to national security, and allowed these requests to be challenged in court.⁴⁹

Beyond legislation, intelligence agencies limited their own privacy-harming practices. In 2017, the Director of National Intelligence (DNI) published guidelines that restricted the CIA's collection of publicly available information. This was the first time restrictions on information collection were placed on the CIA since EO #12333 of 1981.⁵⁰ In the same year, the NSA announced it would stop conducting "about" searches of bulk communications data based on FISA Section 702, and would reduce the likelihood of surveillance of U.S. citizens based on identifiers caught in communications between foreign agents.⁵¹ In addition, the agency announced it would delete most information previously acquired through this practice.

During this period, the private sector also attempted to limit national security practices in court. In 2016, following a motion for assistance from the DOJ, Judge Sheri Pym of the United States District Court for the Central District of California ordered Apple to assist federal investigators in unlocking the phone of Syed Farook, who was responsible for the December 2015 San Bernardino shootings. Apple had judicially challenged the order, filing an appeal in district court. Breaking one phone, the company argued, could create a path to open hundreds of millions of other phones, undermining the privacy, and security, of digital infrastructures.⁵²

Another significant case of private sector resistance to government surveillance practices was *Microsoft Corp. v. United States* (2015), in which Microsoft refused to comply with a search warrant for emails on its servers located outside U.S. jurisdiction. Noting that cloud computing is not properly addressed in warrants based on the 1986 ECPA, the company argued that people's privacy should be protected by the laws of their own countries.⁵³ During Supreme Court hearings on the case, Congress passed the 2018 Clarifying Lawful Overseas Use of Data (CLOUD) Act and made the court dismiss the case. The act gained consensus by clarifying that a warrant issued under the 1986 ECPA applies to data overseas only if it does not violate the law of the country in which the data is hosted. It also required a review of how data is processed by foreign countries and ensured that governments only collect information on their own citizens overseas. Privacy advocates worried that the president could create "executive agreements" with other countries and easily obtain data on citizens located outside U.S. borders.⁵⁴

Despite the incorporation of privacy-protecting measures into national security policies, this period also witnessed a few policies that harm privacy for

national security. Despite a 2014 recommendation from the President's Review Group on Intelligence and Communication Technologies,⁵⁵ the White House declined to reform the 1981 EO #12333.⁵⁶ Currently, the order increases the likelihood of incidental collection of personal information on U.S. citizens who use global communication services and reside overseas. This incidental collection on U.S. citizens can take place without any evidence of wrongdoing and with no limits on the volume of information that can be collected. Additionally, in 2015, Congress passed the CISA, which incentivized companies to share their data with the government and created new avenues of nontransparent government information collection without a court order. Negotiations over the bill took place behind closed doors and did not include privacy actors.⁵⁷ The 2017 DNI guidelines for sharing counterterrorism information also infringed privacy,⁵⁸ as the guidelines allowed domestic security agencies to use information collected by the NSA with lax privacy protections and further eroded the "FISA wall."

Congress also legitimized privacy harms in this period through the 2018 bipartisan reauthorization of FISA Section 702 for six years. This section allows security agencies to collect information on non-U.S. persons located overseas. It also permits incidental collection on U.S. persons who were part of the content of communications gathered. Snowden revealed that Section 702 not only allows collection without a warrant, but also enables the government to search information based on identifiers of U.S. citizens.⁵⁹ The government recently argued that information collected under this section is governed by strict minimization and use rules.⁶⁰ Still, it defines national security crimes such as terrorism or cyber threats as exceptions. Privacy advocates viewed this reauthorization, despite a few new limitations, as permission for the intelligence community to conduct surveillance without a warrant, potentially on U.S. citizens.⁶¹

Overall, the privacy and national security trends in the third period were contradictory (see Table 1). Policy events indicate both privacy harms on behalf of national security and the construction of compromises between the two goals. Congress limited foreign intelligence practices for the first time since 1978 but also reauthorized FISA's Section 702 with mild limitations, making President Bush's 2001 unprecedented expansion of surveillance powers a mainstream national security practice. The executive branch also exhibited conflicting trends; it addressed foreign intelligence-gathering and called on Congress to increase checks and balances, while some of its intelligence agencies self-limited their data collection practices. At the same time, the executive branch increased its powers to collect information for cybersecurity purposes, published internal information sharing policies, and expressed reluctance to reform EO #12333. Commercial companies showed renewed resistance to government surveillance practices through courts, and initiated debates about the appropriate balance between privacy and national security. Technological changes were not as significant as in previous periods but did provide the context for policy debates between commercial companies and the government.

Table 1 summarizes trends in contradictory dynamics between privacy and national security over time. The roles of Congress, the executive branch, and commercial interests are highlighted, together with an assessment of how technology was used as a context in each period.

Table 1. Temporal Policy Trends of Privacy Versus National Security in the U.S. Federal Arena (1968–2018)

	Congress	The Executive Branch	Commercial Interests	Technological Context
Period I (1968-1989): Construction of Compromises	Applied checks on the executive branch following pro-privacy court rulings.	Different presidential administrations limited and expanded surveillance authorities.	Emerging policy influence and promotion of increased consumers' privacy protections.	Technology threatened privacy.
Period II (1993-2012): Harming Privacy through (1) Altering technology (1990s) & (2) Expanding legal authority (2000s)	Eroded ability to put checks on the executive in a fearful atmosphere.	Used national security crises and war powers to require deference to security officials and expand surveillance authorities.	Policy influence gradually eroded. Opposition waned after the 9/11 attacks.	Technology threatened surveillance capabilities and was used as a justification to expand surveillance authorities.
Period III (2013-2018): New privacy oversight mechanisms were established & additional privacy-harming policies were enacted.	Limited foreign intelligence practices for the first time since 1978, but also re-authorized expansions in surveillance powers.	Limited intelligence practices, but also expanded surveillance authorities.	Companies regained their pro-privacy policy role by challenging surveillance practices in courts.	Private companies rely on new technologies to justify opposition to surveillance authorities.

Complementary Relationships

The analysis of complementary dynamics between privacy and national security includes 25 policy events between 1974 and 2017 that protect vital personal information systems. Since the 1960s, federal officials warned that digital information was prone to unauthorized access (Warner, 2012, p. 786). Twenty years later, the protection of both federal and private sector industries became a major policy concern. When technologies like TCP/IP and Hyper-Text Transfer Protocol (HTTP)

boosted the usability of cyberspace and created a digital economy, commercial interests played a larger role in the policy process. But while federal networks were heavily regulated, there was a consistent lack of private sector information security requirements, even though the recent and increasing role of government agencies in the policy process has started to push back this trend.

Congress initiated the cybersecurity regime in 1984 when it criminalized computer property theft and the destruction of data.⁶² The executive branch first regulated U.S. government systems through the 1990 NSC Directive #42.⁶³ In 1996, government departments created the roles of Chief Information Officers (CIOs), who were assigned to oversee information technology (IT) purchases and integration.⁶⁴ When the Department of Homeland Security (DHS) was established in 2002, a new meta-regulator was created to oversee federal networks' protection. Additionally, the 2002 FISMA updated federal networks' mandatory protections. Every federal department had to conduct a risk-management plan, adopt NIST's standards, and faced fines for noncompliance. The act also established a federal incident center for risk mitigation and gave the Office of Management and Budget (OMB) responsibility for federal cybersecurity. Since then, the OMB has published breach notification requirements, expanded DHS authorities, and required the implementation of the secure Domain Name Services (DNSSEC) protocol in federal networks.⁶⁵

While federal networks were heavily regulated, the private sector faced few requirements. Congress's first unsuccessful attempt to regulate private corporations was the 1974 Privacy Act, which would have established a federal privacy protection agency. During the legislation process, private industries argued that there was little evidence of privacy harms in commercial information practices and that they were already overburdened by government regulations (Regan, 1995, pp. 77–79). The Clinton administration, whose "Framework for Global Electronic Commerce" (Clinton & Gore, 1997) described online businesses as essential to the growing economy, was also reluctant to limit business expansion by regulating their operations. The framework instead called for self-regulation and left privacy decisions to commercial companies. These early policy decisions set the stage for decades of lax private sector requirements.

Despite this hands-off approach, Congress passed the Health Insurance Portability and Accountability Act (HIPAA) in 1996, which set privacy and security standards for health records. Following private companies' concerns about the cost and complexity of the regulations, the act became a binding federal rule only in 2003. In 2009 and 2013, Congress amended HIPAA through the Health Information Technology for Economic and Clinical Health (HITECH) Act, which strengthened the Department of Health and Human Services' enforcement powers, increased the amount of liable entities, and created breach notification requirements.

The Gramm–Leach–Bliley Act (GLBA) of 1999, Sarbanes–Oxley (SOX) Act of 2002, and the Dodd–Frank Wall Street Reform and Consumer Protection Act of 2010 each instituted privacy and cybersecurity requirements for financial services providers. Section 501 of GLBA required financial institutions to protect the security and confidentiality of customers' personal financial information. Section 404 of the SOX act allowed the Securities and Exchange Commission (SEC) to

become a federal cybersecurity regulator of publicly traded companies. Since 2013, the SEC has published independent policies that strengthened its authority over cybersecurity. Additional legislation included Title X of the Dodd–Frank Wall Street Reform, which empowered the Consumer Financial Protection Bureau (CFPB) to become a cybersecurity auditor for the financial industry.

In 2010, the Department of Commerce readdressed the private sector; however, instead of instituting mandatory requirements, it issued voluntary guidelines.⁶⁶ Still, some policy events since 2013 reflected an increased independence of government agencies to issue private sector cybersecurity provisions. In 2013, the FCC issued voluntary recommendations to communication providers for mitigating cybersecurity risks,⁶⁷ and in 2016, it published a new rule that required Internet service providers (ISPs) to protect consumer security and privacy. However, the Trump administration has already reversed these mandatory guidelines.⁶⁸ The Federal Trade Commission (FTC) has also recently become more influential, especially after the third U.S. Circuit Court of Appeals in Philadelphia ruled in *FTC v. Wyndham Worldwide Corporation* (2015) that the FTC had the authority to enforce cybersecurity protections in the private sector.

Overall, policies that exhibit complementary relationships between privacy and national security were created in a limited number of sectors (see Table 2). While federal network security was high on the regulators' agenda, they did not impose mandatory requirements on private sector systems. Binding regulation was barely present outside of health and financial services, and companies relied on self-regulation models. Since the 1980s, government agencies have regulated federal networks' security and privacy through the creation of new departments and the assignment of new responsibilities for federal networks' security. In the 1990s, the increasing threat landscape created the need to more directly regulate health and financial service providers. Since 2011, however, a new policy trend

Table 2. Complementary Privacy and National Security Policy Dynamics in the U.S. Federal Arena (1974–2017)

	Congress	The Executive Branch	Commercial Interests	Technological Context
1974-2017 Policies focused on federal networks with limited protections for the private sector.	Created institutions and increased oversight over federal networks. Regulated health and financial services providers.	Since the 1980s, gradually increased role in protecting federal networks. Since 2011, government agencies increasingly gained independent authority to regulate privacy and security in the private sector.	Prevented Congress from passing binding privacy and security requirements on private sector's networks.	In the 1980s, technology introduced new threats that galvanized Congress and the executive branch to act. Recently, government agencies use it as a context for regulating the private sector.

has partially diverged from this equilibrium. The FCC, FTC, SEC, and CFPB all gradually became more independent and elevated their authority to regulate privacy and national security risks posed by private sector networks.

Following the analysis of privacy and national security over time, the next section addresses these policy events across policy arenas to highlight the influence of additional factors on policy outcomes.

Analysis Across Policy Arenas

In this section, the three regulatory regimes are analyzed across the different policy arenas, focusing on: (i) the contextual factors of policy changes; (ii) level of transparency in the policy process; (iii) variance of actors involved; and (iv) influence of commercial interests. Each policy arena can be seen to vary in its policy process, and consequently to construct different types of relationships between privacy and national security. This section highlights the main points for analysis of the policy process according to the criteria above. The list of policy events in each arena is included in the methodological annex (see the Appendix).

Information Collection for Criminal Investigations

Fourteen policy events were analyzed with regards to information collection for criminal investigations between the years of 1968 and 2018. Analysis of the policy context showed that the courts and technological developments were influential drivers of policy change. Courts pushed Congress to initiate the 1968 Wiretap Act (after several failed attempts) and the 1978 RFP, which introduced NSLs as an information collection practice in times of emergency. Meanwhile, technology was taken as grounds for policy debates over the 1968 Wiretap Act, 1986 ECPA, 1993 Clipper Chip, and 1994 CALEA. Challenges posed by new end-to-end encryption and cloud computing technologies were also central in the recent *Microsoft Corp. v. United States* (2015) and Apple's 2016 judicial challenge to assist the FBI in accessing one of its iPhone models. The context of security crises was a less influential driver of policy change. For example, FBI attempts to extend government authority over personal information following the 1995 Oklahoma shooting and 1996 TWA plane explosion did not pass Congress.

Also, in this arena, Congress consistently ensured transparency in privacy and national security policy discussions. It openly discussed the balance between the two during the 1968 Wiretap Act, 1986 ECPA, 1993 Clipper Chip Program, and 1994 CALEA policy debates. Even when the FBI demanded greater access to new technologies, especially during the 1993 Clipper Chip and 1994 CALEA debates, Congress facilitated an open deliberative process. This was also apparent during congressional hearings on Apple's dispute with the FBI and the enactment of the 2018 Cloud Act following Microsoft's opposition to comply with the government's request to access information on commercial servers.

The policy events also reflected high levels of actor variance. Security agencies, Congress, industry, and civil society all participated in the policy

processes of the 1968 Wiretap Act, 1986 ECPA, 1993 Clipper Chip, and 1994 CALEA. Still, despite the involvement of representatives from many sectors in the policy process, consensus was rarely reached, and significant compromises took place. For instance, in the policy debates leading to the enactment of the 1968 Wiretap Act, privacy advocates were reluctant to support a bill that authorizes wiretapping of U.S. citizens' communications but realized that a total ban on wiretapping was unlikely and wanted to influence the policy process. Security agencies, on the other hand, opposed placing any restrictions or extra burdens on wiretapping efforts in the fight against organized crime. During the policy process, the goal of all parties was to allow wiretapping with careful judgment (Regan, 1995, p. 125). The parties had to agree upon the list of crimes appropriate for wiretapping and discuss the type of authorization needed from either a court or the attorney general. Eventually, privacy advocates and security agencies were able to find a middle ground and reached a compromise for the terms of authorized wiretapping, with the requirement of annual reporting by security agencies to Congress on federal and state wiretapping court orders.

Another example of the compromises that took place was in the policy debates before the enactment of the 1986 ECPA. This was an extraordinary case in which consensus was reached within two years by the parties involved. All parties wanted to clarify the legal procedures over wiretapping new methods of communications: Industry wanted to ensure the privacy of customers and increase market competitiveness, security agencies wanted to clarify the legal statutes of collected information from new forms of communications, and privacy advocates were interested in expanding privacy protections to new methods of communication. Each party had its interests to push for a new wiretapping legislation. Specifically, the DOJ was cautious and did not want to lose evidence gained without a warrant according to the Wiretap Act. Further, civil groups headed by the American Civil Liberties Union (ACLU) formed a coalition to come up with a policy proposal in order to ensure privacy protections for new forms of digital communications, protect the content of communications, and pose privacy requirements on communications transmitted over networks not solely operated by common carriers. At the same time, the Office of Technology Assessment (OTA) studied the issue, bringing together privacy advocates, technology experts, business leaders, and the DOJ. Industry was supportive as well and did not raise significant opposition, even though the proposed bill influenced many telecommunications market segments. In order to sell their products and services, telecom manufacturers and providers wanted to ensure the privacy and security of their customers' communications. The OTA report became the baseline for all policy discussions in Congress, and all parties were able to agree on the problems and gaps in the 1968 Wiretap Act that needed to be addressed. Before the passage of the bill, the DOJ was reluctant to change the well-understood structure of the Wiretap Act and hesitated to impose additional burdens on law enforcement agents. The department insisted that emails and computer transmissions over wires would be covered by a new statute, but eventually had to compromise, as the passed

bill included these forms of communications as well. Despite this compromise, the DOJ was able to get its advocated changes, which included expanding the list of felonies for which a wiretap order may be issued, an increase in the number of DOJ officials who may apply for a court order, and the authorization to wiretap unspecified phones in case the surveillance target is changing phones.

In an additional example, during the 1993 Clipper Chip program's implementation, security agencies, and the Clinton administration had to compromise, despite their willingness to impose a new breakable encryption standard on the market. Initially, the White House approved, without congressional authorization, a new encryption standard that allowed the government to access encrypted communications and imposed export controls to prevent the spreading of strong encryption standards. Privacy advocates and technology activists, who were worried that the government could easily wiretap encrypted personal communications, opposed the government's aggressive attempts to impose a particular technology on the entire market. A few congressional officials stated that they would not authorize funding for the program. The telecommunications industry, other than AT&T, also opposed these efforts, claiming that export controls would cripple their ability to compete, and they could lose sales to foreign competitors. On the other hand, the government promised AT&T that it would buy massive amounts of the company's products with the Clipper Chip installed. Clipper Chip defenders argued that the scheme was voluntary and prevented communications from being immune to lawful interception. Terrorist threats moved the Clinton administration to act and approve the Clipper Chip scheme, as the government viewed the crypto-revolution with alarm and wanted to contain it. NIST responded to industry and privacy advocates' objections by claiming that the Clipper Chip standard was voluntary, decryption would occur only when legally authorized, there were no known trapdoors in the secret algorithm, and the adoption of the Clipper Chip program would make stronger encryption available. Despite the aggressive push by the administration and security agencies, the Clipper Chip did not gain momentum in the market. In response, Congress called for an independent study on national encryption policy by a panel of experts from government, industry, and academia under the supervision of the National Research Council. The panel recommended the strong use of cryptography by the market and for an immediate loosening of export-control regulations. The panel also observed that the Clipper Chip was a new technology that came with potential flaws and urged the U.S. government to experiment with the technique rather than aggressively promoting it. They claimed that the United States would be better off with widespread use of cryptography than without it. Eventually, despite consistent promotion by the administration and security agencies, opposition by industry, and privacy advocates led to the removal of export controls and the lack of adoption of the proposed government encryption standard by the market.

In another example, the implementation processes of the 1994 CALEA, it was the industry that had to compromise according to the interests of security agencies. The background to the bill was FBI claims that the new technology of digital phone switches was impeding its wiretapping ability. The head of the FBI, Louis Freeh, provided the House and Senate Judiciary Subcommittees details of 183 instances in which the FBI had encountered difficulties in conducting court-authorized interceptions. The pressure was fruitful, and Congress enacted CALEA, requiring telecommunications networks to deploy new “surveillance-friendly” communication standards by January 1, 1995. The attorney general decided that the FBI would be responsible for determining the level of surveillance standards that telephone companies would have to meet, and the FBI required a capacity to wiretap approximately 30,000 lines simultaneously. The statute, however, required that the industry, rather than government, would be responsible for designing the new system according to the FBI’s needs (Diffie & Landau, 2007, pp. 220–222). The FBI and industry had disputes over the requirement to enable law enforcement agencies to determine the precise location of a wireless user.⁶⁹ The Cellular Telecommunication Industry Association opposed turning all wireless phones into location beacons and argued that it was against the wording of the legislation. The FBI agreed to redraft its purposed cellular standards, and the industry later agreed to include location information in collected telephone data from other devices. Still, the FBI wanted to add even more privacy-intrusive requirements, including multiparty monitoring on participants who had already left the call and the adoption of a vast definition of “call-identifying information” that could be collected, overriding metadata collection limitations set by the 1986 ECPA (Diffie & Landau, 2007, pp. 220–222). These additional requirements tipped off a dispute between industry and the DOJ. As the October 1998 deadline approached, the FBI threatened to fine any company that would not adopt its interpretation of the new law. To settle the dispute, the FCC reported in 1999 that most FBI requirements to include telephone calls’ contents, location information, and metadata were covered by the new industry standard (Gidari & Coie, 2006). Overall, industry had to make significant compromises and implement FBI requirements in digital phone products despite privacy concerns. Without a clear business interest for telecom companies against CALEA, privacy interests lost to the security agencies’ increased appetite for personal information.

Commercial industry and business leaders influenced significant policy events in this arena. They supported privacy protections to satisfy their customers during the 1986 ECPA policy debates and were significant in pushing this wide-reaching legislation so quickly in the legislative process. They also successfully blocked the administration’s Clipper Chip initiative and removed export controls of encrypted products to allow better terms of market competition with foreign competitors; they were similarly influential, albeit less effective, in designing and implementing CALEA’s standards despite disputes with the FBI. Overall, the role of commercial interests in the 1980s and 1990s in this arena was significant given the support of

telecommunications companies in promoting the privacy of their costumers from a business perspective. They also wanted to compete with foreign telecommunication companies and remove barriers to sell encrypted products, despite the interests of security agencies. The resistance of commercial companies to government surveillance became relevant again in this arena after the 2013 Snowden revelations. But this time, the resistance came from software and hardware companies rather than telecommunication companies. New technological contexts led Microsoft, in the *Microsoft Corp. v. United States* (2015) case, and Apple, in its refusal to assist the FBI (2016), to resist government surveillance in order to ensure the privacy of their customers. It is important to note that other global service providers like Google and Facebook, which base their business models on the processing of personal information, did not pose significant opposition to government's surveillance practices. Apple and Microsoft, which do not rely on the personal information of their customers for revenue, became privacy champions in order to promote their commercial interests.

Overall, events in this arena constructed different compromises between privacy and national security. These relationships result from political patterns that: (i) allow an increasing number of policy actors to be part of policy processes that affect privacy and national security; (ii) enable transparency and public debates over privacy and national security issues in Congress; and (iii) are influenced by commercial interests that push for consumers' privacy protections when they converge with their business interests.

Foreign Intelligence

Nineteen foreign intelligence policy events between the years of 1978–2018 were analyzed. They exhibit mostly stable trends in the privacy/national security relationship. The initial balance set in the 1970s skewed toward national security after the 9/11 attacks, and then to some extent has been pushed back since 2015. Privacy scandals and security crises drove policy change. For example, the establishment of the 1976 Church Committee arose from controversies over government collection of U.S. citizens' personal information. Meanwhile, security crises led Congress to prioritize national security over privacy. During this time, Congress (i) amended FISA in 1998; (ii) launched PSPs and passed the 2001 Patriot Act following the 9/11 attacks; and (iii) passed the 2008 and 2012 FAAs to legitimize surveillance that can incidentally include personal information on U.S. citizens with minimal privacy protections. In 2013, new privacy scandals around the Snowden revelations led Congress to pass the 2015 U.S. Freedom Act, limiting foreign intelligence practices for the first time since 1978.

Technology served as a justification both for better privacy protections, as stated by the 1976 Church Committee, and for increased government surveillance capabilities, as reflected in the 2001 Patriot Act. Policy processes

in this arena were less transparent than those in the previous arena analyzed. While Congress set a framework for information collection by security agencies, the executive branch secretly deviated from these policies in such instances as the 2001 Bush administration's expansion of its surveillance authorities. This and other privacy-harming practices only became known to the public after such whistleblowing acts as John Tye's 2014 revelations about the use of 1981 EO #12333 to collect the content of communications overseas, the 2005 *New York Times*' exposure of the unlawful PSP, and the 2013 Snowden revelations about the NSA's metadata and "about" collection practices.

Actor variance in this arena was limited as well. Aside from two outliers in the 1978 FISA and 2015 U.S. Freedom Act, privacy advocates and business leaders were excluded from the policy process. The 1981 EO #12333, 2002 Attorney General Ashcroft Guidelines, 2001–2007 PSPs, 2008 FAA, and 2017 DNI guidelines on information sharing were all privacy breaches that the executive branch mandated in the name of national security, and only partially required congressional authorization. Still, Congress provided some privacy protections in its reauthorizations of FAA and the Patriot Act. Commercial influence on these policy processes was also limited, as businesses did not publicly oppose foreign intelligence gathering. Even though whistleblowers exposed NSA collaborations with private companies,⁷⁰ the policies under analysis do not indicate either convergence or divergence of interests between commercial actors and the intelligence community.

Overall, the analysis revealed a clear preference for national security over privacy. With low actor variance and a high level of secrecy, the executive branch dominated the agenda and aggressively pushed for greater surveillance powers. Security crises provided legitimacy for an expansion of national security authorities, and Congress did not successfully provide checks on the executive branch's surveillance powers. In contrast, privacy scandals following the 1976 Church Committee and 2013 Edward Snowden revelations enabled Congress to produce rare privacy protections through legislation. In the period of 30 years of foreign intelligence gathering policies, this arena was influenced by pro-privacy interests only twice (in 1978 and 2015) and only after significant privacy scandals.

Cybersecurity

Thirty cybersecurity policy events between the years of 1974–2016 were analyzed, finding that the context for policy change has shifted over the years. The rapidly evolving threat landscape in the 1980s framed cybersecurity as a national security issue and laid the groundwork for sanctions on hackers and regulation of federal networks (Dunn Cavelty, 2008, p. 44). In the 1990s, the government tried to respond to new threats by creating CIOs in each federal department and establishing DHS as the meta-regulator for U.S. cybersecurity. The expansion in telecommunications technology in the 1990s increased online

commerce and information processing, but also increased the scope of vulnerabilities beyond federal networks. In response, the government enacted policies to protect health and financial service providers, but did not extend its reach to other private sectors.

Since most cybersecurity policies were uncontroversial, transparency in the process was high. But a few policies created tension between privacy and national security, and reflected limited transparency. President Reagan's 1984 authorization of the NSA to protect federal networks contradicted the 1965 Brooks Act and was later expanded by a 1986 internal policy memorandum without congressional approval (Dunn Cavelty, 2008, p. 50). Congress pushed back against executive branch policies in the 1987 Computer Security Act, which provided oversight mechanisms and re-assigned NIST as the responsible authority. But the executive branch, through a 1989 memorandum of understanding between NSA and NIST, regained influence and increased secrecy in the process of protecting information systems (Dunn Cavelty, 2008, p. 51). The legislative process over 2015 CISA also lacked transparency, as negotiations over the bill took place behind closed doors and the final draft was released two days before voting, preventing any meaningful scrutiny.⁷¹

The variance of policy actors in this arena was high and included Congress, the executive branch, and industry. Privacy advocates tried to intervene in policies that infringed privacy, but their influence was limited. For instance, the FTC played no role in the 2015 CISA policy process, despite the bill's privacy implications. Since 2010, Congress has been less involved, while the SEC, CFPB, FCC, and FTC increasingly initiated information security and privacy policies within their jurisdictions.




Commercial interests had a significant influence on these policy processes. Congress struggled with imposing mandatory requirements on the private sector, from the early debates over the 1974 Privacy Act to its failed attempts to pass a federal breach notification law during the 2000s.⁷² Commercial interests consistently pushed for bottom-up regulatory models⁷³ and relied on the "hands-off" policy approach taken by Congress and the executive branch since the 1974 Privacy Act, the Clinton administration's 1997 Global Electronic Commerce Framework, and Department of Commerce's 2010 voluntary guidelines. Another sign of commercial influence was the successful passage of an information-sharing bill (CISA) after 15 years of failed legislative processes,⁷⁴ and only after liability waivers were introduced to incentivize the support of private companies.

Overall, the 30 policy events studied here reflected complementary relationships between national security and privacy in the federal, health, and financial sectors, with a few outliers that created tension between the two goals. The rapidly evolving threat landscape drove Congress to extend the reach of information security regulations, and elicited pushback from influential private interests. Most policy events were transparent and demonstrated an increasing presence of government agencies. Still, the few policies that created tension

between privacy and national security usually lacked privacy scrutiny and involved a limited number of actors.

Table 3 summarizes privacy and national security trends across policy arenas through the assessment of context, transparency, variance of actors involved, and influence of commercial interests on the policy process.

Table 3. The Construction of Privacy *vis-à-vis* National Security Across Federal Policy Arenas Over Time (1968–2018)

	Contextual Factors	Transparency in Policy Process	Actor Variance	Commercial Interests
Criminal Investigations:  Most events construct compromises.	Technological changes and court rulings pushed Congress and technology companies to resist surveillance practices. Times of crises are usually not effective drivers.	Polymaking and implementation processes were transparent and openly facilitated by Congress.	High variance of actors involved in the policy process – executive branch, Congress, industry and civil society.	Shaped compromises and blocked the executive branch's attempts to alter technology.
Foreign Intelligence:  Rarely punctuated policy equilibrium of harming privacy for national security.	Privacy scandals and national security crises led to policy changes. Technology was used according to the political climate.	Limited transparency in executive branch decisions. Society exclusively relied on whistleblowers to expose executive's deviations from policy frameworks.	Limited variance. Beyond two outliers, businesses and civil society groups were not part of the process. Executive branch circumvented Congress in a few cases.	Limited influence on the policy process.
Cybersecurity:  Complementary, with a few outliers.	The rapidly evolving threat landscape and the complexity of risks pushed the government to defend federal and a few private sector networks.	Usually high, except for cases when policies reflected tensions between privacy and national security. Then, Congress was less involved, secrecy was high, and scrutiny was limited.	Usually high. Congress, the executive Branch, and industry were represented. When privacy actors were involved, their influence was limited. Recently, government agencies promoted policies without Congress.	Significant. Businesses preserved the absence of binding private sector regulations and influenced policies that did pass.

Conclusion

This article finds that U.S. federal decision making over privacy and national security comprises a patchwork of laws and regulations that change over time and across three policy arenas. Overall, the analysis confirms and further elaborates on hypotheses from the literature—finding that privacy often loses to national security in the policy process (Diffie & Landau, 2007; Regan, 1995; Solove, 2011). This is not only reflected quantitatively (out of 38 policies of contradictory dynamics, 21 harmed privacy for national security), but also qualitatively, setting unprecedented expansions in surveillance authorities. Once a privacy-harming policy is introduced, it is unlikely to be fully remedied. For instance, the erosion of the “FISA Wall” by the 2001 Patriot Act and the authority provided by FISA Section 702 to conduct surveillance without a warrant have never been fully reversed.

The analysis also finds that technology is a significant factor for policy change (Diffie & Landau, 2007; Regan, 1995). It is instrumentally used by privacy advocates, security officials, and commercial companies according to the political climate of the time, and can be a source of privacy protections (in the 1970s and 1980s) or harms (in the 2000s). Additionally, the framing of issues was crucial for determining the balance between privacy and national security (Regan, 1995). This policy framing is changing across policy arenas and mediates political patterns that vary on the levels of transparency, variance of actors, and influence of commercial interests, leading to the construction of different types of relationships between privacy and national security.

The academic literature also shows that lawmakers coupled national security policy debates with security crises in order to legitimize the actions of the executive branch. For example, after 9/11, this tendency prevented meaningful evaluations of security measures and encouraged deference to security officials (Solove, 2011). The study reported here, however, finds that this trend varied across time and context. Security crises in the 1990s did not create meaningful privacy harms. In addition, privacy scandals have led to a pushback against surveillance practices and served as a driving context for policy change as well.

Another important finding is that since the 1980s, businesses contributed to the opposition to privacy harms (Diffie & Landau, 2007), but in changing degrees across different periods. Moreover, businesses also resisted information security and privacy regulations on their operations, leaving the public exposed to national security and privacy threats from criminals and foreign states. The ability of the government to effectively regulate cybersecurity is indeed questionable, but the strong private lobby in Congress prevented the establishment of a federal privacy regulator in 1974, fought attempts to pass a federal breach notification rule in the 2000s, and ensured that the public would rely on companies’ judgment and ability to protect against privacy and national security threats.

By considering the full spectrum of policy relationships between privacy and national security, this study provides a better-rounded picture of the factors that drive change and the ways the goals are balanced. Government can be a source of both problems and solutions for citizens’ privacy. Meanwhile, the increasing

influence of independent government agencies in promoting security and privacy in private sector networks has come into conflict with traditional commercial influence on these policy processes. This is a key power struggle to follow in the future, as it could potentially diverge from the existing policy path in this arena. Moreover, convergence of interests between commercial companies and intelligence agencies is revealed across arenas, as both parties push for lax privacy protections in the foreign intelligence and the cybersecurity policy arenas.

Tracing the roles of Congress and businesses over time also reveals an alarming pattern. While both actors influenced the facilitation of a transparent policy process and pushed back against the executive branch's attempts to expand surveillance in the 1980s and 1990s, they were considerably less effective following the 9/11 attacks. Instead of holding the executive branch accountable, Congress provided supportive legislation and passed measures without meaningful debates. Furthermore, after 9/11, commercial interests were excluded from policy processes, despite their influence in previous decades. The political climate and policy course only changed after whistleblowers revealed executive branch abuses of power throughout the 2000s. This happened four decades after the 1976 Church Committee exposed similarly severe and systematic abuses.

Despite a broad empirical approach, this research still does not consider all relevant policy arenas for the study of privacy and national security policies. U.S. states, which fill the federal vacuum in private sector privacy and cybersecurity regulations, may have also influenced these relationships. Moreover, further study of failed federal legislation attempts could reveal more nuanced trends in the privacy and national security policy balance. Future research might also conduct an in-depth study of just one policy arena and explain drivers for policy change in comparison to other nations.

In this article, I have asked how and why privacy is governed *vis-à-vis* national security and found that there is no single equilibrium between the two goals. Rather, they are mediated by a plurality of contexts, interests, and policy arenas. This complexity stresses the importance of understanding what shapes these governance systems. Solove (2011, p. 30) argues that privacy is rarely lost at once, but rather eroded over time. An overall erosion of privacy over time is indeed revealed by this study, but there are multiple policy trends to follow, which are shaped by different actors and policy processes. To better understand the balance between privacy and national security, we need to assess the context of power relationships between Congress, the executive branch, and commercial interests, and pay close attention to the types of policy processes mediated by these actors and the different levels of transparency and variance of actors they allow in the policy process. As digital technologies increasingly shape our lives, understanding how and why these governance systems operate will be essential to the liberal nature of society.

Ido Sivan-Sevilla, M.A., Ph.D. Candidate, The Federmann School of Public Policy and Government, The Hebrew University of Jerusalem, Mount Scopus, Jerusalem, Israel [ido.sivan@mail.huji.ac.il].

Notes

1. Such vulnerabilities include “back doors” that make infrastructures less secure and more easily accessible to government information collection (e.g., by decreasing encryption standards). Technologists and civil libertarians argue that the technology does not differentiate between government officials and criminal actors, and this introduction of back doors makes infrastructures more vulnerable to hackers, and thus, less secure and less private. See https://www.schneier.com/blog/archives/2016/02/the_importance_.html.
2. Progress in computer processing, networking, and storage capacities removed most technical barriers to surveillance. Instead of hand-picking their surveillance targets, governments can easily spy on large portions of the population on a regular basis. Beyond searching homes, people, and papers, governments now use technology to gather vast amounts of data, engage in audio, video, and Internet surveillance, and track the movements of the public. Additionally, inexpensive techniques for storing and processing personal information allow the government to create profiles of citizens. By integrating distinct pieces of information, government can reveal one’s intimate habits, interests, concerns, and passions (Granick, 2017, pp. 9–27; Solove, 2011, pp. 22–24).
3. In the 2015 U.S. National Security Strategy, the variety of nonmilitary “national security” issues reflected this perception, and includes financial stability, energy supply, environmental threats, food safety, terrorism, global health, and cybersecurity. See <http://nssarchive.us/wp-content/uploads/2015/02/2015.pdf>.
4. Solove (2011, p. 66) distinguishes between national security issues and other criminal acts based on the number of victims, which is usually higher in national security events, or by the means of the attack, which tend to be more lethal and deadly in national security attacks. However, he acknowledges that these categories are flawed. If one attempts to murder the president, it is still a national security incident, despite the low number of victims. He also does not classify an incident in which a man flew a plane into an IRS building because he objected to income tax as a national security issue, despite the use of an airplane as a means of attack.
5. I find Diffie and Landau’s (2007) suggested national security practice of maintenance of military forces less relevant for the study of the federal policy relationships between national security and privacy.
6. Notable studies include: Westin (1967), Jarvis (1975), Bevier (1989), Bennett (1992), Innes (1992), Regan (1995), Moore (2003), Lindsay (2005), Solove (2008), Nissenbaum (2010), Raab (2014), and Hughes (2015).
7. The first metaphor is based on George Orwell’s book *1984* (1949), in which a totalitarian government controls its citizens through constant surveillance. This metaphor emphasizes the privacy harms inflicted by techniques of social control. Solove (2011) argues that much of the data gathered by governments is not sensitive (e.g., birth dates, gender, address) and therefore would not embarrass people or create chilling effects on their behaviors. He also presents the bureaucracy described in Franz Kafka’s *The Trial* (1925) as another metaphor of privacy infringement. The protagonist of the book is arrested but not informed why. Kafka describes a bureaucracy that uses people’s information to make important decisions about them, but denies the people any knowledge of or participation in how their information is used. It shows that information processing, in addition to information collection, disempowers individuals, and creates intransigent structures between state institutions and citizens.
8. Since this article focuses on how privacy is managed *vis-à-vis* national security practices of information collection, I do not include Warren and Brandeis’ (1890) spatial definitions of privacy.
9. For example, cyber-crimes, financial frauds, and crimes linked to terrorism.
10. By definition, cybersecurity is meant to make the digital information and network eco-system safer. It refers to a set of technical and nontechnical activities and measures that protect the components of cyberspace—hardware, software, and the information they contain—from threats (Dunn Cavelty, 2010). The goals of a cybersecurity regulatory regime are threefold: to ensure the confidentiality, integrity, and availability of information in cyberspace (Dhillon, 2006). Confidentiality protects information from being disclosed to unauthorized actors, integrity prevents information from being changed by unauthorized actors, and availability enables authorized parties to access the information upon request.
11. These “policy events” include: federal statutes, executive orders, presidential orders and directives, national security directives, federal register rules, court rulings, and policy guidelines that provide additional interpretation to federal statutes.

12. In these five cases of conflict between policy purpose and features, the decision was taken to classify them according to features since the privacy-harming features of these policies are greater than the privacy protections they aim to provide. These features infringe privacy in the face of government's information collection, and this threat to privacy can therefore be viewed as a more significant privacy implication in comparison to the privacy protection these policies aim to provide against external threats. These policies include 1984 NSD #145, 1986 National Telecommunications and Information Systems Security Policy (NTISSP) No. 2 policy memo, 1987 Computer Security Act, 1989 NIST and NSA Memorandum of Understanding, and 2015 CISA.
13. These new methods include: wireless voice communications, stored electronic communications, and recording devices for outgoing dialed numbers.
14. This was an antitrust decision that split the Bell System monopoly into separate and regional companies. AT&T would continue to provide long-distance service, while several new "Regional Bell Operating Companies" would provide local service that would no longer be directly supplied by AT&T.
15. In *United States v. U.S. District Court* (1972), the court considered the legality of an attorney general's authority to permit electronic surveillance without a warrant of a U.S. citizen accused of bombing a CIA building.
16. The Watergate scandal began in 1972, when five burglars who worked on behalf of President Nixon broke in to the Democratic National Committee headquarters and bugged the phone of Democratic Party Chairman Lawrence O'Brien. Nixon's impeachment committee deemed this a misuse of presidential power that attempted to affect the elections (Diffie & Landau, 2007, pp. 199–200).
17. The Committee revealed that the FBI and CIA followed secret presidential orders, from Roosevelt's to Nixon's administrations, to illegally accumulate information on more than 400,000 people, including Members of Congress (The President's Review Group on Intelligence and Communications Technologies, 2014).
18. The Committee further cautioned that in an era of increased technological capabilities, secrecy is a threat to liberty (Church Committee 94th U.S. Congress Report, Book III, 1976, p. 65). See https://www.intelligence.senate.gov/sites/default/files/94755_III.pdf.
19. According to 1986 ECPA, agents need to justify the belief that surveillance will turn up evidence of a crime and are required to explain why alternative investigation methods would not be effective. The act also requires transparency and notification to data subjects. In contrast, the 1978 FISA allows secrecy and longer periods of surveillance on individuals without notice.
20. *The Washington Post* revealed in October 2013 that EO #12333 allowed the NSA to collect information in transition between Google and Yahoo! data centers outside the United States. See https://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html.
21. The collected data, according to Tye, included information on every person using popular services like Gmail, Yahoo!, and Dropbox. The EO does not require the NSA to notify or obtain consent from a private company before collecting its users' data. See https://www.washingtonpost.com/opinions/meet-executive-order-12333-the-reagan-rule-that-lets-the-nsa-spy-on-americans/2014/07/18/93d2ac22-0b93-11e4-b8e5-d0de80767fc2_story.html.
22. The 1986 NTISSP No. 2 is viewed by Dunn Caveltty (2008, p. 50) as a significant extension of the NSA's authority over information security in the public and private sectors.
23. The NIST and NSA's memorandum of understanding from 1989 is available at https://csrc.nist.gov/CSRC/media/Projects/Crypto-Standards-Development-Process/documents/NIST_NSA_MOU-1989.pdf.
24. Even though the tension between national security and privacy was less on the agenda of federal policymakers between 1989 and 1993, privacy was still an important policy objective in those years. With the emergence of digital databases, policymakers focused on regulating the ability of government agencies to build personal profiles of citizens. By that time, federal government agencies had 910 major databases containing personal data (Diffie & Landau, 2007). In 1988, Congress passed the Computer Matching and Privacy Protection Act to safeguard privacy in light of matching practices between different governmental databases for the building of profiles of individual citizens to increase government's efficiency.
25. The NSA tried to make NIST dictate this vulnerable encryption standard on all telecommunications instead of only "telephone communications," but failed to do so after strong NIST opposition (Diffie & Landau, 2007, p. 238).
26. For more on the public outcry over Clipper Chip, see <https://www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html>.

27. More conclusions of this study are detailed in the Committee's 1996 report at <https://www.nap.edu/catalog/5131/cryptographys-role-in-securing-the-information-society>.
28. New phone systems made it harder for FBI agents to conduct surveillance from multiple sources, trace the caller information, follow the numbers that were dialed, and monitor call forwarding techniques (Diffie & Landau 2007, pp. 205–206).
29. For more on this expansion, see the report from the Congressional Research Service (CRS) by Patricia Moloney Figliola (2007), "Digital Surveillance: The Communications Assistance for Law Enforcement" at <https://fas.org/sgp/crs/intel/RL30677.pdf>.
30. In 1995, the head of the FBI, Louis Freeh, with the support of the White House, proposed new legislation that would permit law enforcement agents to obtain roving wiretap permission, expand the list of crimes that require a wiretap order, and use illegally obtained information in court. Congress turned down all the proposals. Another example took place after the TWA flight explosion in 1996. President Clinton suggested that terrorist actions should be included among the list of crimes governed by ECPA. Clinton also recommended more liberal provisions for roving wiretaps, 48-hour emergency warrantless wiretapping, and the profiling of airline passengers through electronic records. Yet again, all these proposals did not pass Congress (Diffie & Landau, 2007, pp. 223–224).
31. One exception to that was the mild expansion of the use of NSL. In 1993, Congress relaxed the requirement on the type of data subjects that could be targeted by NSLs, and permitted the FBI to issue a letter not only when the target itself is a foreign power, but also when it was communicating with a foreign agent.
32. That is, tracing phone numbers and emails—these are surveillance devices that allow wiretapping of communications' metadata.
33. Regan (2004) notes that the Act was introduced only days after the 9/11 attacks and during the anthrax attacks, which led to the closure of the Hart Senate office building. The Senate voted 98–1 on the Act and the House passed it with a majority of 357–66.
34. These privacy reductions include provisions in which: (i) Educational institutions were required to disclose students' records when law enforcement certifies that they may be relevant to a terrorism investigation. Special attention was given to the authority to collect foreign students' information; (ii) Financial data that was protected through the Fair Credit Reporting Act and the Financial Privacy Right would now be available to law enforcement when the FBI certifies that these records are relevant to a terrorism investigation. Banks receive special attention in the Act and are permitted by Section 358 to disclose banking records to government authorities. They can also share information (Section 314) with federal law enforcement in a process that requires the bank to match financial reports to names of suspects; (iii) Communications providers, which were previously required to follow ECPA, had to allow law enforcement access to more types of data such as routing and address information of Internet communications. Lee (2003) further details how the act creates voluntary mechanisms for ISPs to hand information to the government without any court order or subpoena. ISPs can also disclose content when they have a reasonable belief that there is an emergency situation involving an immediate danger; (iv) Customer's cable company records, previously protected by the 1984 Cable Communications Policy Act, are now less protected when law enforcement agencies seek to obtain the information. Previously, FBI collection of subscribers' information was only permitted upon advance notice and justification in court. However, when cable companies began to offer Internet access services, the information they held became extremely valuable for law enforcement. Section 211 of the Patriot Act gives law enforcement easier access to that information.
35. The 9/11 Commission (2004) discussed barriers to information sharing and recommended dissolving some of the current barriers (pp. 78–80, 327–328, 394, 416–427; see <https://www.9-11commission.gov/report/911Report.pdf>).
36. Ashcroft's proposed changes allowed the FBI to use private sector databases to predict and prevent terrorist attacks, and monitor websites and online chatrooms, without any evidence of criminal activity or suspicious behavior. These surveillance powers are not limited to terrorism-related investigations and could apply to any violation of federal law. Ashcroft justified this increase of investigatory powers as necessary in the age of terrorism and the shift in the FBI's role from mitigating crimes to preventing plots altogether.
37. For more on this aspect of Snowden's revelation, see <https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order>.
38. Since the passage of the Patriot Act, the number of issued NSLs has significantly increased, from "hundreds" in 1978–2001, to perhaps more than 30,000 in 2002–05 (Office of the Inspector General, 2007, "A review of the FBI's use of NSLs"). See <https://oig.justice.gov/special/s0703b/final.pdf>.

39. According to *The Wall Street Journal*, the NSA has monitored large volumes of records and domestic emails and Internet searches as well as bank transfers, credit-card transactions, travel, and telephone records. See <https://www.wsj.com/articles/SB120511973377523845>.
40. Recipients of NSLs were able to consult a lawyer and courts could decide that an NSL request was unreasonable. The FBI had to also provide semi-annual reports to Congress about the usage of NSLs (Nieland, 2007).
41. *The Wall Street Journal*. See Note 39.
42. See <https://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html>.
43. For more on Klein's revelations, see <http://www.washingtonpost.com/wp-dyn/content/article/2007/11/07/AR2007110700006.html>.
44. See page 7 in the report from the CRS by Edward C. Liu (2013) on FISA's reauthorization. <https://fas.org/sgp/crs/intel/R42725.pdf>.
45. The "about" collection addresses information gathered from Internet infrastructures based on certain selectors, such as an email address, within the communication content itself. If Americans get caught in a conversation between foreign intelligence targets, they can be surveilled without a court order.
46. These exceptions are listed at <https://www.lawfareblog.com/presidents-speech-and-ppd-28-guide-perplexed>.
47. See more in Wittes's (2014) Lawfare blog post, available at <https://www.lawfareblog.com/presidents-speech-and-ppd-28-guide-perplexed>.
48. Agents are now required to minimize their selection terms, avoid using broad geographical regions, and demonstrate the relevance of information obtained. The Inspector General should report to Congress on the importance of collected information and the efficiency of minimization requirements. See more in Wizner (2017).
49. This has not discouraged the government from increasingly using NSLs. For instance, the Apple company reported 16,249 NSL requests between July 1 and December 31, 2017. This is almost three times higher than the 5,999 requests received during the same period in 2016. See <https://www.cyberscoop.com/apple-reports-spike-u-s-national-security-requests-amid-promises-transparency/>.
50. The 2017 CIA's procedures were approved by the attorney general and are available at <https://www.cia.gov/about-cia/privacy-and-civil-liberties/CIA-AG-Guidelines-Signed.pdf>.
51. The NSA's statement is available at <https://www.nsa.gov/news-features/press-room/statements/2017-04-28-702-statement.shtml>.
52. See Tim Cook's 2016 statement at <https://www.apple.com/customer-letter/>.
53. See the official response by Microsoft's president, Brad Smith, at <https://blogs.microsoft.com/on-the-issues/2017/10/16/us-supreme-court-will-hear-petition-to-review-microsoft-search-warrant-case-while-momentum-to-modernize-the-law-continues-in-congress/>.
54. Privacy advocates' concerns are summarized at <https://www.wired.com/story/us-vs-microsoft-supreme-court-case-data/>.
55. See Recommendation #12 at https://www.justsecurity.org/wp-content/uploads/2013/12/2013-12-12_rg_final_report.pdf.
56. See Note 20.
57. See Jennifer Granick's view on CISA's policy process at <https://www.justsecurity.org/28386/omnicisa-pits-government-against-self-privacy/>.
58. DNI Guidelines are available at https://www.odni.gov/files/documents/Newsroom/Domestic_Sharing_Counterterrorism_Information_Report.pdf.
59. This aspect of Snowden's revelations is highlighted at <https://www.theguardian.com/world/2013/aug/09/nsa-loophole-warrantless-searches-email-calls>.
60. These include limitations on queries for searches in databases subject to FISA Court review. In addition, the FBI must obtain a court order and demonstrate probable cause to access these contents. Moreover, the Act states that Congress must be notified of uses of this procedure to surveil U.S. citizens 30 days in advance. The written notice should include a FISA Court approval of the surveillance and a list of privacy protections to be applied. The DNI and attorney general are also required to publicly release the minimization procedures, and even in emergency situations, a judge must approve the surveillance retroactively. The reauthorization also extends whistleblower protections to contractor employees in the intelligence community and the FBI, and requires the NSA and FBI to appoint a privacy official.
61. Privacy advocates' views on this issue are summarized at <https://www.vox.com/2018/1/11/16878220/house-vote-surveillance-spying-fisa>.
62. Through the 1984 Crime Control Act that was later amended by the 1986 Computer Fraud and Abuse Act.
63. Through the Directive, new committees within the executive branch were created, responsibilities were assigned, and the sharing of technical expertise across executive agencies was required.

64. The 1996 Clinger–Cohen Act mandated this assignment.
65. As outlined in OMB’s policy memos—M-07-16 (2007), M-08-23 (2008), M-10-28 (2010), M-17-05 (2016)—the agency (i) posed breach notification requirements in 2007; (ii) required the deployment of the more secure DNSSEC protocol in 2008; (iii) expanded the operational role of DHS in federal networks in 2010; and (iv) published a policy to increase its oversight capacities over information security in federal agencies in 2016.
66. DOC’s strategy document, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework*, argues that “many key actors, due to the sectorial privacy and cybersecurity approach of the U.S., operate without specific statutory obligations to protect personal data” (p. 12; see https://www.ntia.doc.gov/files/ntia/publications/iprf_privacy_greenpaper_12162010.pdf). The strategy addresses the privacy and security problems of “non-critical” sectors and recommends the adoption of privacy standards and federal breach notification rules, after a decade of failed attempts to do so. These are rules that require companies to report and face financial consequences in case of a data breach. Currently, the United States has 47 versions of breach notification laws across states and was unable to pass unified federal legislation despite many attempts since 2003. There is controversy over issues like federal preemption, desired policy goals, scope of notification, and effectiveness of policy (Thaw, 2015).
67. The strategy document is the *Cybersecurity Risk Management and Best Practices Working Group 4: Final Report March 2015*, FCC. See https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf.
68. The new FCC chairman, Ajit Pai, blocked FCC requirements from ISPs to apply common sense security practices and protect personal information. More on this policy process is available at <http://stlr.org/2016/12/12/the-fccs-latest-privacy-regulations-a-new-stance-on-private-sector-protections/>.
69. James X. Dempsey’s testimony before the Subcommittee on Crime in the Committee on Judiciary, 1997. See https://fas.org/irp/congress/1997_hr/h971023d.htm.
70. For example, NSA wiretapping of an AT&T facility and Microsoft’s, Yahoo!’s, Google’s, Facebook’s, and Apple’s data centers through the PRISM program. See <https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>.
71. See Note 57.
72. For a summary of these failed attempts, see <https://www.accessnow.org/no-more-waiting-its-time-for-a-federal-data-breach-law-in-the-u-s/>.
73. See the June 21, 2016 meeting minutes from the Commission on Enhancing National Cybersecurity on private sector cybersecurity challenges at https://www.nist.gov/sites/default/files/june_21_2016_ucb_meeting_minutes.pdf. Also see an overview of the role of the state in the private-sector cybersecurity challenge: <https://www.georgetownjournalofinternationalaffairs.org/online-edition/2018/5/27/the-role-of-the-state-in-the-private-sector-cybersecurity-challenge>.
74. See CRS 2012 report by Eric A. Fischer on the numerous failed attempts to pass a federal information sharing legislation in Congress at <https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-073.pdf>.

References

- Benn, S.I. 1971. “Privacy, Freedom, and Respect for Persons.” In *Privacy*, eds. J.R. Pennock and J.W. Chapman. New York: Atherton Press, 1–26.
- Bennett, C.J. 1992. *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*. Ithaca, NY: Cornell University Press.
- Bevier, L.R. 1989. “What Privacy Is Not.” *Harvard Journal of Law & Public Policy* 12: 99–103.
- Bevier, L.R. 1999. “The Communications Assistance for Law Enforcement Act of 1994: A Surprising Sequel to the Break Up of AT&T.” *Stanford Law Review* 51 (5): 1049–125.
- Birnhack, M., and N. Elkin-Koren. 2003. “The Invisible Handshake: The Reemergence of the State in the Digital Environment.” *Virginia Journal of Law and Technology Association* 8 (6): 1–57.
- Bygrave, L.A. 2002. *Data Protection Law—Approaching its Rationale, Logic, and Limits*. The Hague: Kluwer Law International.
- Chandler, J. 2009. “Privacy Versus National Security: Clarifying the Trade-Off.” In *Lessons From the Identity Trail: Privacy Anonymity and Identity in a Networked Society*, eds. I. Kerr, C. Lucock, and V. Steeves. Oxford, England, UK: Oxford University Press, 132–38.

- Chertoff, M. 2008. "The Cybersecurity Challenge." *Regulation & Governance* 2 (4): 480–84.
- Church Committee. 94th U.S. Congress. 1976. *Book III: Intelligence Activities and the Rights of Americans*. Washington, DC: U.S. Government Printing Office.
- Clinton, W.J., and A. Gore. 1997. *A Framework for Global Electronic Commerce*. Washington, DC: Office of the President.
- Dempsey, J.X. 1997. "Communications Privacy in the Digital Age: Revitalizing the Federal Wiretap Laws to Enhance Privacy." *Albany Law Journal of Science & Technology* 8 (1): 65–120.
- Dhillon, G. 2006. *Principles of Information Systems Security: Texts and Cases*. Hoboken, NJ: John Wiley & Sons.
- Diffie, W., and S. Landau. 2007. *Privacy on the Line: The Politics of Wiretapping and Encryption*. Updated and Expanded Edition. Cambridge: MIT Press.
- Dunn Cavelti, M. 2008. *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*. Abingdon, UK: Routledge.
- Dunn Cavelti, M. 2010. "Cyber-Security." In *The Routledge Handbook of New Security Studies*, ed. P.J. Burgess. Oxford: Taylor and Francis, 154–62.
- Dworkin, R. 1977. *Taking Rights Seriously*. Cambridge: Harvard University Press.
- Etzioni, A. 1999. *The Limits of Privacy*. New York: Basic Books.
- Etzioni, A. 2011. "Cybersecurity in the Private Sector." *Issues in Science and Technology* 28 (1): 58–62.
- Flaherty, D.H. 1989. *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada and the United States*. Chapel Hill: University of North Carolina Press.
- Fried, C. 1968. "Privacy." *Yale Law Journal* 77: 475–93.
- FTC v. Wyndham Worldwide Corporation* (2015).
- Gavison, R. 1980. "Privacy and the Limits of Law." *Yale Law Journal* 89: 421–71.
- Gidari, A. 2006. "Companies Caught in the Middle." *University of San Francisco Law Review* 41: 535–58.
- Gidari, A., and P. Coie. 2006. "Designing the Right Wiretap Solution: Setting Standards Under CALEA." *IEEE Security & Privacy* 4 (3): 29–36.
- Granick, J. 2017. *American Spies: Modern Surveillance, Why Should You Care, and What To Do About It*. Cambridge: Cambridge University Press.
- Hiller, J.S., and R.S. Russel. 2013. "The Challenge and Imperative of Private Sector Cybersecurity: An International Comparison." *Computer Law & Security Review* 29: 236–45.
- Hughes, D.R.L. 2015. "Two Concepts of Privacy." *Computer Law & Security Review* 31: 527–37.
- Innes, J. 1992. *Privacy, Intimacy, and Isolation*. New York: Oxford University Press.
- Jarvis, J.T. 1975. "The Right to Privacy." *Philosophy and Public Affairs* 4 (4): 295–314.
- Johnson, K.N. 2015. "Managing Cyber Risks." *Georgia Law Review* 50 (1): 547–92.
- Kafka, F. 1925. *The Trial*. Berlin: Verlag Die Schmiede.
- Katz v. United States*, 389 U.S. 347 (1967).
- Kerr, O. 2003. "Internet Surveillance Law After the Patriot Act." *Northwestern University Law Review* 97 (2): 607–74.
- Kleinig, J., P. Mameli, S. Miller, D. Salane, and A. Schqartz. 2011. *Security and Privacy: Global Standards for Ethical Identity Management in Contemporary Liberal Democratic States*. Canberra: ANU Press & CAPPE Publication.
- Laudon, K.C. 1996. "Markets and Privacy." *Communications of the ACM* 39 (9): 92–104.
- Lee, L.T. 2003. "The USA PATRIOT Act and Telecommunications: Privacy Under Attack." *Rutgers Computer & Technology Law Journal* 29 (2): 371–404.
- Lessig, L. 1999. *Code and Other Laws of Cyberspace*. New York: Basic Books.
- Levi-Faur, D. 2006. "A Question of Size?" In *Innovative Comparative Methods for Policy Analysis*, eds. B. Rihoux and H. Grimm. Boston: Springer, 43–66.
- Lindsay, D. 2005. "An Exploration of the Conceptual Basis of Privacy and the Implications for the Future of Australian Privacy Law." *Melbourne University Law Review* 29 (179): 131–48.

- Loader, I., and N. Walker. 2007. *Civilizing Security*. Cambridge: Cambridge University Press.
- Logan, C. 2009. "The FISA Wall and Federal Investigations." *New York University Journal of Law & Liberty* 4: 209–51.
- Microsoft Corp. v. United States* (2015).
- Moore, A.D. 2003. "Privacy: Its Meaning and Value." *American Philosophical Quarterly* 40 (3): 215–27.
- Newman, A.L., and D. Bach. 2004. "Self-Regulatory Trajectories in the Shadow of Public Power: Resolving Digital Dilemmas in Europe and the United States." *Governance* 17 (3): 387–413.
- Nieland, A.E. 2007. "National Security Letters and the Amended Patriot Act." *Cornell Law Review* 92 (6): 1201–38.
- Nissenbaum, H. 2010. *Privacy in Context. Technology, Policy, and the Integrity of Social Life*. Stanford, CA: Stanford University Press.
- Nylund, J. 2000. "Fire With Fire: How the FBI Set Technical Standards for the Telecommunications Industry Under CALEA." *CommLaw Conspectus* 8: 329–48.
- Orwell, G. 1949. 1984. London: Secker and Warburg.
- Quigley, K., and J. Roy. 2012. "Cyber-Security and Risk Management in an Interoperable World: An Examination of Governmental Action in North America." *Social Science Computer Review* 30 (1): 83–94.
- Raab, C. 2014. "Privacy as a Security Value." In *Jon Bing: En Hyllest/A Tribute*, eds. J. Bing, D.W. Schartum, L.A. Bygrave, and A.G.B. Bekken. Copenhagen, Denmark: Gyldendal, 39–58.
- Rachels, J. 1975. "Why Privacy Is Important." *Philosophy & Public Affairs* 4 (4): 323–33.
- Regan, P.M. 1995. *Legislating Privacy: Technology, Social Values, and Public Policy*. Chapel Hill: UNC Press.
- Regan, P.M. 2004. "Old Issues, New Context: Privacy, Information Collection, and Homeland Security." *Government Information Quarterly* 21: 481–97.
- Regan, P.M. 2009. "Federal Security Breach Notifications: Politics and Approaches." *Berkeley Technology Law Journal* 24 (3): 1103–32.
- Reiman, J.H. 1976. "Privacy, Intimacy and Personhood." *Philosophy & Public Affairs* 6: 26–44.
- Reveron, D.S., N.K. Gvosdev, and J.A. Cloud. 2018. "Introduction: Shape and Scope of U.S. National Security." In *The Oxford Handbook of U.S. National Security*, eds. D.S. Reveron, N.K. Gvosdev, and J.A. Cloud. Oxford, UK: Oxford University Press, 1–16.
- Romm, J.J. 1993. *Defining National Security: The Nonmilitary Aspects*. New York: Council on Foreign Relations.
- Schwartz, P.M., and E.J. Janger. 2007. "Notification of Data Security Breaches." *Michigan Law Review* 105: 913–84.
- Soghoian, C. 2012. "The Spies We Trust: Third Party Service Providers and Law Enforcement Surveillance." PhD dissertation. Indiana University, School of Informatics, Department of Computer Science.
- Solove, D. 2008. *Understanding Privacy*. Cambridge, MA: Harvard University Press.
- Solove, D. 2011. *Nothing to Hide: The False Tradeoff Between Privacy and Security*. New Haven: Yale: University Press.
- Thaw, D. 2014. "The Efficacy of Cybersecurity Regulation." *Georgia State University Law Review* 30 (2): 287–374.
- Thaw, D. 2015. "Data Breach (Regulatory) Effects." University of Pittsburgh Legal Studies Research Paper No. 2015–13.
- The 9/11 Commission. 2004. *Final Report of the National Commission on Terrorist Attacks Upon the United States*. New York and London: W. W. Norton & Company.
- The President's Review Group on Intelligence and Communications Technologies. 2014. *The NSA Report: Liberty and Security in a Changing World*. Princeton, NJ: Princeton University Press.
- United States v. U.S. District Court*, 407 U.S. 297 (1972).
- United States v. Miller*, 425 U.S. 435 (1976).
- Waldron, J. 2003. "Security and Liberty: The Image of Balance." *Journal of Political Philosophy* 11 (2): 191–210.
- Waldron, J. 2006. "Safety and Security." *Nebraska Law Review* 85: 454–507.

- Warner, M. 2012. "Cyber Security: A Pre-History." *Intelligence and National Security* 27 (5): 781–99.
- Warner, M. 2015. "Notes on the Evolution of Computer Security Policy in the U.S. Government 1965–2003." *IEEE Annals of the History of Computing* 37 (2): 8–18.
- Warren, S.D., and L.D. Brandeis. 1890. "The Right to Privacy." *Harvard Law Review* 4: 193–220.
- Westin, A. 1967. *Privacy and Freedom*. New York: Atheneum.
- Wizner, B. 2017. "What Changed After Snowden? A U.S. Perspective." *International Journal of Communication* 11: 897–901.
- Wolfers, A. 1952. "National Security as an Ambiguous Symbol." *Political Science Quarterly* 67 (4): 481–502.
- Zedner, L. 2003. "Too Much Security?" *The Journal of Sociology of Law* 31 (3): 155–84.
- Zelikow, P. 2003. "The Transformation of National Security." *National Interest* 71. <http://nationalinterest.org/article/the-transformation-of-national-security-491>.

Appendix: Methodological Annex

This section covers the sources of data collection and presents the article's classification of policy events by: (i) the type of national security and privacy relationships based on policy purpose and features; and (ii) according to policy arenas.

Data Collection and Sources

The collection of all policy events that address national security and privacy in the U.S. federal arena required familiarity with the policy actors and debates. The data collection started with the Federation of American Scientists website (fas.org), which makes CRS reports publicly accessible on a regular basis. Documents were browsed from the category of "National Security Topics" and searched for the keyword: "cyber." This search yielded 10 reports between 2005 and 2016 that related to the ways Congress handled security and privacy issues in cyberspace. The key word "privacy" was also searched in the "Intelligence Policy" category. Three reports yielded by this search related to national security versus privacy issues in the federal arena.

The reports provided a list of the laws, executive orders, and government agencies that address the national security and privacy balance. Then, (i) The relevant federal statutes from the Library of Congress website (www.loc.gov) were downloaded and (ii) The White House and Government Agencies websites (FTC, FCC, Department of Commerce, DoD, DHS, OMB, DNI, SEC, CFPB, NSA, DOJ, and NIST) were accessed to gather all policy documents and agency rules that address national security and privacy.

The first two data collection steps yielded documents that revealed how the U.S. conducts surveillance and promotes cybersecurity. Then, through access to the website whistleblower.org, which archives major whistleblowing acts, previously classified documents that address privacy and security were accessed. Online search engines were also used to search for news headlines regarding the content of leaked documents that relate to the way the U.S. government

constructed national security and privacy relationships. Some of the major whistleblowing acts were explored chronologically, including: Joseph Nacchio on NSA engagements with the private sector (2001), William Binney and J. Kirk Wiebe on NSA Trailblazer data collection programs (2001), Thomas Tamm on the PSPs after 9/11 (2003), Thomas Drake on NSA programs (2005), Mark Klein on the NSA facility within AT&T's facility (2006), Samy Kamkar on mobile phone hacking (2010), and Edward Snowden on U.S. government surveillance programs (2013). Official investigative committees' reports were also a major data collection source. For instance, the 1976 Church Committee Report following FBI's and Watergate domestic surveillance scandals, the 9/11 Commission Report, and the 2014 "Liberty and Security in a Changing World" report, which included the President's Review Group on Intelligence and Communication Technologies' recommendations after Snowden's revelations.

Scholarly works were also an important secondary source for data collection. The works of Charles Raab, Collin Bennett, Priscilla Regan, David Thaw, Abraham Newman, Amitai Etzioni, Susan Landau, Daniel Solove, Charles Fried, David H. Flaherty, William Diffie, and Albert Gidari were extensively reviewed. This is a partial list of scholars who address the relationships between national security and privacy, and their work enriched the study's empirical insights and analytical perspectives on these issues. Additionally, the Google Alerts tool was used to receive daily emails based on the following keywords: "US cyber security," "national security," and "privacy," exposing the work of think tanks, independent bloggers, and law firms in the field. These include publications from think tanks such as New America, Electronic Frontier Foundation, the Center for Democracy and Technology, and Stanford University's Center for Internet and Society, reports from law firms such as "Skadden, Arps, Slate, Meagher & Flom's Monthly Privacy and Cybersecurity updates," and the works of independent bloggers like Bruce Schneier and Brian Krebs. Finally, the IT Wiki Law website, an encyclopedia of policy measures in the fields of IT, was a useful source that was also used to collect information on the studied policy relationships.

Data Classification

The initial classification of the 63 policy events to categories and arenas according to policy features and purpose (in this order of importance) was done by the author, followed by an intercoder reliability process in which two independent coders classified the data as well. The process yielded five cases of conflict that were resolved after discussion. The classifications of the 63 policy events included in the study are shown in the following table.

Year	Name	Purpose	Features	Dynamic	Arena
1968	The Wiretap Act	Regulates information collection	Attentive privacy measures	Compromise	Crime
1972	<i>United States v. U.S. District Court</i>	Regulates information collection	Attentive privacy measures	Compromise	Foreign Intelligence
1974	Privacy Act	Regulates information collection	No privacy-harming features	Complementary	Cybersecurity
1976	Church Committee	Regulates information collection	Attentive privacy measures	Compromise	Foreign Intelligence
1976	<i>United States v. Miller</i>	Regulates information collection	Attentive privacy measures	Compromise	Crime
1976	EO 11905	Regulates information collection	Attentive privacy measures	Compromise	Foreign Intelligence
1978	EO 12036	Regulates information collection	Attentive privacy measures	Compromise	Foreign Intelligence
1978	FISA	Regulates information collection	Attentive privacy measures	Compromise	Foreign Intelligence
1978	Right to Financial Privacy Act	Regulates information collection	Attentive privacy measures	Compromise	Crime
1981	EO #12333	Regulates information collection	Lax privacy measures	Harm	Foreign Intelligence
1984	Comprehensive Crime Control Act of 1984	Protects vital information systems	No privacy-harming features	Complementary	Cybersecurity
1984	Reagan's National Security Directive 145 (NSD-145)	Protects vital information systems	Lax privacy measures	Harm	Cybersecurity
1986	CFAA	Protects vital information systems	No privacy-harming features	Complementary	Cybersecurity
1986	Memo by John Poindexter on NSA Authority—1986 NTISSP No.2	Protects vital information systems	Lax privacy measures	Harm	Cybersecurity
1986	ECPA & Title II (SCA)	Regulates information collection	Attentive privacy measures	Compromise	Crime
1987	Computer Security Act	Protects vital information systems	Attentive privacy measures	Compromise	Cybersecurity
1989	NIST and NSA Memorandum of Understanding	Protects vital information systems	Lax privacy measures	Harm	Cybersecurity
1990	NSC Directive 42	Protects vital information systems	No privacy-harming features	Complementary	Cybersecurity

Continued

Year	Name	Purpose	Features	Dynamic	Arena
1993	Clipper Chip framework and export restrictions on encryption devices	Regulates information collection	Lax privacy measures	Harm	Crime
1993	Amendment that relaxed NSL restrictions	Regulates information collection	Lax privacy measures	Harm	Crime
1994	CALEA/Digital Telephony and Privacy Improving Act of 1994	Regulates information collection	Lax privacy measures	Harm	Crime
1995	A failed legislation attempt to harm privacy after Oklahoma shooting	Regulates information collection	Lax privacy measures	Harm	Crime
1996	A failed legislation attempt to harm privacy after TWA plane explosion	Regulates information collection	Lax privacy measures	Harm	Crime
1996	Clinger-Cohen Act	Protects vital information systems	No privacy-harming features	Complementary	Cybersecurity
1996	HIPAA	Protects vital information systems	No privacy-harming features	Complementary	Cybersecurity
1997	Global Electronic Commerce Framework	Protects vital information systems	No privacy-harming features	Complementary	Cybersecurity
1998	FISA Amendment	Regulates information collection	Lax privacy measures	Harm	Foreign Intelligence
1999	GLBA	Protects vital information systems	No privacy-harming features	Complementary	Cybersecurity

Continued

Year	Name	Purpose	Features	Dynamic	Arena
2001	Authorization for use of military force against terrorists	Regulates information collection	Lax privacy measures	Harm	Foreign Intelligence
2001	Patriot Act	Regulates information collection	Lax privacy measures	Harm	Foreign Intelligence
2002	PSFs	Regulates information collection	Lax privacy measures	Harm	Foreign Intelligence
2002	Attorney General Ashcroft Guidelines	Regulates information collection	Lax privacy measures	Harm	Foreign Intelligence
2002	Sarbanes-Oxley Act	Protects vital information systems	No privacy-harming features	Complementary	Cybersecurity
2002	FISMA	Protects vital information systems	No privacy-harming features	Complementary	Cybersecurity
2006	USA Patriot Improvement and Reauthorization Act of 2005	Regulates information collection	Lax privacy measures	Harm	Foreign Intelligence
2006	FCC extension to 1994 CALEA law to include Internet access and Voice over IP providers	Regulates information collection	Lax privacy measures	Harm	Crime
2007	OMB Memo M-07-16	Protects vital information systems	No privacy-harming features	Complementary	Cybersecurity
2008	OMB Memo M-08-23	Protects vital information systems	No privacy-harming features	Complementary	Cybersecurity
2008	FISA Amendments Act (FAA)	Regulate information collection	Lax privacy measures	Harm	Foreign Intelligence
2009	HITECH	Protects vital information systems	No privacy-harming features	Complementary	Cybersecurity
2009	FTC rule over the HITECH Act	Protects vital information systems	No privacy-harming features	Complementary	Cybersecurity
2010	OMB Memo M-10-28	Protects vital information systems	No privacy-harming features	Complementary	Cybersecurity

Continued

Year	Name	Purpose	Features	Dynamic	Arena
2010	Commercial Data Privacy and Innovation in the Internet Economy: A dynamic policy framework	Protects vital information systems	No privacy-harming features	Complementary	Cybersecurity
2011	Dodd-Frank Wall Street Reform	Protects vital information systems	No privacy-harming features	Complementary	Cybersecurity
2011	Patriot Sunset Extensions	Regulates information collection	Lax privacy measures	Harm	Foreign Intelligence
2012	FISA Amendments Act	Regulates information collection	Lax privacy measures	Harm	Foreign Intelligence
	Reauthorization Act of 2012				
2013	HITECH	Protects vital information systems	No privacy-harming features	Complementary	Cybersecurity
2013	SEC and CFTC Rule	Protects vital information systems	No privacy-harming features	Complementary	Cybersecurity
2014	PPD-28—Signals Intelligence Activities	Regulates information collection	Attentive privacy measures	Compromise	Foreign Intelligence
2014	FISMA (Federal Information Security Modernization Act)	Protects vital information systems	No privacy-harming features	Complementary	Cybersecurity
2014	SEC Policy Memo on SCI Regulation	Protects vital information systems	No privacy-harming features	Complementary	Cybersecurity
2015	FCC Cybersecurity Risk Management and Best Practices	Protects vital information systems	No privacy-harming features	Complementary	Cybersecurity

Continued

Year	Name	Purpose	Features	Dynamic	Arena
2015	The Cyber-Security Act of 2015	Protects vital information systems	Lax privacy measures	Harm	Cybersecurity
2015	<i>Microsoft Corp. v. United States</i>	Regulates information collection	Attentive privacy measures	Compromise	Crime
2015	U.S. Freedom Act	Regulates information collection	Attentive privacy measures	Compromise	Foreign Intelligence
2016	Apple's judicial challenge to a court order for unlocking one of its iPhone models	Regulates information collection	Attentive privacy measures	Compromise	Crime
2016	OMB Memo M-17-05	Protects vital information systems	No privacy-harming features	Complementary	Cybersecurity
2016	FCC Regulations on ISPs	Protects vital information systems	No privacy-harming features	Complementary	Cybersecurity
2017	DNI Information Sharing on Counter Terrorism	Regulates information collection	Lax privacy measures	Harm	Foreign Intelligence
2017	CIA updated guidelines for information collection under EO #12333	Regulates information collection	Attentive privacy measures	Compromise	Foreign Intelligence
2017	NSA statement on stopping "about" collection procedures	Regulates information collection	Attentive privacy measures	Compromise	Foreign Intelligence
2018	Cloud Act	Regulates information collection	Attentive privacy measures	Compromise	Crime
2018	FISA Reauthorization	Regulates information collection	Lax privacy measures	Harm	Foreign Intelligence

CHAPTER 2

Framing and Governing Cyber Risks: Comparative Analysis of U.S. Federal Policies [1996-2018]

This chapter presents a manuscript accepted for publication at the *Journal of Risk Research*

Framing and Governing Cyber Risks
Comparative Analysis of U.S. Federal Policies [1996-2018]

ABSTRACT

Cyber risk governance has been occupying U.S. policymakers in the past two decades. This pressing challenge calls for a better understanding of how policymakers frame and consequently craft risk governance frameworks using public policies. Through a novel typology that analyzes the patchwork of laws and regulations in this policy space, this article investigates how policymakers design risk governance frameworks to address cyber risks. This typology is based on a systematic text analysis of thirty federal policies from the past twenty-two years (1996-2018) in which (N=463) key sentences were recognized and coded to ten risk governance categories. Existent literature highlights the significance of risk framing to policy outputs and explains cross-national rather than cross-sector variance in risk governance. It also considers only specific cyber policy measures and does not question the link between policymakers' risk framings and chosen policy paths. In contrast, this study finds that policymakers create three distinct risk governance frameworks across private owners of critical infrastructures, health and financial service providers, and companies in the broader digital economy. These risk regimes are comparatively analyzed to gauge variance (1) *across sectors*: in the role of the government and the extent to which it dictates coercive risk management steps, and (2) *over time*: on the ways in which the government has responded to cyber threats. I found that variance stemmed from the institutional configurations in each regulated sector and the consequent decision-making structures that had been institutionalized early on, rather than the framing of cyber risks. Tracing the governance of cyber risks and the missing link between policymakers' risk framings and actions, this study sheds light on how seemingly technical decisions of cybersecurity governance can be social and political issues that are contingent on institutional settings and early policy decisions, questioning the central role of framing to risk governance outputs.

1 – INTRODCUTION

Governing the security of cyberspace is a challenging task for state officials. Despite efforts to improve the ability of the private sector to assess, reduce, or mitigate risks from digital technologies, the number of cyber incidents is on the rise. Criminals exploit cyberspace for profit, intellectual property and personal information are regularly stolen, and national infrastructures are constantly targeted (U.S. Government Accountability Office, 2017).

This ongoing policy challenge highlights the importance of understanding how policymakers frame and design cyber risk governance frameworks through public policies. Theoretically, cyber risk governance provides an appealing case study since these risks cut across all sectors in the economy and can potentially highlight the impact of risk framing and the influence of different institutional configurations on policy outputs.

I examined thirty policies from the U.S. federal cybersecurity policy arena in the past two decades to realize how policymakers frame and subsequently design governance arrangements across sectors. A closer examination of this policy arena revealed three distinct framing of cyber risks by policymakers. I built on Fichtner (2018) who had recognized three common approaches to cybersecurity – as a public/private infrastructure concern, a data protection problem, or a tool to safeguard financial interests. Different sets of values inform every approach: national security, privacy, or economic order. Each approach, in turn, puts forth different objects to protect, threats to consider, and roles for the actors involved. But how these different risk framings impact cyber risk governance? I recognized how these distinct approaches yield three different risk governance frameworks and comparatively analyzed them across sectors and over time to realize the impact of risk framing on policy outputs, explain cross-sector variance in risk governance, and advance our understanding on the development of cyber risk governance.

While risk scholars stress the importance of risk framing to risk governance outputs, its impact has yet to be analyzed for the governance of cyber risks. Moreover, the risk governance literature mostly considers cross-national rather than cross-sector variance, and this study aims to take us one step closer in understanding how different institutional configurations impact risk policies within the same political system. In addition, these different approaches to cyber risk governance are empirically under-studied. Despite works by governance scholars on specific policy measures, in certain time frames, we still do not

know what shape and form those cyber risk governance frameworks take or how they change over time.

I therefore ask: how have U.S. federal policies constructed cyber risk governance frameworks across sectors between the years of 1996 and 2018? How have these governance frameworks changed over time and across sectors? And how have different framings and characterizations of cyber risks impacted the policy paths policymakers have chosen?

In order to answer these questions, I conducted a text analysis of thirty U.S. federal cybersecurity policies between the years of 1996 and 2018, extracted (N=463) key sentences in these texts, and suggested a typology for translating federal policies into risk governance frameworks. The analysis revealed three distinct risk governance frameworks that differently affect private owners of critical infrastructures, health and financial service providers, and companies in the broader digital economy. Then, based on the implied risk framings and characterizations of cyber risks in these texts and the initial decision-making structures they have created, I explained the extent to which cyber risk governance frameworks have changed across sectors and over time.

Answering these questions is important for four reasons. Empirically, governance arrangements for cybersecurity have not been studied to trace variance over the course of two decades. Methodologically, a comparative approach across private sectors based on text-analysis of policy contents allows to trace similarities and differences in cybersecurity governance and clarify sources of variations across private sectors. In addition, such methodological approach disentangles cybersecurity policies according to the practices of risk-management they deploy and reveals the plurality of dimensions in each federal policy. Policy-wise, this study throws light on the extent to which cyber risk framings and governance arrangements have remained unaltered over time. In light of increased sophistication of the cyber threat landscape, policy stability is an alarming pattern that needs to be better explained. Theoretically, such policy stability is surprising since policymakers are known to be responsive to new risks that arise (e.g. Vogel, 2012) and risk framings tend to be dynamic for a given risk during the policy process (e.g. Plein, 1991; Dunlop, 2007). Furthermore, due to paucity of cross-sector studies in risk governance and a few empirical studies on cyber risk governance, we lack a theoretical understanding on the extent of the impact of cyber risk framings on governance outputs, the factors that drive variance across sectors within the same political system, and the importance of time and self-reinforcing mechanisms (Pierson, 2000) on cyber policy outcomes. While trends of ‘risk-colonization’ (Rothstein et al., 2006) and ‘securitization’ (Buzan et al., 1998) often occupies cybersecurity

scholars, the role of institutional configurations in dictating cyber governance has not been given full scholarly attention.

Thus, this contribution goes beyond existing literature that studies certain instances of cybersecurity policies in specific time frames and mostly ignores the different framings of the cybersecurity problem across sectors. Contrarily, I consider policymakers as risk agents that are influenced by their own risk governance processes; they assess, estimate, and evaluate the risk in their policy texts before producing policy outputs. I also find that careful comparative examination of cyber policies clarifies how cybersecurity governance can be explained not by nature of the cyber problem to tackle per se (Weiss and Jankauskas, 2018), but rather through decision-making structures, which were determined by the early stages of policy development. Unsurprisingly, increased sophistication of cyber threats over time has led the federal government to respond, albeit in ways that mirrored existing paradigms and did not diverge from two decades old decision-making structures.

This article comprises four sections. The next section presents a literature review that highlights the importance of risk frames to risk governance and particularly to cyber risk governance. This part also derives expectations of what kind of risk governance frameworks I expected to find and what can explain variance across sectors. The second section sets forth the analytical framework and text analysis methodology used for analyzing federal policies. The third section is an empirical analysis that demonstrates how federal policies have been translated into risk governance frameworks across sectors. In the fourth section I comparatively analyze these frameworks across sectors and over time. The final section concludes by discussing how research findings contribute to risk governance theory and broaden the current literature.

2 - LITERATURE REVIEW: THE ROLE OF RISK FRAMES IN (CYBER) RISK GOVERNANCE ACROSS SECTORS

This article links between two bodies of knowledge: (1) risk and science & technology studies (STS) that discuss meanings, framings, and outputs of (cyber) risk governance, and (2) policy scholars that study cybersecurity governance. I aim to stress the importance of risk frames to risk governance and realize how and why policymakers frame cyber risks and govern them over time and across sectors. This would fill a void in the literature in three important elements.

First, despite the importance of risk framing to governance outcomes, there is a disconnection in the literature between the way policymakers characterize cyber risks and the

policy paths they consequently choose. Risk frames, in that sense, are used to structure situations and attribute meanings to them. They selectively encode objects, situations, events, and experiences with one's present and past environments (Snow and Benford, 1992), and promote a particular problem definition, causal interpretation, and treatment recommendation for the risk described (Entman, 1993). Such frames subjectively define risks, change over time, and influence the way risks are perceived, assessed, and characterized in ways that reveal how actors interpret the risks to govern (Clark, 2013).

The policy scholarship provides evidence on the importance of framing to policy outcomes. Within this literature, frames are used interchangeably with the term 'issue definition,' that is viewed as a process in which decision-makers' choices are mediated based on certain ideas or paradigms (Dunlop, 2007). The definition of issues in the policy process provides boundaries, defines what counts as relevant for attention and assessment, and biases for action (Perri 6, 2005). It encourages audiences to interpret the issue at hand using accessible concepts as opposed to other relevant ones that could be made salient (Druckman, 2004; Schuldt et al., 2017). Moreover, policy scholars argue that politics is simply the struggle over issue definitions (or ideas), their meaning, and competing interpretations (Stone, 2012). Such scholars focus on the primacy of ideas in explaining policy variation and view them as independent sources for change (e.g. Hall, 1993; John, 2012). They contrast ideational theory with other theories that emphasize the role of interests (e.g. Bachrach and Baratz, 1962) and institutions (e.g. March and Olsen, 1984) in the policy process. They argue that ideas or frames represent causal beliefs of policymakers that promote policy change and develop viable solutions when uncertainty is present (Koon et al., 2016). Studying these frames is specifically useful to understand the path of institutional change at early points in time – at the origin of the change itself (Blyth, 1997).

The framing of risks is present in the first three phases of the risk governance cycle (Renn, 2008). In the pre-assessment phase, policymakers interpret phenomena as risks and conceptualize what counts as risk. In the risk assessment phase, policymakers identify and estimate the hazards. Then, in the risk characterization and evaluation phase, policymakers provide their judgement on the seriousness of the risk as well as its tolerability and acceptability.

The framing of risks at these phases has huge implications for their subsequent governance (Hom et al., 2011). This has been highlighted by the risk literature across issues: Schuldt et al. (2017) studied how the intersection of different framings impacted tolerability toward environmental risks, Koon et al. (2016) found significant impact of frames on health

policy design, Clark (2013) showed how framing of risks influenced policy development for genetically modified foods, Hom et al. (2011) investigated framing of risks from electromagnetic fields of mobile cell phone towers to explain diverging policy approaches, Perri 6 (2005) analyzed the dynamics of individual framing of privacy risks, and Plein (1991) detailed the power of framing in promoting social acceptance of bio-technology risks.

Surprisingly, there is a scarcity of empirical works on the importance of cyber risk framings to governance outcomes. This is intriguing especially due to the relative stability in the past two decades in the framing and governance practices in the field of cybersecurity by US policymakers. Despite the dynamic threat landscape, US policymakers have been slow to respond. This does not come into terms with the risk literature: A meta-analysis of this literature by Jacob and Schiffino (2015) revealed a strong trend of responsiveness by policymakers when a new risk arises (e.g. Vogel, 2012). Specifically, scholars of risk framing (e.g. Plein, 1991; Dunlop, 2007) emphasized how dynamic risk framings are, and analyzed the ongoing ‘battles’ between different set of definitions for a given risk in the policy process.

For the governance of cyber risks, however, framing and policy outputs have not significantly changed in the past two decades. Scholars who do study the framing of cyber risks are mostly STS scholars that apply the analytical framework of ‘securitization’ (Buzan et al., 1998) on cyber issues and focus on the values that affect the different risk framings. They question the ‘objectiveness’ of the risk definition in order to capture a more diverse and rich sense of reality. The ‘securitization’ approach proposes to widen the study of security beyond its traditional focus on military affairs and include a variety of threats across security, including cyber issues (Buzan et al., 1998). Such approach views security as a ‘speech act,’ that moves an issue for the realm of normal politics to the realm of security and gives it precedence over other issues, allowing the deployment of extraordinary measures to cope with it (Buzan et al., 1998). ‘Securitizing’ an issue justifies certain activities and policies that override other ethical or social concerns. This can be used to convince an audience of the need for taking action over issues such as cyber security.

For instance, Nissenbaum (2005) and Wolf (2016) studied the meanings of cyber risks by policymakers. These meanings include certain threats, reference objects, judgement of the seriousness of the problem, and practices to deploy (also in Hansen and Nissenbaum, 2009). Fichtner (2018) takes this a step further and discusses three common approaches to cybersecurity that are motivated by different sets of values and therefore derive different objects to protect: (1) Cyber risks can be framed as risks to the protection of public infrastructures. According to this framing, damage to infrastructures can result in injuries or

deaths. The threats can emerge from nation states and capable hackers who aim to destabilize the nation. The relevant actors for coping with this problem are intelligence agencies, military units, and security agencies. In case these infrastructures are ran by private corporations, significant responsibilities are to be assigned to private companies. (2) Cyber risks can also be framed as risks to the protection of personal data. According to this framing, cyber risks jeopardize privacy; threats can come from criminal hackers, but also from corporations who engage in surveillance. Solutions usually include encryption and legislation. Finally, (3) cyber risks can be framed as risks to the advancement of the economy. According to this framing, cyber risk governance aims to defend financial assets and secure commercial revenues. Threats are posed by criminals, competitors, activists, and political groups, and guarding against them guarantees economic advantage. Within this framing, data protection is perceived as a tool for earning consumers' trust rather than defending a human right.

All these works address cybersecurity as a contested concept which can be constructed to be about different objects, threats, and responses, according to the way it was 'securitized' in the policy discourse. Each approach proposed by Fichtner (2018), or more specifically – each risk framing - constructs a unique set of relationships between the actors involved and suggests different structures and priorities for cyber risk governance. But to what extent these framings impact policy paths for cyber risk governance?

The different approaches do not consider, for instance, the institutional configurations that enable or constrain cybersecurity policy development. These different perceptions of the cybersecurity problem across sectors beg the question of whether and how different meanings of the problem affect chosen policy paths? And how institutional configurations enable or constrain such policy development?

Surprisingly, research on the link between framing and governing cyber risks is sparse. Quigley et al. (2015) studied the discourse of policymakers and the implied meanings they ascribe to cybersecurity in the field of critical infrastructure protection. They revealed how battlefield metaphors were tapped to imply that risk should be understood in military terms and chiefly as one of survival, as opposed to a trade-off between costs and benefits. This has led the government to apply a 'worst case scenario' paradigm that might be very expensive to implement. Despite the lack of sound evidence to support the widespread fear from cyber threats, the government has expended significant resources to protect guard against them. Ulmer (2014) also tied cybersecurity discourse to regulatory paths. She recognized the militarized language in the U.S. and the strong link of national security to cyber risks. Such 'war analogy,' she argued, implied military response to cyber intrusions.

My empirical analysis endeavors to shed light on this rather unexplored connection, revealing how and why different risk framings across economic sectors have translated into distinct policy paths. Thus, the *first* goal of this study is to uncover the link between the different framings of cyber risks to governance outputs and policy design.

Second, there is a paucity of studies that explain variance in risk frames and governance decisions across sectors. While the comparative approach allows policy scholars to trace causes for similarities and differences in policy outcomes and explain policy change (Lijphart, 1971), comparative risk scholars have mostly addressed cross-national (e.g. Lees, 2007; Vogel, 2012; Rothstein et al., 2013 and 2015; Krieger, 2013) rather than cross-sector (e.g. Hood et al., 2001) variance in risk governance.

Despite the trend of ‘risk colonisation,’ (Rothstein et al., 2006), according to which policymakers universally frame problems as risks as an organizing decision-making concept, scholars have found variance in the way these risks are framed and governed across policy domains and political systems. This variance is attached to institutional patterns such as - separation of powers, accepted norms, policy styles, and state structures. Scholars found that it is not much the character of the risk problem, but rather the character of the polity that determines whether or how problems are framed as risks to be governed (Rothstein et al., 2013). The most notable research that did study variance in risk governance across sectors was conducted by Hood et al. (2001), who analyzed nine risk domains in the UK and reached the conclusion that private interests are the most suitable explanation for variance in risk governance. They also found that in risk domains with strong and clear institutional norms, private interests were less effective in influencing policy change.

In addition, Dunlop (2007), who studied risks from the usage of growth hormone in animals (rbST), showed how institutionalized policy ideas, structures, and approaches shape risk framings because of path dependency in policymaking (Pierson, 2000). Dunlop (2007) stressed the importance of time in framing risks and argued that this is an interactive process interceded by policies and events from the past. Dunlop (2007) followed Pierson (2000) to recognize how self-reinforcing sequences in an initial risk framing can set the trajectory for the future. Thus, the timing of an issue definition uncovers why certain framings prevail.

I use Dunlop’s (2007) study as my starting point for temporal analysis and rely on historical institutionalism to try and explain the (lack of) divergence from initial cyber risk governance decisions by US policymakers based on early institutional configurations in each governed sector.

Expectations for different institutional configurations across sectors can be derived from the existent cross-national and cross-sector comparative studies on risk governance: Rothstein et al. (2013) found that the presence of multiple decision makers in a fragmented government system is likely to introduce varying philosophical approaches for governing risks. Since the US government is differently structured across sectors, I expect this to influence the way cyber risk framing and governance are developed in each sector. In addition, different regulatory styles across private sectors might yield a range of risk assessment techniques and policy making approaches that characterize certain sectors and not others (Hood et al., 2001). Finally, the overarching regulatory style in the US as a liberal capitalist economy might create public pressure restrict government's interventions to minimal response necessary to correct market failures (Hood et al., 2001). This is likely to encourage self-regulatory and voluntary approaches to risk governance as the most 'rational' basis for regulatory design across sectors.

Thus, the *second* goal of this study is to account for variance in cyber risk framings across sectors and recognize institutional drivers for (lack of) divergence from initial risk framings and policy outputs, despite the 'risk colonization' trend that was identified in early works (Rothstein et al., 2006).

Third, despite extensive writing on cybersecurity governance, we lack a broad empirical understanding of how cyber risks are federally governed in the U.S. across time and space. Nonetheless, policy scholars did address ways in which policymakers have tried to respond to cyber threats, enabling me to derive some trajectories from that literature:

Several scholars studied decision-making structures in this policy arena and emphasized the dominant role of the private sector: a group of scholars canvassed public-private partnerships in protecting critical infrastructures (Eckert, 2005; Quigley and Roy, 2012; Hiller and Russel, 2013; Carr, 2016; Eichensehr, 2017; Boeke, 2017). Underlining the tension between national security and private economic interests, they elaborated the decision-making structure of shared responsibility through private sector leadership. Hiller & Russel (2013) and Harknett & Stever (2011) also discussed the dominance of the business sector and stressed the influence of private actors on government decisions. The central role of the private sector was specified in the regulatory processes that governed the health and financial sectors as well (Johnson, 2015; Thaw, 2013 & 2014). Representatives of private entities were allowed to be part of the rule-making process and utilize their expertise to develop required standards. However, for all other sectors of the broader digital economy, scholars recognized a federal gap. Balitzer (2016) argued that the government left personal

information and corporate assets vulnerable, while Hartzog and Solove (2015) addressed the increasing authority and capacity of the Federal Trade Commission (FTC) as an enforcer of data security standards for sectors that have not been regulated by federal statutes. Therefore, I expect the private sector to have been the dominant actor in crafting cyber risk governance frameworks. For the broader digital economy, I expect the FTC to have fulfilled the federal gap, leading the enforcement efforts of risk governance frameworks.

Another group of scholars studied U.S. cyber governance over time and underscored specific aspects of policy development. Harknett and Stever (2011), for instance, emphasized the voluntary and rather incremental nature of cybersecurity policies, while Russo and Rishikof (2016) highlighted the increasing monitoring & enforcement capabilities for policy compliance after the 9/11 attacks. Finally, Weiss and Jankauskas (2018) tied governance arrangements over time to the nature of the cybersecurity problem and the rationale calculations of policymakers who either delegated or orchestrated third parties in the governance process. They distinguished between policymakers' efforts to either build capacities against cyber-attacks or create resiliency against structural vulnerabilities.

Thus, the *third* goal of this study is to validate and add new findings on the development of cyber risk governance over time. Specifically, in my analysis over time, I expect to find incremental policy changes, increased monitoring and enforcement capacities, and different strategies for mobilizing third parties.

3 - ANALYTICAL FRAMEWORK & METHODOLOGY

I use qualitative research methods to study the framing and governance of cyber risks by US federal policymakers in the past 22 years. I examined in a systematic way my corpus of federal cybersecurity policies (N=30) that includes statutes, executive orders, policy strategies, and secondary legislation of federal agencies between the years of 1996 and 2018 (for the list of analyzed policies see Appendix 1). The time frame represents the period between the very first cybersecurity-related policy that was introduced at the federal level (The 1996 Health Insurance Portability and Accountability Act (HIPAA)) and the last federal policy in the field (The 2018 SEC's guidelines). I chose the U.S. federal cybersecurity policy arena as my case study because it has been evolving for the past 22 years, which allows me to mine the rich seam of cyber risk frameworks and governance practices.

While the risk framings by policymakers might be better assessed by using interviews as well, I exclusively rely on policy texts in order to capture the framings, meanings, logics,

and justifications that policymakers were able to agree upon in each policy output. I follow Schattschneider's (1960) approach who said that "the definition of alternatives is the supreme instrument of power. the antagonists can rarely agree on what the issues are because power is involved in the definition." (p. 68) I wanted to capture the exact reasoning used for each policy and realize what kinds of framings eventually guided policy outcomes.

I analyzed federal policy texts in two phases. *First*, I applied thematic analysis which is an inductive research methodology for 'systematically identifying, organizing, and offering insight into patterns of meanings across a data set' (Braun and Clarke, 2012). This approach is appropriate for this research due to the scarcity of works that have rigorously examined the different risk governance components of cybersecurity policies. The inductive analysis was conducted in two steps. In the first step, I recognized 'key' sentences and assigned code or several codes per sentence, representing its principal content or theme. I ignored general legal language and considered only sentences that added new meanings or additional risk management practices to the text. Therefore, each key sentence contributes to the design of cyber risk governance practices. Then, after removing redundancies and duplicate codes, seven codes that uncover different categories of cyber risk-management emerged:

1.1- Suggested Decision-Making Structure: This category discusses horizontal and vertical principles of authority distribution and levels of engagement between public and private actors in cyber risk management efforts.

1.2 - Actors & Institutions involved: This category stresses the addition of new actors and institutional structures to cyber risk management efforts.

1.3 - Improving Risk Assessment: This category details policymakers' efforts to promote cyber risk assessment in companies. It includes efforts to improve companies' external risk assessment regarding cyber threats in the ecosystem as well as practices to encourage companies to undertake internal risk assessment based on their local networks. External risk assessment is improved by facilitating information sharing and exchange of cyber- threats information, whereas inspection and internal auditing are the practices whereby internal risk assessment is ameliorated.

1.4 - Risk Reduction: This category describes preventive practices to reduce cyber risks in private companies through steps such as standardization.

1.5 - Improving Risk Mitigation: sentences that pertain to this category address governance practices that improve companies' incident response efforts and reporting requirements upon a cyber-breach to quickly minimize damage after a cyber-attack.

1.6 - Increasing Expertise: This category refers to efforts to provide greater expertise in addressing cyber risks, in any part of the risk governance cycle.

1.7 - Monitoring & Enforcement: This category addresses efforts to monitor and enforce cyber risk governance practices, by requiring periodic reporting, posing sanctions, or creating new enforcement agencies.

In the *second* phase of the text analysis, I conducted a deductive analysis based on pre-defined categories derived from Renn's study (2008), to capture the framings of cyber risks in the policy texts, as agreed between policymakers, and based on the first phases in the risk governance cycle – pre-assessment, assessment, characterization and evaluation. My goal was to deductively detect additional categories in the policy texts and understand how policymakers perceive, assess, characterize, evaluate, and all together frame cyber risks. In this phase I was reanalyzing the texts with a special attention to the following categories:

2 - Pre-assessment: Problem Framing – sentences were classified to this category if they indicated policymakers' framings of cyber risks. Such problem framing includes 'the selection and interpretation of phenomena as relevant risk topics' (Renn, 2008, p. 48) and 'the different perspectives of how to conceptualize the issue' (Renn, 2008, p.51). What counts as risk can vary among actors and across regulated sectors. In these sentences we can learn about the values that govern the selection of policymakers' goals, interests, framings and concerns.

3 - Risk Assessment: sentences were classified to this category if they included identification and estimation of the hazards (hazard estimation) or the vulnerability of the targets of cyber risks (vulnerability assessments) as captured by policymakers framing (Renn, 2008, p. 73).

4 - Risk Characterization and Evaluation: this category of sentences includes policymakers' judgement on the seriousness of the risk (characterization) as well as its tolerability and acceptability (evaluation) (Renn, 2008, p. 149) as part of their framing of the risk. Indicators in the texts include statements on the need to take prompt action and the level of threats to targets.

Overall, in the thirty policy texts, 463 key sentences were identified. The two phases of the text analysis yielded a typology of ten categories that were then used to classify key

sentences in each federal policy into a risk governance phase of either pre-assessment, assessment, characterization and evaluation, or risk management. In addition, I drew on secondary sources of information, i.e. the work of scholars who had empirically observed these governance practices (e.g. Eckert, 2005; Thaw, 2014; Hartzog and Solove, 2015) – to further understand how federal policies shape cyber risk governance frameworks for each sector.

4 – U.S. FEDERAL POLICY FRAMEWORKS FOR CYBER RISK GOVERNANCE

In the span of twenty-two years, U.S. federal policymakers have embraced three distinct framings, and consequently, deployed three different frameworks for cyber risk governance. These frameworks vary across private sector domains such as critical infrastructures, health and financial service providers, and non-critical sectors of the broader digital economy.

Critical infrastructures are defined by the Department of Homeland Security as ‘sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.’ (DHS.gov). Health and financial service providers are defined as the sectors the process personal health and financial information. ‘Non-critical’ sectors are defined by the Department of Commerce as ‘sectors that include functions and services that create or utilize the Internet or networking services have large potential for growth and vitalization of the economy,’ but fall outside the classification of covered critical infrastructure as defined by the Department of Homeland Security (Department of Commerce, 2011).

The thirty policy texts in question include eleven federal statutes, seven executive orders and presidential directives, four federal agencies guidelines, four federal strategies, three agency rules, and one commission report. Within these policy texts, 463 key sentences were identified and categorized: 76 of them were coded to the pre-assessment phase, 18 were coded to the risk assessment phase, 30 to the risk characterization and evaluation phase, and 339 to the different sub-categories of risk management. It is worth mentioning that these cybersecurity policy texts usually addressed additional topics, so only specific portions of them were coded and key sentences were extracted.

4.1. Critical Infrastructures

I analyzed thirteen federal policies that had broached cyber risks in critical infrastructures between the years of 1997 and 2015. Within these texts, 226 key sentences were identified and categorized. Fifteen of them specify how policymakers pre-assess and frame cyber risks in the domain of critical infrastructures. Twenty-Seven sentences reveal policymakers' characterization and evaluation of cyber risks in critical infrastructures. Finally, the majority of key sentences, 184 out of 226, expounded how the federal government influenced cyber risk management in private operators of critical infrastructures.

Table 1 below summarizes how the protection regime of critical infrastructures has been designed according to different phases in the risk governance framework. In the following paragraphs I discuss how public policies shape the different risk governance phases.

<TABLE 1 HERE>

Pre-assessment: Problem Framing

Protection from cyber risks in critical infrastructures was consistently framed as a national security priority and a vital interest of the state. The Marsh Commission Report (1997) highlighted the dependency of the nation on its infrastructures, the essential role of infrastructures in public health and safety, and their effect on social well-being, the economy, and national defense. This framing was used after the 9/11 attacks as well, but this time with a greater sense of urgency to act (Eckert, 2005). In 2003, The Department of Homeland Security (DHS) used the word terrorism to describe potential attacks against critical infrastructures and viewed their protection as a supreme national priority. A decade later, President Obama issued PDD-21 and adopted a similar framing, arguing that critical infrastructures are 'vital to the nation's safety, prosperity, and well-being, as well as to public confidence.' In the years of 2014 and 2015, federal statutes and executive orders used the word 'terrorism' again and adopted similar problem framing.

Risk Assessment: Vulnerability Assessment and Hazard Estimation

Policymakers relate to cyber risks in critical infrastructures as a new dimension of vulnerability. In 1997, policymakers acknowledged that the threat can come from everywhere – 'a personal computer and a telephone connection to an Internet Service Provider anywhere

in the world are enough to cause harm’ (Marsh Commission, 1997, p. 10). Policymakers described how easily an adversary can bypass national defense to directly attack U.S. critical infrastructures. In the years of 2001 and 2002 policymakers enumerated the vulnerable sectors that had become susceptible. When estimating the hazards, no clear evidence was available. The Marsh Commission stated that it found ‘no evidence of an impending cyber attack which could have a debilitating effect on the nation’s critical infrastructures’ (p. 1). In 2003, the DHS listed the different hazards that were theoretically feasible following a cyber-attack on critical infrastructures that might disable essential public services, damage the orderly functioning of the economy, and disrupt key vital resources.

Risk Characterization and Evaluation:

Risks were characterized as serious and alarming. In 1997, they were perceived as ‘unprecedented national risks’ that the nation had ‘little defense against.’ The consequences were described as severe and ‘devastating as a backpack full of explosives.’ (Marsh Commission, 1997, p. 10). In 1998, President Clinton had viewed these risks as risks for military power as well, and in 2003 the DHS used the word terrorism for the first time in this context and argued that such risks could cause mass casualties, catastrophic health effects, and damage to public morale and confidence. The consequences were compared to those from weapon of mass destruction (WMDs). Ten years later, president Obama viewed the risk as a constantly growing one, which was still one of the ‘most serious national security challenges we must confront’ (EO 13636, 2013). The consequences were viewed as catastrophic for vital domains such as health, safety, economic security, and national security, and risks were evaluated as ‘unacceptable’, requiring ‘immediate action.’

Risk Management:

The majority of coded sentences – 81 percent – addressed risk management practices. Out of 184 key sentences, 27 subsumed two different codes, yielding 211 sentences (or rather statements), which were then assigned to different risk management categories.

Fifteen percent of the coded sentences conveyed the *suggested decision-making structure* to protect critical infrastructures. With approximately eighty-five percent of U.S. infrastructures privately owned or operated (Harrell, 2017), the paradigm of shared responsibility with private sector leadership has dominated the policy agenda. From 1997, shared responsibility was perceived as ‘the only sure path to protected infrastructures’ and as a challenge to the ‘conventional way of thinking about government and private sector

interaction’ (Marsh Commission, 1997, p. 1). Private owners should take the steps to protect themselves and the government ought to facilitate pertinent information sharing practices to assist them. Expressions such as ‘genuine partnerships’, ‘trust’, and ‘mutual responsibilities’ were commonly used, even though these risks were framed as national security risks for which the state was traditionally the main policy actor. Policymakers viewed private owners and operators of critical infrastructures as those who had the knowledge, access, and technology to defend themselves, while the federal government was regarded as an intelligence resource with law enforcement capabilities that could deter potential threat actors. Increased government regulation was deliberately avoided. Market incentives were viewed as ‘the first choice for addressing the problem... regulation will be used only in the face of a material failure of the market to protect the health, safety, or well-being of the American people’ (PDD-63, 1998). The broad federal mandate to private operators continued to 2013.

Third of the risk-management sentences detailed new *institutions & actors to be involved* in cyber risk governance, as the government experimented with various institutional structures to find the most suitable one for defending critical infrastructures. In 1997 and 1998, owners and operators were assigned responsibility to self-set their protection measures, while intelligence agencies were deemed responsible for facilitating and sharing relevant information. Each infrastructure sector had to select a sector coordinator to work with the government with a designated Sector Liaison Official in the federal department. Moreover, each department had to nominate a Chief Infrastructure Assurance Officer (CIAO) that was responsible for the department’s critical infrastructure protection mission, and a new Senior Director for Infrastructure Protection was appointed, becoming part of the National Security Council (NSC) staff. In 1998, the FBI was ordered by President Clinton to expand its National Infrastructure Protection Center (NIPC) and sanitize law enforcement and intelligence information about cyber threats. The Department of Defense (DoD) and Department of Commerce (DoC) were ordered to work with the private sector and provide expertise to develop security-related best practice standards. In 2001, additional coordination bodies were established – a senior executive branch board to coordinate federal efforts, and the National Infrastructure Advisory Council (NIAC) that advised the president. The Department of State and law enforcement agencies were also engaged in developing programs for increasing enforcement against cyber criminals. Through the 2001 Patriot Act, the government established the National Infrastructure Simulation and Analysis Center (NISAC) to serve as a source of national competence while catering to operators and private

owners. In 2002, the Administration decided to eliminate the infrastructure protection office within the NSC and to create the DHS. With its establishment, most responsibilities for information sharing and infrastructure protection were carried out through the DHS' Under Secretary for Information Analysis and Infrastructure Protection. The new Under Secretary had to work with the Director of Central Intelligence (CIA) to ensure that intelligence or other information related to terrorism could be accessed by the relevant federal entities. In 2009, the DHS launched a new National Cybersecurity and Communications Integration Center (NCCIC), which served as a 'Watch and Warning Center' to address threat and incidents affecting critical infrastructures. The unified entity brought together the U.S. Computer Emergency Readiness Team (US-CERT) and the National Coordinating Center for Telecommunications (NCC). In 2013, president Obama restated the responsibility of federal departments and agency heads for the security of their respective critical infrastructures while authorizing the DHS to serve as the 'meta-regulator' and provide guidance and coordination for overall efforts. The protection of national monuments lay with the Department of Interior whereas the Nuclear Regulatory Commission (NRC) was vested with the protection of commercial nuclear power reactors through cooperation with DHS, DOJ, the Department of Energy, and the Environmental Protection Agency. The Federal Communications Commission (FCC) was vested with the responsibility to guard communications' infrastructures. President Obama also named two national critical infrastructure centres – one for physical infrastructure and one for cyber infrastructure. They served as focal points for critical infrastructure partners to obtain situational awareness and integrated actionable information to protect the physical and cyber aspects of critical infrastructure. President Obama's Executive Order 13636 also required the Attorney General, The Secretary of Homeland Security, and the Director of National Intelligence to issue reports on emerging cyber threats. In 2015, President Obama published sanctions against cyber criminals who posed a threat to U.S. critical infrastructures, enforceable by the Secretary of Treasury.

A quarter of the risk-management sentences address practices to *improve external and internal risk assessments* of critical operators. The lack of threat information was perceived as fundamental to protection efforts. Private actors were reluctant to share information and did so only after they had suffered substantial loss or had been convinced of imminent danger to the continuity of their operations. In 1998, President Clinton ordered the opening of a national center to warn of significant infrastructure attacks – the National Infrastructure Protection Center (NIPC) – based on law enforcement and intelligence information. The voluntary creation of private sector information sharing and analysis centers (ISACs) was

highly encouraged. When the DHS was established in 2002, information sharing responsibilities were consolidated. The DHS has had a central information sharing program - the Cyber Information Sharing and Collaboration Program (CISCP), providing information sharing partnerships between enterprises and the department at no cost. The DHS set up the U.S. Cyber Emergency Response Team (CERT) center to provide the latest computer-related threats information. In order to incentivize sharing, voluntary information sharing was protected and could not be used against a company. In 2013, the FBI was requested to lead 'federal efforts for collecting, analysing, and disseminating cyber threat information through a dedicated National Cyber Investigative Joint Task Force.' The Director of National Intelligence (DNI) furnished intelligence assessments. With these efforts, unclassified reports of cyber threats were to be provided by the intelligence community, and private sector experts were brought into federal service on a temporary basis to advise on the best structure and type of information most useful to operators of critical infrastructures. In 2015, President Obama further encouraged voluntary information sharing by setting in train mechanisms to improve the capabilities of private Information Sharing and Analysis Organizations (ISAOs), allowing private operators to better partner with the federal government.

Risk Reduction steps are discussed in nine percent of the sentences. Nonetheless, the approach is mostly voluntary and provides discretion to private operators and regulators in each critical sector over if and how to implement standards. Since 1997 policymakers have recognized the importance of 'protecting our infrastructures against cyber threats before they materialize and produce major system damage' (Marsh Commission, 1997, p. 5). Owners of critical infrastructures were strongly encouraged to take prudent steps to reduce or completely eliminate their vulnerabilities. Business groups, however, noted that shareholders had little financial incentive to invest in security beyond their stake in the corporation, and thus shareholders would have supported security investments only to the extent that to do so had been profitable (Eckert, 2005). In 2007, the need for mandatory risk reduction steps in the chemical sector was codified in the 2007 DHS Appropriations Act. In 2013, President Obama pushed this a step further and ordered the development of the 'Cybersecurity Framework' by the National Institute for Standards and Technology (NIST) to 'reduce cyber risks to critical infrastructure' (PDD-21, 2013). The Secretary of Homeland Security was ordered to establish a voluntary program to support the adoption of NIST's Cybersecurity Framework by private operators. Sector-specific-agencies were called upon to guide implementation, and agencies charged with the regulation of critical infrastructures were supposed to review the framework to determine whether existing regulatory requirements were sufficient. The degree to which

these activities were obligatory and enforced varied across sectors. For instance, nuclear power plants had to meet very specific standards for vulnerability assessment and take necessary actions enforced by the NRC. In the electricity sector, it was the non-profit self-regulation body, The North American Electric Reliability Corporation (NERC), that issued and enforced mandatory requirements. In contrast, in sectors such as information and communications or oil and gas, these measures were voluntary rather than compulsory.

Risk mitigation practices to minimize the damage after a cyber incident were addressed by six percent of the sentences. In 2001, President Bush ordered the Attorney General to increase support to computer forensic laboratories and help companies obtain and compile evidence of criminal activity. President Bush established the National Infrastructure Simulation and Analysis Center (NISAC) to serve as a source of national competence and respond to cyber incidents. The DHS Act of 2002 heralded the establishment of ‘NET Guard’— local teams of volunteers with expertise in relevant areas to assist in responding and minimizing cyber damages. In 2013, President Obama ordered DHS to ‘demonstrate a near real-time situational awareness capability for critical infrastructure...mitigating damage or reducing further degradation of a critical infrastructure capability throughout an incident’ (PDD-21, 2013).

Expertise issues are mooted in five percent of the sentences. The need to increase expertise was raised for the first time after the 9/11 attacks. President Bush ordered extensive modelling for evaluating appropriate mechanisms to ensure the stability of complex infrastructure systems. In 2002, one of DHS’ roles was to provide technical assistance to the private sector. In 2013, President Obama called for the engagement of the DoC in efforts related to critical infrastructures in an attempt to keep services and products accessible and timely. To better utilize information sharing practices, President Obama also requested ‘subject matter experts’ to get involved in rendering advice regarding the content, structure, and type of available information to reduce and mitigate cyber risks.

Finally, four percent of the sentences describe *monitoring and enforcement* processes. In 2001 enforcement capabilities increased through the establishment of a national network of electronic crime task forces. In 2013 president Obama required annual reporting from sector-specific-agencies on critical infrastructure assurance, and the extent to which they complied with NIST’s Cybersecurity Framework. In 2015 enforcement capacities were boosted as President Obama, through the Department of Treasury, sanctioned the entry and financial resources of individuals who were engaged in cyber-crimes against critical infrastructures.

4.2. HEALTH AND FINANCIAL SERVICE PROVIDERS

I analyzed eight federal policies that address cyber risks pertaining to healthcare and financial service providers between the years of 1996 and 2013. Within these texts, 52 key sentences were identified and categorized. Most sentences, 46 out of 52, address risk management practices, and six describe how policymakers frame the problem. Since they share the same risk framing and hierarchical regulatory style, I chose to consolidate cyber risk governance in healthcare and financial service providers under a single regime. Some differences are nonetheless evident, and I address them in detail in the paragraphs below.

Table 2 summarizes how the protection of health and financial sectors was designed according to different phases in the risk governance framework. In the following paragraphs I discuss how public policies shape the different risk governance phases in these sectors.

<TABLE 2 HERE>

Pre-Assessment: Problem Framing

There is only little evidence in the data on how policymakers framed cyber risks in these sectors. Still, from the coded sentences I witnessed how policymakers from both sectors share similar framings and perceive cyber risks as a problem of protecting personal information. For financial service providers, the 1999 Gramm–Leach–Bliley Act (GLBA) framed the problem as a problem of privacy for which Congress must ensure ‘that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers’ personal information.’ This framing was updated in 2013 by the Securities Exchange Commission (SEC) and the Commodity Futures Trading Commission (CFTC) that viewed the growth and expansion of information technology as an increased threat to ‘the integrity and privacy of personal information... the federal government should take steps to help individuals protect themselves from risks of theft, loss, and abuse of their personal information.’ For health service providers, the FTC defined in 2009 breach of security as an ‘acquisition of identifiable health information without the authorization of the individual.’ The problem was framed as a problem of protecting ‘personal health records’ and there was a need to prevent the exposure of sensitive information that jeopardized individuals’ privacy.

Risk Management:

The suggested *decision-making structure* is hierarchical but provides a lot of influence to industry stakeholders. In the healthcare sector, administrative agencies have run the gamut of regulatory responsibilities. In 1996, the Secretary of Health and Human Services (HHS) was recognized as the ultimate regulatory authority in this domain, but private actors were allowed to be part of the rule-making process. In the financial sector, the design of policies and enforcement mechanisms has taken place through traditional and hierarchical financial regulators. At the same time, the SEC provided flexibility to private actors to decide which identity theft risks were most apposite to their operations and suggested that a designated individual within the corporation be responsible for overseeing those risks.

In terms of *actors and institutions to be involved*, the healthcare industry was regulated through a single department, HHS, while financial service providers were regulated through a variety of legacy financial regulators: the 1999 GLBA incorporated Federal banking agencies, The National Credit Union Administration, the Secretary of Treasury, the FTC, SEC, CFTC, and National Association of Insurance Commissioners as relevant actors to guide and enforce regulations. The 2010 Dodd-Frank Wall Street Reform and Consumer Protection Act created the Consumer Financial Protection Bureau (CFPB) as an additional monitoring and enforcement entity for information security in the financial sector. The CFPB has had rulemaking, enforcement, and supervisory powers over many consumer financial products and services, including the authority to develop identity theft guidelines. It could have also issued rules declaring certain acts or practices to be unlawful. Additional important enforcement agency was the FTC. It was established in 1914 to protect consumers from deceptive or unfair business practices (Section 5 authority) and has used this authority to bring enforcement actions against companies that failed to protect consumers' personal information. The 1999 GLBA gave the FTC direct authority over data protection in the financial services industry. Previously, many entities in this industry such as banks were explicitly excluded from the FTC's Section 5 authority.

Risk Assessment for health service providers was addressed through the requirement for periodic audits by the 1996 HIPAA. For financial service providers, companies' risk assessment processes were addressed through the 2002 Sarbanes–Oxley (SOX) Act that required an assessment of the effectiveness of 'internal control structure and procedures', including information security controls. At the same time, risk-assessments of external cyber threats have developed through DHS' Financial Sector Information Sharing and Analysis Center (FS-ISAC). It was originally used for critical financial services, and now provides membership-based access to cyber threats.

Healthcare policies have emphasized *risk reduction* measures that are apparent in 24 percent of the analyzed risk management sentences. These measures include standardization of both privacy and information security. The standards were to be developed with industry stakeholders. In 2009, the scope of regulated entities has increased as business associates of covered entities became directly liable for information security. For financial service providers, *risk reduction* steps were mainly addressed by the 1999 GLBA that established appropriate standards for financial institutions with regard to the administrative, technical, and physical safeguards, endeavoring to ensure the security and confidentiality of customer records by guarding against any anticipated threats or hazard to the security or integrity of information records. The statute left a great deal of flexibility for corporate managers to choose among the methods to use and outcomes to achieve based on their risk-management planning (Thaw, 2014).

Healthcare policymakers also addressed *risk mitigation* measures, which are apparent in 21 percent of the sentences. The 2009 FTC's health breach notification rule specified the required steps upon a discovery of a data breach, including setting in motion notifications and measures to mitigate risk and minimize damage no later than '60 calendar days after the discovery.' The 2013 HITECH supplanted the breach notification rule harm's threshold with a more objective standard, mandating HHS Secretary to post a list of covered entities that had experienced breaches involving more than 500 individuals on the Department's website. Such breaches were to be immediately reported to the Secretary. *Improving risk mitigation* in financial institutions was addressed by the 2013 SEC and CFTC rule to mitigate identity theft. The rule required financial institutions to establish a program to minimize damage from identity theft.

Most sentences that have to do with healthcare policies, 45 percent, deal with *monitoring and enforcement* practices. In the 1996 HIPAA, the Congressional Committee was asked to post a report to Congress on the implementation of the act. Furthermore, the 2009 HITECH introduced civil pecuniary penalties for violations of HIPAA, establishing categories of violations and respective penalties based on the nature and extent of the violation. The Act also allows an individual who believed a covered entity was not complying with HIPAA to file a complaint. In terms of monitoring, the HITECH Act required the HHS Secretary to conduct periodic audits to ensure that covered entities and business associates abide by the Law. The HITECH Act also required the Secretary to submit annual reports to Congress and summarize the number and types of complaints received, enforcement actions, audits preformed, and plans for improving compliance. In 2013,

HIPAA's Enforcement Rule changed to incorporate further, tiered civil pecuniary penalty structure.

In financial federal policies, *monitoring and enforcement* was also addressed by the majority of sentences – 44 percent. In the 1999 GLBA, enforcement was vested in the relevant federal financial regulators, state insurance auditors, and the FTC. The SOX 2002 Act required to include information security controls in regular financial reporting of companies. Section 404 of the act provided the framework for SEC to become an active federal cybersecurity regulator over publicly-traded companies. The 2010 Dodd-Frank Act referred to CFPB and SEC as the authorities to prescribe regulations of information security based on GLBA, and specifically ordered the CFPB to enforce a ban on unfair, deceptive, or abusive acts or practices and complement FTC's efforts in the field in that regard. Monitoring and enforcement efforts were addressed further by the 2013 SEC and CFTC Rule, as it required effective oversight of the arrangements of financial service providers.

4.3. NON-CRITICAL SECTORS

I analyzed nine federal policies that address cyber risks in non-critical sectors between the years of 1997 and 2018. These sectors are defined by the 2011 DoC's strategy for cybersecurity that recognized a variety of business sectors that fall outside the classification of covered critical infrastructures, but 'create or utilize the Internet and have a large potential for growth, entrepreneurship, and vitalization of the economy.' (p. iv) Within these texts, 185 key sentences were identified and categorized. Fifty-five of them lay down how policymakers pre-assess and frame cyber risks. Eighteen sentences reveal policymakers' characterization and evaluation of the risks, and finally, 109 out of 185 detail risk management practices.

Table 3 below summarizes how the protection of non-critical sectors was designed according to different phases in the risk governance framework. In the following paragraphs I discuss how public policies shape the different risk governance phases in these sectors.

<TABLE 3 HERE>

Pre-Assessment: Problem Framing

Thirty percent of the sentences analyzed describe policymakers' framing of the problem. The risk framing has been institutionalized since the 1997 Framework for Global Electronic

Commerce. In this framework, cyber risks were framed as challenges for economic development and to the ‘new models of commercial interactions...that has the potential to revolutionize commerce by dramatically lowering transaction costs and facilitating new types of commercial transactions.’ Privacy and data security in the network environment were perceived as ‘essential for people to feel comfortable doing business...if Internet users do not have confidence that their communications and data are safe...they will be unlikely to use the Internet on a routine basis for commerce.’ In 2010 and 2011, this problem framing persisted in two DoC’s strategy documents. These texts depicted the Internet as central to the economy but challenged by the need to secure a vast amount of stored, sensitive personal information . Therefore, commercial data privacy and security were portrayed as an ‘urgent economic and social matter,’ and cybersecurity protections were described as ‘critical to ensuring that the Internet fulfills its social and economic potential.’ Without proper cybersecurity, customers could be lost and trust in the online environment could be eroded. The commercial importance of cybersecurity was also limned in president Obama’s 2011 Strategy for Trusted Identities that looked upon cybersecurity as critical for prosperity and productivity. In 2015, the SEC identified cybersecurity as a ‘public interest and appropriate for the protection of investors and the maintenance of fair and orderly markets to assure the economically efficient execution of transactions.’ Policymakers perceived cybersecurity as a practice that would advance the goals of the national market system. This paradigm has continued into 2018 through SEC’s guidelines that describe how cybersecurity risks pose ‘threats to investors and capital markets.’ Investors, the general public and the economy are viewed as dependent upon ‘security and reliability of information and communications technologies.’

Risk Assessment: Vulnerability Assessment and Hazard Estimation

Risk Assessment by policymakers is described by five percent of the sentences. In the DoC’s strategy from 2011, policymakers provided hazard estimates that explicated the exploitation of the interconnectedness of the Internet in the form of, inter alia, targeted attacks for stealing, manipulating, destroying, or denying access to sensitive data. In 2018 SEC’s guidelines, hazard estimation also broached ‘substantial costs and negative consequences’ that a company might face due to the ‘theft of financial assets, intellectual property, or other sensitive information belonging to companies, their customers, or their business partners.’ These costs consisted of remediation costs, repairs of system damage, and incentives to customers or business partners to maintain relationship after an attack. Damage to a company’s competitiveness, stock price, and long-term shareholder value in the aftermath

were also mentioned. With regard to vulnerability assessment, policymakers noticed how the evolution of U.S. securities markets in recent years has become almost entirely electronic and highly dependent on sophisticated trading technologies, which made it vulnerable. Policymakers based their fears on incidents of delayed trading, halted trading, and errors in trading due to cyber risks that had come about in the past.

Risk Characterization & Evaluation:

Risk characterization and evaluation is described by seven percent of the sentences analyzed. In 2010 DoC's strategy, cyber risks in non-critical systems were viewed as increasingly acute because 'the U.S. economy and society depend more heavily on broadened use of personal information that can be more easily gathered, stored, and analyzed.' In the 2011 strategy, cyber risks were described as 'exponentially growing...with tens of thousands of new malware threats every day that had more than doubled since 2009.' Non-critical sectors were portrayed as 'sectors at great risk that can put others at great risk if private owners do not adequately secure their networks and services... the constantly evolving nature of threats and vulnerabilities not only affects individual firms and their customers, but collectively poses a persistent economic and national security challenge.' SEC's policy from 2015 further elaborated on the tolerability of the risk: 'a seemingly minor system problem at a single entity can quickly create losses and liability for market participants, and spread rapidly across the national market system, potentially creating widespread damage and harm to market participants, including investors.' The urgency to act upon cyber risks was also evident in 2011 Obama's strategy that articulated a 'compelling need to address these problems as soon as possible.' SEC's regulation from 2015 argued that 'it is necessary and appropriate at this time to address technological vulnerabilities... of the core technology of key U.S. securities market entities.' SEC's guidelines from 2018 have further accentuated the 'frequency, magnitude, and cost of cybersecurity incidents' and how critical it has been for public companies to immediately take all necessary actions to inform investors about material cybersecurity risks and incidents.

Risk Management

The majority of coded sentences – 59 percent – address risk management practices for coping with cyber risks in non-critical sectors. Out of 109 key sentences, six comprise two different codes, which translates to 115 sentences (or more precisely statements) to which different risk management categories have been assigned.

The *suggested decision-making structure* is discussed by 34 percent of the sentences. In 1997, policymakers called for a non-regulatory, market-oriented approach, to ‘support global businesses and commerce.’ The private sector was considered the main leader since ‘innovation, expanded services, broader participation, and lower prices will arise in a market-driven arena, not in an environment that operates as a regulated industry.’ The role of the government as a facilitator was also described in the 2010 & 2011 DoC strategies for the digital economy: ‘industry codes would develop faster and provide more flexibility than legislation or regulations...our approach recognizes a key role for government in convening stakeholders and leading the way to policy solutions that protect the public interest...but pure government prescription is a prescription of failure.’ Policymakers highlighted the important role of incentives to ‘motivate all parties in the Internet economy to make appropriate security investments...that are carefully balanced to heighten cybersecurity without creating barriers to innovation, economic growth, and the free flow of information.’ In the 2011 Obama’s strategy for trusted identities, the private sector was required to lead the development; it was specifically stated that ‘the government will neither mandate that individuals nor that companies use the Identity Ecosystem credentials.’ Some cracks in this self-regulation paradigm was evident in the 2015 SEC’s Systems Compliance and Integrity (SCI) regulation, which on the one hand praised SEC’s voluntary approach to security, but on the other hand noted how such approach ‘constrains the Commission’s ability to assure compliance with standards.’

Actors and institutions were discussed by seven percent of the sentences. The private sector was perceived as the main resource for coping with the risks. In the 2010 DoC’s strategy, The DoC and FTC also have been assigned important roles in ‘reducing barriers to digital commerce, while strengthening protection for cybersecurity’. Specifically, the FTC has made data security self-regulation more meaningful through its enforcement of the promises that companies made about the way they collect, use, and protect data. It has filled the regulatory gap over large industries that have not been regulated by federal data protection statutes. Instead of imposing top-down rules all at once, the FTC has integrated itself into a largely self-regulatory approach, gradually developing it into a more robust regulatory system for enforcing norms that have been developed by the industry (Hartzog and Solove, 2015). Additional actors emerged in the 2015 Cyber Information Sharing Act (CISA). The Act addressed information sharing and urged security actors – DHS, DoD, and Attorney general – to develop and issue procedures to facilitate and advance timely sharing of

cyber threats. Over the years, SEC has become an important regulator of public companies with respect to cybersecurity owing to its reporting requirements.

Risk Assessment is addressed by 17 percent of the sentences and is facilitated through voluntary information sharing programs with the involvement of the government, and specifically DoC and DHS. These practices were viewed as ways to ‘increase defensive knowledge’ (DoC Framework, 2011). In 2014, a dedicated memo signed by The Department of Justice and the FTC was issued to remove anti-trust restrictions over information sharing practices. The passage of CISA in 2015 also aimed to encourage voluntary and timely sharing of cyber threat information, something which came in conjunction with authorization for owners to monitor their private networks. The Act provided liability protections against privacy suits ensuing from the monitoring or the sharing of threat information with the government. Within this legislation, The DHS Center – The National Cybersecurity and Communications Integration Center (NCCIC) – may ‘enter into a voluntary information sharing relationship with non-Federal entity.’ SEC SCI’s regulation in 2015 has advanced internal risk assessment for SCI organizations by requiring quarterly review reports of the systems. Enforcement actions by CFPB has fostered further internal data-security risk assessments.

Steps for *Risk Reduction* are described by 18 percent of the sentences. They include standardization practices, which were viewed in 1997 as ‘critical in the long term...they encourage competition and reduce uncertainty in the global marketplace...but can also lock-in outdated technology.’ In the years of 2010 and 2011, the DoC recommends ‘the consideration of the broad adoption of comprehensive Fair Information Practice Principles (FIPPs),’ and that ‘the U.S. government and stakeholders come together to promote security standards.’ The 2011 strategy acknowledged that NIST’s Cybersecurity Framework have become the ‘leading source for cybersecurity protection for the private sector,’ and called for rapid development and implementation of sector-specific, consensus-based, codes of conduct. The DoC identified the incapacity of small sectors to establish their own voluntary codes of conduct and underscored its role to convene stakeholders and facilitate the development of proper codes. The DoC urged passage of a national cyber-breach notification law, ‘because requiring such disclosures may encourage firms to take more care to avoid breaches in the first place.’ SEC’s policy on SCIs required the establishment of written policies and producers to ensure in advance that systems have adequate capacities to function in the current threat landscape. The first CFPB enforcement also emphasized the importance of adopting reasonable and appropriate data-security measures to protect ‘consumers’ personal

information on its computer networks and applications.’ In 2018, SEC guidelines specifically asked public companies to ‘consider preventive measures in the context of a cyber event.’

Risk Mitigation steps appear in ten percent of the sentences. The 2010 DoC strategy specifically called for federal data security breach law that would set national standards for steps to be taken following cyber incidents, and ‘provide clarity to individuals regarding the protection of their information throughout the United States, streamline industry compliance, and allow businesses to develop a strong nationwide data management strategy.’ In 2018, SEC set forth the importance of setting an appropriate time frame for the disclosure of cyber risks and incidents that ‘provide an appropriate method of discerning the impact that such matters may have on the company and its business.’ The risk was regarded as risk to investors. Companies were expected to disclose cybersecurity risks and incidents that were material to their investors and such disclosures should include ‘specific information that is useful to investors to mitigate their risks.’

Expertise issues were rarely discussed in these policies. They were clearly mentioned once in the 2011 DoC strategy that called on the DoC to promote research and development of technologies that would increase protection.

Issues of *monitoring and enforcement* are discussed in 13 percent of the sentences. FTC’s role in challenging deceptive and unfair acts in the market was described by the 2011 DoC strategy as vital to companies’ voluntary efforts to implement specific best practices. Hertzog and Solove (2015) discussed the significant role of FTC as a ‘standard codifier in this sector.’ Instead of creating new norms and standards, the FTC waited until norms and standards have developed to begin enforcement. The 2011 DoC strategy substantiated the 2002 SOX Act that ‘requires management to certify internal controls are in place to address a wide range of issues including data security.’ In 2015, SEC required SCI entities to participate in scheduled testing of the operation of their business continuity and disaster recovery plans. This would help monitor compliance in advance and take preventive steps if needed. In 2016, CFPB’s enforcement act explicated how false representations of data security practices violated the Consumer Financial Protection Act of 2010. The CFPB then ordered further civil pecuniary penalties in cases of violation: ‘Respondent must pay a civil pecuniary penalty of \$100,000 to the Bureau.’ In 2018, SEC discussed the expectation from companies financial reporting ‘to provide reasonable assurance that information about the range and magnitude of the financial impacts of a cybersecurity incident would be incorporated in financial statements on a timely basis.’

5 – COMPARATIVE ANALYSIS: CYBER RISK GOVERNANCE ACROSS SECTORS AND OVER TIME

I demonstrated how federal cybersecurity policies created three distinct risk frames and governance outputs across sectors. I found that each regime was based on different perception, characterization, and evaluation of cyber risks that constituted the overall risk framing by policymakers. These different framings only partially influenced the various decision-making structures and risk-management strategies as described in table 4 below.

<TABLE 4 HERE>

For the pressing and potentially catastrophic issue of protecting *critical infrastructures*, early policies from 1997, and those that were enacted after the 9/11 attacks, contained the majority of risk framing sentences. Policymakers tried to embrace a rather revolutionary approach, one that was based on their assessment that a new dimension of vulnerability had emerged. This required immediate action before it affected fundamental aspects in society such as public health, safety, and economic security.

Still, despite an alarming risk framing, government intervention included only limited number of mandatory requirements. A new model of shared public-private responsibility had developed and persisted over time, as traditional top-down regulation has been avoided for the most part. The private sector was perceived as primarily responsible for protection practices in critical sectors. Hence, coercive risk reduction steps and monitoring and enforcement capacities were carefully designed, in a rather late stage of policy development (2013), bringing private influence into play.

This discrepancy between the sense of urgency over risks from critical infrastructures that was evident already in 1997, and the late steps taken by policymakers to require risk reduction can be explained by the fragmented structure of the critical infrastructures' domain. With the proliferation of government agencies and decision makers over critical sectors in the US, policymakers had to create governance structures that align with existing industry practices. In addition, the variety of regulatory styles in each critical sector led to the creation of shared models of responsibility that go along with the US capitalist regulatory approach to encourage self-regulatory and voluntary market practices. Still, in its role as an enabler and facilitator of information sharing initiatives, the government laid out significant resources and involved more than dozen federal branches in its efforts, this time in accordance with the way these risks were perceived.

For *health and financial service providers*, cyber risks were framed as traditional problems of privacy. According to policymakers, the main role of the government was to address the potential theft, loss, and abuse of personal information in these sectors. Therefore, hierarchical and legacy institutions were authorized to federally govern cybersecurity. Accordingly, significant efforts were expended in the more coercive aspects of risk-management: risk reduction and mitigation steps as well as monitoring and enforcement capacities. Within this framework, companies were required to implement preventive measures and disclose cyber breaches, the scope of regulated entities increased over time, civil penalties were introduced, and a growing number of federal agencies augmented their enforcement authority.

The traditional regulatory styles in health and finance domains – of capable and influential regulatory agencies – led the way for policymakers to design vertical, top-down governance practices, that pushed for coercive risk reduction steps. Despite this rather traditional approach, there was much room in the policy process for industry actors to craft standards and compliance requirements. It seems that policymakers acknowledged the lack of expertise in the government and the need to work with industry experts. In addition, the fragmented regulatory landscape of financial regulators that include multiple decision makers led policymakers to allow representation of the various approaches in the initial phases of policy design.

For *non-critical sectors*, cyber risks were framed as a serious obstacle for economic development. They undermined consumer confidence and damaged companies' reputation and competitiveness. Based on experience and evidence, policymakers addressed market participants and investors as those who were at a great risk, and instructed companies to take immediate steps to unleash the potential of the digital economy.

Yet again, similar to risk governance frameworks for critical infrastructures, the alarming risk framing did not lead to significant government intervention in market practices. Vice versa, the suggested decision-making structure was completely market- and incentives-based, working in conjunction with traditional actors from the commerce sector – the FTC, DoC, and SEC. Accordingly, the government recommended rather than mandated risk reduction and mitigation steps: risk reduction was encouraged to create market clarity and competition, and timely disclosure of breaches was advocated to safeguard investors. The main and almost only domain for government intervention was through monitoring and enforcement of self-regulation practices. These capacities improved with the growing scope of FTC's involvement and competences over time, and the mandate given to SEC and CFPB

in this policy area. This also included the introduction of civil pecuniary penalties for non-compliance. In recent years, the government has started to copy information sharing practices from the critical infrastructures sector. Traditional security agencies – DHS, DoD, and DoJ – have become more involved, and legal restrictions to information sharing have been removed.

This discrepancy between the alarming risk framing and governance outputs can be explained by the fragmented federal structure of the US government system and the role that states fulfill in regulating data security in these sectors. According to the National Conference of State Legislatures, half of US states have laws that require mandatory data security practices in non-critical sectors (NCSL, 2019). The number of states with these types of laws has doubled since 2016, reflecting growing concerns about computer crimes in ways that fit the framings of those risks. Moreover, the liberal capitalist regulatory style in the US can explain why the government has yet to pass a binding federal law that requires data security practices from all companies across the economy. The federal government relies on states' intervention and market forces, and does not diverge from traditional liberal regulatory norms in those sectors.

A second set of comparative findings arises from tracing which risk-management practices have been addressed by policymakers over time. The *critical infrastructures protection* regime had been initially designed in 1997-1998 and remained rather stable with two punctuation points: (1) post 9/11, the government advanced new institutional structures, introduced new agencies, improved operators' risk assessment, aiming to increase expertise and mitigation efforts. (2) In 2013, the Obama Administration passed significant executive orders that comprehensively addressed risk-reduction steps for the first time for these sectors, engendering new institutional structures and addressing expertise and risk assessment issues after more than a decade. The risk was consistently perceived as serious and alarming, but decision-making structures stayed rather the same. Initial issue definition and the persistence of risk governance practices in critical sectors highlight the significance of self-reinforcing practices (Pierson, 2000) and the inability of policymakers to diverge from early policy paths.

Figure 1 below underlines the two punctuation points – 9/11 and 2013 and visualizes how risk management issues developed, materializing in policies in this sector.

<FIGURE 1 HERE>

The regime to protect *health and financial service providers* was even more stable, with less punctuation points over time. Risk reduction steps and pertinent actors were

introduced at an early stage, with increasing monitoring and enforcement capacities coming into effect in 2009 and broadening the scope of regulated entities in 2013. The traditional approach of improving monitoring and enforcement capabilities rather than other risk management practices led to the development of private initiatives in the fields of risk assessment and reduction. In the financial sector it has taken effect through FS-ISACs for information sharing and Payment Card Industry (PCI) for standards, and in the healthcare sector through HiTrust, an information sharing initiative. The private sector was able to fill the vacuum created by federal policymakers, who were unable to diverge from their initial policy paths. Figure 2 below visualizes how risk management issues have materialized in policies in these sectors and highlights the relatively stable nature of the risk governance framework.

<FIGURE 2 HERE>

Finally, the more dynamic risk regime over time, especially since 2013, is the regime that aims to protect *non-critical sectors*. Federal policy strategies and instruments promote different aspects of risk-management in certain time frames. But while the suggested decision-making structures remain constant and the voluntary approach persists, since 2015, significant developments are discernible in the (1) type of actors that have been involved – traditional security agencies joined information sharing efforts, (2) efforts to improve risk assessment – through new mechanisms and incentives for information sharing that were introduced, and (3) risk mitigation steps - that were promoted in 2018 by SEC to protect investors. At the same time, risk reduction steps that policymakers perceived as vital and crucial at an early stage, have remained voluntary throughout the years. Policymakers have chosen not to diverge from the self-regulation paradigm of this regime, despite evidence-based hazard estimates and the perceived level of seriousness of the risk. Figure 3 below visualizes how risk management issues have materialized in policies in these sectors, stressing the rather unstable nature of these governance frameworks in certain risk management topics.

<FIGURE 3 HERE>

6 – CONCLUSION

U.S. policymakers have espoused three distinct risk framings to address cybersecurity risks from digital technologies. Each framing entailed a separate set of actors and objects to protect, but despite a sense of urgency, was less effective in mobilizing coercive risk management steps. In line with existent literature, I conclude that federal cybersecurity governance operates through a patchwork of laws and regulations (Weiss and Jankauskas, 2018; Sivan-Sevilla, 2018; Johnson, 2015), but can also detect three distinct sub-regimes across private sectors.

While the literature highlights the importance of risk frames to the construction and maintenance of regulatory structures, this paper found that institutional configurations – regulatory norms and administrative structures – were more influential in shaping two decades of federal policy decisions to address cyber risks. Despite the perception of risk frames as having a direct consequence on how risk regulation operates (Fisher, 2013), I found that their impact is limited and institutionally constrained.

This finding questions Nissenbaum's (2005) argument about the importance of meanings and framings to policymakers' choices in the field of cybersecurity. It also shows how Fichtner's (2018) typology of three approaches to cybersecurity holds empirically, but their influence on cybersecurity policy paths is minimal. The analysis also questions Quigley et al. (2015) findings on the 'worst-case scenario' paradigm of U.S. policymakers in governing critical infrastructures' protection. The government has expended significant resources and got more than dozen federal branches on board in protecting against cyber threats but did not fully control the security posture of critical sectors. Government intervention diverged across critical sectors and did not always justified the alarming framings of cyber risks in this domain. The same discrepancy framing and governing cyber risks is evident for non-critical sectors. Despite clear evidence of serious risks to develop the development of the economy, cyber risks were addressed based on a self-regulatory and voluntary approach, leaving market actors to decide on their own protection levels.

Therefore, this study finds a vague link between cyber risk framings and policy decisions. In contrast, cross-sectors comparison highlighted the importance of institutional configurations to cyber policy outputs. These include norms in regulated sectors and fragmented state structures in each of the sectors. They better explain chosen policy paths and validate Rothstein et al. (2013) and Hood et al. (2001) findings on the importance of institutional settings for risk governance. Across sectors, policymakers were bind to certain framings, assessments, and evaluations of cyber risks that only loosely informed their risk management policy decisions. The role of the government across sectors and the extent to

which it dictated coercive risk management steps was contingent on the institutional configurations in each regulated sector, rather than on how cyber risks were framed. This confirms and further expands previous findings in the cybersecurity governance literature: (1) the private sector has been dominant in crafting risk governance frameworks (Hiller and Russel, 2013; Johnson, 2015; Thaw, 2014 & 2015; Carr, 2016; Eichensehr, 2017; Boeke, 2017), but this dominance has been differently embedded in each of the three risk regimes according to the decision-making structures they hinged upon. (2) Monitoring and enforcement capacities have increased over time (Hartzog and Solove, 2015; Russo and Rishikof, 2016), albeit unequally across different private sector domains and in direct relation to the decision-making structures in each regime. (3) Incremental policy changes have been clearly evident (Harknett & Stever, 2011), but only in two out of the three regimes, and to different degrees. And (4) a federal gap in governing cyber risks in the broader digital economy has been in existence (Hartzog and Solove, 2015; Balitzer, 2016), but it has gradually narrowed: monitoring and enforcement capacities of new agencies have come into play, SEC and CFPB and all sorts of practices and initiatives for information-sharing copied from critical infrastructure sectors (isomorphism) have been on the rise.

In addition, the comparative analysis over time reveals the importance of self-reinforcing mechanisms for cyber risk governance outputs. It seems that the government has been responding to the dynamic cyber threat landscape, but within the boundaries and paradigms of the decision-making structures that were decided upon during early regime development, and in line with institutional constraints in regulated sectors. For each regime, the government tried to improve risk management practices without diverging from previous policy paths considerably: the private sector still enjoys significant discretion in decisions pertaining to the protection of critical infrastructures, whereas health and financial industries encounter the increasing monitoring and enforcement capacities of top-down regulators. Non-critical sectors are still governed based on incentives and completely self-regulatory models, despite evidence-based hazard estimations and the perceived seriousness of the risk. Moreover, each regime has had its own punctuation points in time. But while the protection of critical infrastructures and health and financial service providers has remained stable over time, the protection of non-critical sectors seems to be more dynamic and open to prospective changes. This validates, for the first time to the best of my knowledge, the importance of time and self-reinforcing sequences (Pierson, 2000) for policy outcomes in the field of cybersecurity.

Overall, these findings question the significance of risk framing to policy outcomes in the field of cybersecurity and increase our understanding of variance in risk governance frameworks across sectors within the same political system. The paper validates Rothstein et al. (2013) and Hood et al. (2001) observations on the importance of institutional configurations - regulatory norms and fragmented structures – in the governance of risks. This is significant especially given the different risk frames across sectors that only loosely influenced policy outputs. Despite the ‘securitization’ and ‘risk colonization’ trends in risk governance, institutional configurations hold significant explanatory power for variance in cyber risk governance.

Limitations to this study arise from the scope of federal policies I analyzed. I chose to study legislative proposals that were enacted but could learn more about policymakers’ framing and suggested policies from looking into legislative proposals that were aborted as well. Another limitation stems from the different length and scope of texts and materials available for each sector. For health and financial service providers, I mostly analyzed federal statutes, which were usually not as elaborate as government strategies, for instance, that I canvassed in the two other regimes. Longer texts are likely to include more sentences for each category of analysis and skew the results of how risk management topics have changed over time across policies. To cope with this limitation, I scrutinized the substance in each sentence to realize whether more sentences actually translate into more risk management practices or different framings of the problem.

Looking ahead, this methodology and analytical framework could be used to trace and compare cyber risk governance frameworks across political systems, or more generally, compare different risk domains within the same political system, and test where else the influence of risk frames is limited and why. This may serve to shed light on the importance of institutional configurations for risk governance policies across risks and nations, in addition to their observed influence within the same political system.

REFERENCES

- Bachrach, P., M. Baratz. 1962. "Two Faces of Power". *American Political Science Review* 56, pp. 947-52.
- Balitzer, S. 2016. "What Common Law and Common Sense Teach Us About Corporate Cybersecurity." *University of Michigan Journal of Law Reform* 49(4), pp. 891-919.
- Blyth, M. 1997. "Any More Bright Ideas? The Ideational Turn of Comparative Political Economy". *Comparative Politics* 29(2), pp. 229-50.
- Boeke, S. 2017. "National Cyber Crisis Management: Different European Approaches." *Governance* (31), pp. 449-64.
- Braun V., V. Clarke. 2012. "Thematic analysis." In: H. Cooper, P. M. Camic, D. L. Long, A. T. Panter, D. Rindskopf, & K. J. Sher (eds.). *APA Handbook of Research Methods in Psychology*, Vol. 2. Research designs Quantitative qualitative, neuropsychological, and biological. Washington, DC, US: American Psychological Association, pp. 57-71.
- Buzan, B., Wæver, O., and de Wilde, J. 1998. *Security: A new framework for analysis*. Boulder, CO: Lynne Rienner Pub.
- Carr, M. 2016. "Public-Private Partnerships in National Cyber-Security Strategies." *International Affairs* 92(1), pp. 43-62.
- Clark, L. 2013. "Framing the Uncertainty of Risk: Models of Governance for Genetically Modified Foods". *Science and Public Policy* 40, pp. 479-491
- The Department of Commerce Internet Policy Task Force, "[Cybersecurity, Innovation, and the Internet Economy](#)", *Department of Commerce*, Washington DC, 2011.
- Druckman, JN. 2004. "Political preference formation: competition, deliberation, and the (ir)relevance of framing effects." *American Political Science Review* 98, pp. 671-86.
- Dunlop, C. 2007. "Up and down the pecking order, what matters and when in issue definition: the case of rbST in the EU". *Journal of European Public Policy* 14(1), pp. 39-58
- Eckert, S. 2005. "Protection Critical Infrastructure – The role of the Private Sector." In: P. Dombrowski (ed.), *Guns and Butter: The Political Economy of International Security*. Lynne Rienner Publishers, Boulder, Colorado
- Eichensehr, K. E. 2017. "Public-Private Cybersecurity." *Texas Law Review* 95, pp. 466-538.
- Entman RM. 1993. "Framing: toward clarification of a fractured paradigm". *Journal of Communication* 43, pp. 51-8.
- Fichtner, L. 2018. "What Kind of Cyber Security? Theorising Cyber Security and Mapping Approaches." *Internet Policy Review* (7)2.
- Fisher, E. 2013. "Framing Risk Regulation: A Critical Reflection". *European Journal of Risk Regulation* 4(2), pp. 125-32.
- Hall, P. 1993. "Policy Paradigms, Social Learning, and the State: The Case of Economic Policymaking in Britain". *Comparative Politics* 25(3), pp. 275-96.
- Hansen L., H. Nissenbaum. 2009. "Digital Disaster, Cyber Security, and the Copenhagen School." *International Studies Quarterly* 53, pp. 1155-75.
- Harknett, R. J., J. A. Stever. 2011. "The New Policy World of Cybersecurity." *Public Administration Review*. May/June 2011: pp. 455-60.
- Harrell, B. "The Private Sector is the Key to Success for The Department of Homeland Security". *csoononline.com*. <https://www.csoononline.com/article/3161793/the-private-sector-is-the-key-to-success-for-the-department-of-homeland-security.html>
- Hiller, J. S., and R. S., Russel. 2013. "The Challenge and Imperative of Private Sector Cybersecurity: An International Comparison." *Computer Law & Security Review* 29: 236-45.

- Hom A. G., R. M. Plaza, and R. Palmen. 2011. "The framing of risk and implications for policy and governance: the case of EMF". *Public Understanding of Science* 20(3), pp. 319-33.
- Hood C., Rothstein H., Baldwin R. 2001. *The Government of Risk: Understanding Risk Regulation Regimes*, Oxford, OUP.
- Jacob S., and N. Schiffino. 2015. "Risk Policies in the United States: Definition and Characteristics Based on a Scoping Review of the Literature". *Risk Analysis* 35(5), pp. 849-58.
- John P. 2012. *Analyzing Public Policy, 2nd edition*. Oxon: Routledge.
- Johnson, K. N. 2015. "Managing Cyber Risks." *Georgia Law Review* 50 (1): 547-92.
- Koon, A. D., B. Hawkins, and S. H. Mayhew. 2016. "Framing and the health policy process: a scoping review". *Health Policy and Planning* 31, pp. 801-16.
- Krieger, K. 2013. "The limits and variety of risk-based governance: The case of flood management in Germany and England." *Regulation & Governance* 7, pp. 236-57.
- Lees, C. 2007. "Environmental Policy in the United Kingdom and Germany." *German Politics* 16, pp. 164–83.
- Lijphart, A. 1971. "Comparative Politics and the Comparative Method." *The American Political Science Review* 65(3), pp. 682-93.
- March J., and J. P. Olsen. 1984. "The new institutionalism: organizational factors in political life." *The American Political Science Review* 78, pp. 734–49.
- National Conference of State Legislatures (NCSL). 2019. "Data Security Laws – Private Sector." *Ncsl.org*. Retrieved from here: <http://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx>
- Nissenbaum, H. 2005. "Where Computer Security Meets National Security." *Ethics and Information Technology* 7, pp. 61-73.
- Perri, G. 2005. "What's in a frame? Social organization, risk perception and the sociology of knowledge." *Journal of Risk Research* 8(2), pp. 91-118.
- Pierson, P. 2000. "Not just what, but when: timing and sequence in political processes". *Studies in American Political Development* 14(1), pp. 72–92.
- Plein, L. C. 1991. "Popularizing Biotechnology: The Influence of Issue Definition." *Science, Technology, & Human Values* 16(4), pp. 474-90
- Quigley K. and J. Roy. 2012. "Cyber-Security and Risk Management in an Interoperable World: An Examination of Governmental Action in North America." *Social Science Computer Review* 30(1), pp. 83-94.
- Quigley K., Calvin Burns, Kristen Stallard. 2015. "'Cyber Gurus': A rhetorical analysis of the language of cybersecurity specialists and the implications for security policy and critical infrastructure protection", 32 *Government Information Quarterly*: 108-17.
- Renn, O. 2008. *Risk Governance: Coping with Uncertainty in a Complex World*. Earthscan, London:UK
- Rothstein H., Huber M., Gaskell G. 2006. "A Theory of Risk Colonization: The Spiraling Regulatory Logics of Societal and Institutional Risks." *Economy and Society*, pp. 91–112.
- Rothstein H., Borraz O., Huber M. 2013. "Risk and the limits of governance: Exploring Varied Patterns of risk-based governance across Europe." *Regulation and Governance* 7(2), pp. 215-35.
- Rothstein H., Beaussier A., Borraz O., Boudier F., Demeritt D., de Haan M., Huber M., Paul R., Wesseling M. 2015. "When 'Must' Mean 'Maybe': Varieties of Risk Regulation and the Problem of Trade-Offs in Europe". *King's College Working Paper*.
- Russo K., H. Rishikof. "Cybersecurity: Executive Orders, Legislation, Cyberattacks, and Hot Topics." *Chapman Law Review* 19(2), pp. 421-44.
- Schattschneider, E. E. 1960. *The semi-sovereign people*. New York: Holt, Rinehart & Winston
- Jonathon P. Schuldt, Katherine A. McComas & Colleen A. Burge. 2017. "Intersecting frames in communicating environmental risk and uncertainty." *Journal of Risk Research*, DOI: 10.1080/13669877.2017.1382559
- Sivan-Sevilla, I. (2018). "Complementaries and Contradictions: National Security and Privacy Risks in U.S. Federal Policy, 1968-2018", *Policy & Internet*. DOI: [10.1002/poi3.189](https://doi.org/10.1002/poi3.189)

- Snow D. A., R. D. Benford. "Master Frames and Cycles of Protest". In: Morris A. D. and C. M. Mueller (eds.). *Frontiers in Social Movement Theory*. New Haven:London, pp. 133-55.
- Solove D. J., W. Hartzog. 2015. "The FTC and the New Common Law of Privacy." *Columbia Law Review* 114(3), pp. 583-676.
- Stone, D. 2012. *Policy Paradox: The Art of Political Decision Making*, 3rd edition. London: W.W. Norton&Company Ltd.
- Thaw, David. 2013. "The Efficacy of Cybersecurity Regulation." *Georgia State University Law Review* 30 (2):1.
- Thaw, David. 2014. "Enlightened Regulatory Capture." *Washington Law Review* (89): 329-77.
- Ulmer, K. 2014. "Cyber Risks and Cyber Security – Risk Communication and Regulation Strategies in the U.S. and Germany." *Working Paper FGI SWP Berlin*.
- U.S. Government Accountability Office. 2017. "Cybersecurity: Actions Needed to Strengthen U.S. Capabilities". *Testimony before the Subcommittee on Research and Technology, Committee on Science, Space, and Technology, House of Representatives*.
- Vogel, D. 2012. *The Politics of Precaution: Regulating Health, Safety, and Environmental Risks in Europe and the United States*, Princeton University Press, NJ
- Weiss, M., V. Jankauskas. 2018. "Securing Cyberspace: How States Design Governance Arrangements". *Governance* 32(2), pp. 259-75.
- Wolf, J. 2016. "What we talk about when we talk about cybersecurity: Security in internet governance debates." *Internet Policy Review* 5(3). doi:10.14763/2016.3.430

APPENDIX #1: LIST OF ANALYZED FEDERAL DOCUMENTS

Name	Year	Sector	#Key Sentences
Health Insurance Portability and Accountability Act (HIPAA)	1996	Healthcare	6
Marsh Commission Report: Critical Foundations Protecting America's Infrastructure	1997	Critical Infrastructures	64
Framework for Global Electronic Commerce	1997	Non-Critical Sectors	28
Presidential Decision Directive 63	1998	Critical Infrastructures	25
Gramm-Leach-Bliley Act	1999	Financial Service Providers	4
Executive Order 13231	2001	Critical Infrastructures	12
The PATRIOT Act	2001	Critical Infrastructures	15
Sarbanes-Oxley (SOX) Act	2002	Financial Service Providers	2
Homeland Security Act	2002	Critical Infrastructures	19
Homeland Security Presidential Directive (HSPD) #7	2003	Critical Infrastructures	12
DHS Appropriations Act	2007	Critical Infrastructures	1
The Health Information Technology for Economic and Clinical Health (HITECH) Act	2009	Healthcare	9
FTC's Health Breach Notification Rule	2009	Healthcare	6
National Cybersecurity and Communications Integration Center (NCCIC) Opening	2009	Critical Infrastructures	6
Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework	2010	Non-Critical Sectors	31
Dodd-Frank Wall Street Reform And Consumer Protection Act	2010	Financial Service Providers	4
National Strategy for Trusted Identities in Cyberspace	2011	Non-Critical Sectors	19
Cybersecurity, Innovation and the Internet Economy	2011	Non-Critical Sectors	34
Amendments to The Health Information Technology for Economic and Clinical Health (HITECH) Act	2013	Healthcare	9
SEC and CFTC's Identity Theft Red Flags Rules	2013	Financial Service Providers	12
Presidential Policy Directive/PPD-21	2013	Critical Infrastructures	38
Executive Order 13636	2013	Critical Infrastructures	17

Department of Justice and Federal Trade Commission: Antitrust Policy Statement on Sharing of Cybersecurity Information	2014	Non-Critical Sectors	9
National Cybersecurity Protection Act	2014	Critical Infrastructures	7
Regulation Systems Compliance and Integrity	2015	Non-Critical Sectors	16
Cybersecurity Information Sharing Act (CISA)	2015	Non-Critical Sectors	11
Executive Order 13691	2015	Critical Infrastructures	6
Executive Order 13694	2015	Critical Infrastructures	4
U.S. Consumer Financial Protection Bureau – Consent Order	2016	Non-Critical Sectors	12
SEC’s Statement and Guidance on Public Company Cybersecurity Disclosures	2018	Non-Critical Sectors	25

TABLES & FIGURES

Table 1: Risk Governance Framework for Critical Infrastructure Protection based on Federal Policies [1997-2015]

Risk Governance Phase	Critical Infrastructures' Protection
Framing:	
<i>Pre-Assessment; Problem Framing</i>	The problem was perceived as a supreme national priority, vital to safety, public health, and economic security.
<i>Assessment:</i>	A new dimension of vulnerability emerged. The threat could come from anywhere, including terrorists, but no actual evidence on the hazards was available.
<i>Characterization & Evaluation:</i>	Risks were perceived as unprecedented national risks that can cause mass casualties and catastrophic health effects like WMDs. They entailed immediate action.
Management:	
<i>Decision-Making Structure</i>	Shared responsibility with private sector leadership and government assistance. Regulation was mostly avoided when possible.
<i>Actors & Institutions</i>	Various governance structures were used with the involvement of many branches of the government: intelligence agencies, private sector coordinators, federal liaison officials, NSC, FBI, ISACs, DoD, DoC, the Department of State, DHS, The Department of Interior, FCC, NRC, and the Treasury.
<i>Improving Risk Assessment</i>	Intelligence agencies and law enforcement authorities assisted in sharing information about threats. DHS consolidated efforts, CERT centers opened, FBI & DNI assisted, ISACs & ISAOs were standardized.
<i>Risk Reduction</i>	Only in 2013 a voluntary framework has been established and adopted by regulatory agencies based on their discretion. Tension between national security and private economic interests was evident.
<i>Improving Risk Mitigation</i>	Post 9/11, dedicated forensic center was introduced, NetGuard teams were created, and situational-awareness capability was developed.
<i>Expertise</i>	The newly established DHS provided technical assistance, and later, DoC and private experts helped with information sharing initiatives.
<i>Monitoring & Enforcement</i>	Arised after 9/11 through national crime task forces. In 2013, annual reporting on compliance with NIST's Cybersecurity Framework had been required, and in 2015 sanctions were introduced by the Treasury.

Table 2: Risk Governance Framework for Health and Financial Service Providers based on Federal Policies [1996-2013]

Risk Governance Phase	Health & Financial Service Providers' Protection
Framing:	
<i>Pre-Assessment: Problem Framing</i>	Identifiable health information and consumers' financial information was at risk of theft, loss, and abuse. Policies should prevent the exposure of sensitive personal information and protect privacy.
Management:	
<i>Decision-Making Structure</i>	Hierarchical top-down structures, under the authority of the secretary of HHS / traditional financial regulators. Still, private sector was integral to the development and implementation of standards.
<i>Actors & Institutions</i>	Healthcare industry was regulated through HHS and FTC. For the financial sector, many different regulators were involved - SEC, CFTC, Federal banking agencies, the Treasury, and National Association for Insurance Commission, and in 2010 the CFPB was established.
<i>Improving Risk Assessment</i>	For healthcare providers, assessment took place through internal audit requirements in HIPAA standards. For financial service providers, the 2002 SOX Act created requirements for assessment of internal information security controls, and FS-ISACs were used by the industry to gain threat information.
<i>Risk Reduction</i>	Both industries were required to establish and implement standards for information security and privacy, with broad discretion to federal agencies and industry stakeholders. In the healthcare industry, the scope of regulated entities increased over time.
<i>Improving Risk Mitigation</i>	In the healthcare industry, mitigation improved through notification to the FTC or HHS. Timely reports on breaches that involved more than 500 individuals were mandated. In the financial industry, mitigation improved through SEC's efforts to minimize the damage from identity thefts.
<i>Monitoring & Enforcement</i>	For the healthcare industry, compliance reports to Congress were put in place. Over time, civil pecuniary penalties have been introduced, individual complaints might be submitted, and periodic audits were required. For the financial industry, 1999 GLBA required enforcement by the different financial regulatory agencies, 2002 SOX required monitoring over information security controls of financial companies through SEC, and CFPB was authorized to monitor and enforce compliance with information security provisions. FTC authority increased over time as well.

Table 3: Risk Governance Framework for Non-Critical Sectors based on Federal Policies [1997-2018]

Risk Governance Phase	Non-Critical Sectors' Protection
Framing:	
<i>Pre-Assessment: Problem Framing</i>	Cyber risks hamper the development of the economy. Protecting these sectors would increase trust and consumers' confidence and this would in turn unleash the economic potential of the online environment.
<i>Assessment:</i>	Infrastructures that drive the U.S. economy were increasingly vulnerable. Evidence-based hazard estimations detailed how trade was badly affected in the past. Hazards also included thefts or manipulation of sensitive data, as well as breach-associated costs and damages to companies' reputation and competitiveness.
<i>Characterization & Evaluation:</i>	Risks were perceived as very serious. They exponentially grow, and consumers' information is in great danger. This posed a persistent economic challenge. Market participants and investors were at great risk. Companies needed to respond and act immediately.
Management:	
<i>Decision-Making</i>	Non-regulatory, incentive-based, market-oriented approach.
<i>Actors & Institutions</i>	Private sector industries, and commerce-related regulators: DoC, FTC, SEC, CFPB. Recently, traditional security agencies - DHS, DoD, The Attorney General - facilitate information-sharing.
<i>Improving Risk Assessment</i>	Voluntary information sharing programs are facilitated. Legal restrictions removed, and liability protections are provided. Internal risk assessments are encouraged by enforcement actions.
<i>Risk Reduction</i>	The government supports companies' voluntary efforts to apply preventive measures for the sake of 'market clarity and competition.' Breach disclosure steps have been encouraged to incentivize risk reduction.
<i>Improving Risk Mitigation</i>	Recommended time frames for breach disclosures and mitigation actions has been mentioned. Federal breach law has been encouraged. Without proper disclosure and mitigation procedures, investors are perceived to be at risk.
<i>Expertise</i>	The DoC should promote research & development efforts.
<i>Monitoring & Enforcement</i>	FTC has been significant in filling the gap of many 'uncovered' industries by enforcing industry-based standards. SEC has also increased monitoring efforts through scheduled testing of businesses under its jurisdiction. Civil pecuniary penalties have been introduced by CFPB.

Table 4: Comparative Risk Governance Frameworks Across Private Sectors

	Critical Infrastructures	Health & Finance	Non-Critical Sectors
Framing	Unprecedented National Risks in a New Domain of Vulnerability. No Clear Hazard Evidence was Provided.	‘Traditional’ Privacy Risks	Serious Economic Development Risks with Clear Evidence Provided
Decision-Making	Unique shared public-private responsibility	Vertical and based on legacy institutions in these sectors	Market-based
Government’s Role	Facilitator. Regulates only if necessary in specific critical sectors.	Top-down regulator with industry involvement in policy design.	Enabler of private initiatives. Enjoys increasing monitoring and enforcement capacities over self-regulation practices.
Coercive Risk Management Steps: Reduction, Mitigation, Monitoring and Enforcement	Carefully and rather sparingly applied with industry input and interchange	Designed at the beginning of policy development	Encouraged on a voluntary basis

Figure 1: Risk Management Topics in Federal Critical Infrastructure Policies Over Time [1997-2015]

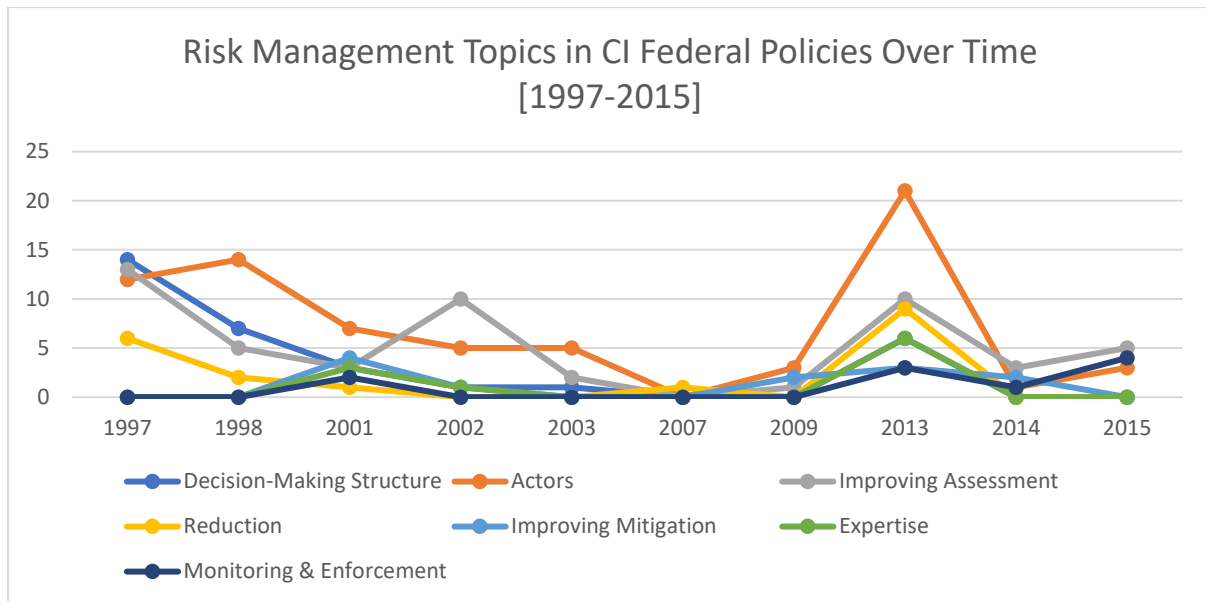


Figure 2: Risk Management Topics in Federal Healthcare and Financial Services Policies Over Time [1996-2013]

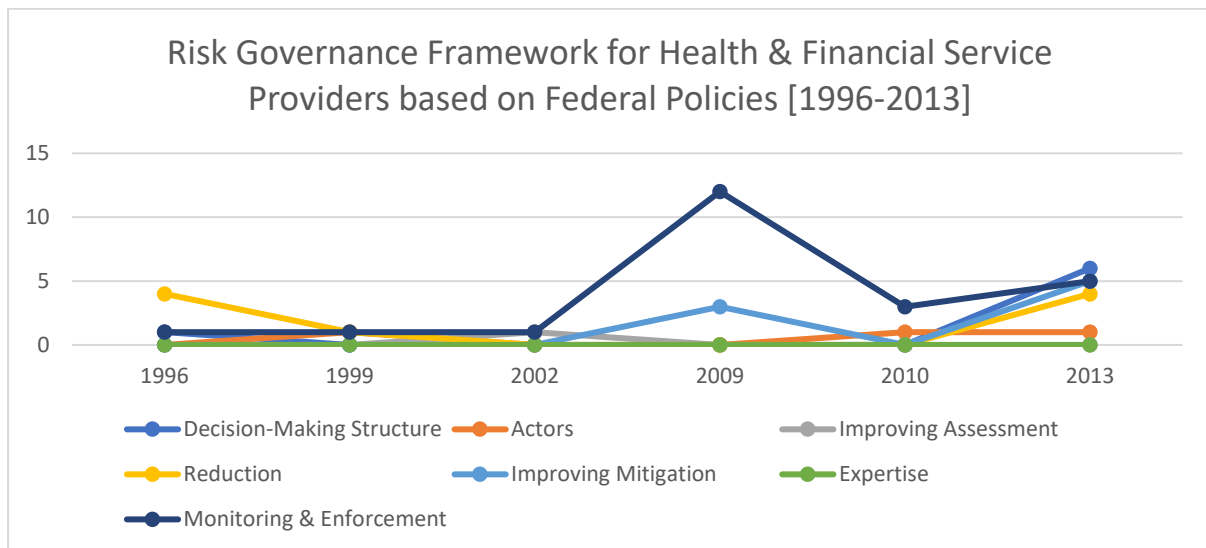
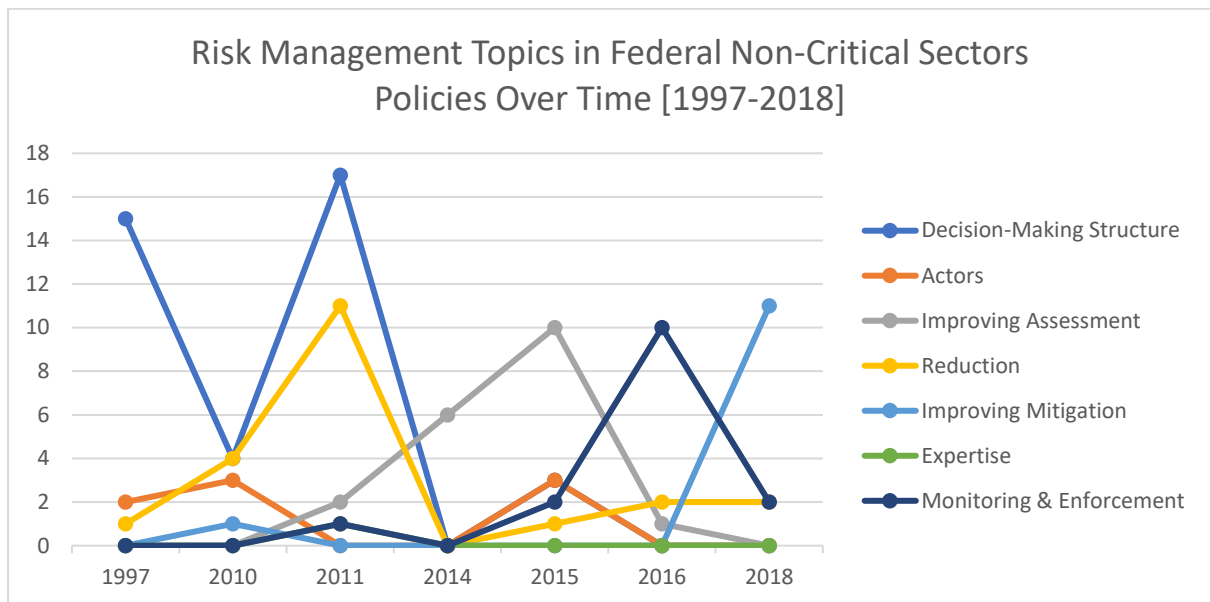


Figure 3: Risk Management Topics in Federal Non-Critical Sectors Policies Over Time [1997-2018]



CHAPTER 3

EU Publicization of Private Certifiers for Cybersecurity: Explaining Public-Private Interactions through the Context of Institutional Change

This chapter presents a manuscript that is currently under review at the *Journal of Public Policy*

EU Publicization of Private Certifiers for Cybersecurity
Explaining Public-Private Interactions through the Context of Institutional Change

ABSTRACT

A recent innovation in EU cybersecurity governance suggests a rarely explored type of public control over private actors in indirect governance arrangements. Through the establishment of the EU Framework for Cybersecurity Certification, policymakers have elevated the role of private certification bodies to issue certificates on behalf of the EU, while increasing public control over their operations. In contrast to full public hierarchical control in delegation dynamics, or lack thereof in orchestration interactions, this interaction implies a different type of dynamic for private actors, who voluntarily enlist themselves to govern on behalf of public authorities and become subordinate to their supervision. This intriguing dynamic begs the questions of how and why such public-private interaction has evolved. I frame this dynamic of public control over market-driven governance arrangements as ‘publicization,’ and argue that we should appreciate its institutional context in order to explain its evolvement. Through a process-tracing analysis based on 40 policy documents and 18 interviews, I find that the EU reached a policy compromise and designed an institutional change in the form of layering, whereby public-private interactions of co-option have been diffusing from the current to the proposed certification regime. To explain this diffusion, I test three hypotheses that consider: (1) Member States’ powerful influence in this policy space, (2) EU’s supranational aspirations, and (3) The significant benefits to private interest groups in the new framework. By studying the institutional context of a rarely explored public-private interaction, this study sheds light on a hybrid form of governance, questioning the dichotomous portrayal of the shift from government to governance.

EU Publicization of Private Certifiers for Cybersecurity

Explaining Public-Private Interactions through the Context of Institutional Change

1- INTRODUCTION

Indirect governance via private intermediaries is growing across sectors and political systems (Abbott et al., 2015, 2017, 2019). We increasingly witness regulation operating in an array of private sector, multi-stakeholder, and hybrid public-private institutions (Elberlein et al., 2014). These forms of governance allow policymakers to cope with complex problems and bridge deficiencies in information and regulatory capacities. Within such governance arrangements, a rarely explored type of public-private interaction has emerged in EU cybersecurity certification. In contrast to the dichotomous understanding of public control over private governance actors that implies either full control through hierarchical *delegation* interactions (Egan, 2001; Frankel and Hojberj, 2007; Buthe and Matli, 2011), or lack thereof in horizontal *orchestration* interactions (Donahue and Zeckhauser, 2008; Hysing, 2009; Abbott et al., 2015), EU policymakers have built a cybersecurity certification framework where public authorities increase their monitoring and enforcement capacities over voluntary enlisted private certification bodies, creating an intriguing form of state control over market-driven governance practices, for domains in which the state had no authority whatsoever.

To frame the character of this public-private interaction, I build on Arcuri's (2015) concept of 'publicization' that captures how the regulatory roles of standard-setting, monitoring, or enforcement are turning from private to public. I define interactions based on Elberlein et al. (2014), who argue that interactions address how governance actors and institutions emerge with and react to one another. As opposed to other uses of the term 'publicization,' that mainly address norms and characteristics of services provided by the government (Haque, 2001; Benish and Levi-Faur, 2012), 'publicization' here refers to the transformation of standard-setting, monitoring, and enforcement from private to public authorities, shifting the attention from regulatory privatization to an inverse pattern whereby public authorities take a central role in the operation of private ones. My goal is to treat the nature of such interaction as an empirical question (Wood, 2015), and understand where it comes from in the policy process.

Through the recently agreed Cybersecurity Act (CSA), EU policymakers have incorporated private certification bodies into a new European Cybersecurity Certification Framework. The Commission has elevated the role of private certification bodies to

voluntarily issue certificates on behalf of the EU, but significantly increased public control over their operations. National agencies in Member States register and accredit private certifiers that are bound to certification schemes crafted by hybrid form of public and private authorities. Public bodies audit those private certifiers, holding them accountable to their public supervisors. This rarely studied public-private interaction begs the questions of how and why private certification bodies are publicly controlled in the EU Cybersecurity Certification Framework? How private certification authorities were successfully co-opted by public bodies?

The literature provides little attention to this type of interaction. Scholars of private governance mostly address the emergence of private regulators due to states' inaction (Knill and Lehmkuhl, 2002; Cashore, 2002; Pattberg, 2005; Bartley, 2007; Bernstein and Cashore, 2007; Borzel and Risse, 2010; Grabosky, 2013; Grabs, 2018). When the government becomes involved, public-private interactions usually take one of two forms: (1) top-down interactions in the form *delegation*, granting state authority and outsourcing specific regulatory tasks to private actors under strict control, or (2) non-hierarchical interactions in the form of *orchestration*, where private regulatory capacities are voluntarily enlisted in exchange for public material support (Abbott et al., 2015 and 2019). Hereby, a third public-private dynamic of increased state control over the operation of voluntary enlisted private regulators in the form of co-optation emerges.

Principle-Agent theory is useful for explaining forms of delegation (Büthe and Mattli, 2011; Abbott et al. 2015) and goals divergence between national and international government organizations (IGOs), which along with weak control mechanisms can explain why IGOs choose orchestration (Abbott et al., 2015), but it is still unclear how and why co-optation of private regulators by the state emerges. Scholars of standardization and certification do not fill this gap. They are mostly concerned with standard-setting processes and provide limited insights on the political contexts of standards' implementation.

Contrarily, I explain the political drivers for co-optation of private authorities by public regulators (publicization), by highlighting the importance of its institutional context. Regarding public control over private regulators as a component in a broader institutional change, I find that despite promises by EU policymakers to 'completely replace' and 'fundamentally change' the ecosystem for certification (EU Commission Impact Assessment Part 4, 2017), new institutional paths emerge *in tandem with* existing frameworks. The sway of public certification bodies over private laboratories has shifted to a regime where national agencies control private certification bodies.

Whereas scholars of endogenous institutional change overlook the public or private nature of institutional frameworks and do not tie modes of change to the distribution of public or private authorities, I argue that tracing institutional change can elucidate why policymakers choose certain public-private interactions in their design of new institutional frameworks.

A qualitative process-tracing analysis based on 40 official policy documents and 18 interviews serves to trace how new institutional layers added to current certification frameworks, explaining the publicization of private certification bodies through three hypotheses that consider how: (1) Member States' powerful influence, (2) EU's supranational aspirations, and (3) Private interest groups' benefits, had led to a policy compromise that bolstered both private certification bodies and national control over their operations.

This lens enhances our understanding of the political considerations of the often-overlooked phase of standards implementation. Second, it creates a novel link between patterns of endogenous institutional change and public-private interactions. Third, it underscores a rarely studied form of intervention by the state through the publicization of market-driven governance practices.

The article is organized in five sections. Next, I review the literature and underline theoretical gaps therein. After expounding why I choose to test those specific research hypotheses, I describe my methodology for answering the research question and testing the three hypotheses. In the third section I analyze the institutional change in EU cybersecurity certification and frame the dependent variable of this research – public-private interactions in current and proposed certification regimes. The fourth section tests the three research hypotheses. The final section discusses the results and concludes.

2 - LITERATURE REVIEW: PUBLIC-PRIVATE INTERACTIONS IN CERTIFICATION REGIMES

The governance literature has conceptualized forms of indirect governance as three- rather than two-party systems, that include rule-maker, rule intermediary, and rule taker. Such structures emerge when public authorities cannot govern unilaterally and lack the legitimacy, authority, or operational capacities for governing their targets (Abbott et al., 2015 & 2017). Within these indirect governance arrangements, scholars of private governance usually explain two types of public-private interactions: (1) hierarchical *delegation*, in which public actors delegate some of their authority to private intermediaries and seek to control their operations, or (2) non-hierarchical *orchestration*, where private actors voluntarily govern

targets on behalf of public authorities in exchange for material support. A third type of interaction, in the form of *co-optation*, suggests that public authorities take over market-driven governance arrangements, such as standardization and certification, by increasing their control over the operation of voluntary enlisted private regulators, and in domains they had no authority before (Abbott et al., 2019). The theoretical understanding of the evolution of this rather unusual form of soft but hierarchical interactions is incipient, as private governance scholars have hitherto focused on delegation and orchestration.

Delegation denotes a hard and hierarchical interaction between public and private authorities couched in terms of Principle-Agent theory. Governance is perceived as a problem of information, where public actors choose to delegate authority to better-informed private intermediaries while fully controlling their operations (Frankel and Hojberj, 2007; Büthe and Mattli, 2011; Abbott et al., 2015). *Orchestration*, in contrast, is a soft and non-hierarchical interaction whereby public and private actors collaborate and complement each other's competences, with no control measures in place. According to Abbott et al. (2015), IGOs are likely to orchestrate when there is a divergence of goals with Member States and weak national control mechanisms over their operations.

These public-private interactions frame public control and hierarchical structures as an all-or-nothing feature. In the case of *co-optation*, this dichotomous understanding of public control does not hold. Private actors are free to choose whether to enlist themselves with public authorities, even though it makes them prone to increased public monitoring and limited enforcement measures. This tips the scales of the ostensible horizontal or vertical relationships, defying the conceptualizations of *orchestration* or *delegation*.

Abbott et al. (2019) draw the general conditions for such interaction to emerge, pointing to the balance of power and divergence of goals between public and private actors as potential explanatory factors without providing extensive empirical examples of how these conditions create the publicization of private regulators on the ground. Scholars of standardization and certification pay even less attention to the political considerations of controlling these governance practices, discussing mainly the benefits, legitimacy, and private influence on these governance strategies (Havighurst, 1994; Spruyt, 2001; Borraz, 2007; Loconto and Busch, 2010; Lytton, 2014; Fougilleux and Locontol, 2016). Private governance scholars, and specifically those who study standardization and certification, rarely touch upon the politics of publicizing these governance tools. Instead, they assign legitimacy and credibility considerations to public control (Gulbrandsen, 2014) and analyze

the enabling and constraining effects of publicizing certification programs (Arcuri, 2015), barely scratching the surface of the politics of standards implementation and its evolution. Moreover, they do not consider publicization as part of an endogenous institutional change, where policymakers are politically constrained in their efforts to control private actors in new institutional frameworks.

In the section below, I propound three research hypotheses to further study the institutional context of publicization and explain why public-private interactions emerge in institutional frameworks. I argue that the case study of EU cybersecurity certification is a case of endogenous institutional change, and in order to explain the publicization of private certification bodies we should study the driving forces behind this change.

2.1. RESEARCH HYPOTHESES: EXPLAINING PUBLIC-PRIVATE INTERACTIONS IN THE CONTEXT OF INSTITUTIONAL CHANGE

Scholars of private governance rarely interact with the literature on endogenous institutional change and do not consider the settings in which policymakers embed private governance actors. Bartley (2011) addresses this gap and argues that in order to understand how private regulators are governed by public authorities we need to pay attention to the layering of multiple rules and the politics surrounding them in a given context. Since standards and certification programs do not add new rules to a previously ungoverned phenomenon, we should consider their political, legal, and regulatory context. Bartley (2011) argues that the literature routinely ignores this layering of rules, portraying private standards as filling a "regulatory void" created by the lack of state action instead.

This holds the other way as well. The proliferation of public-private governance arrangements has received only scarce attention from the literature on institutional change. Scholars are chiefly concerned with explaining ideal types of incremental and continuous change through the addition of rules or actors to existing institutions (e.g. Ackrill & Kay, 2006; Bruszt, 2008; Thatcher & Coen, 2008). Institutional frameworks are, nonetheless, not distinguished based on their public or nature, thereby missing the opportunity to tap the explanatory power of such interactions to account for institutional change as its chosen modes or avenues.

I suggest two types of linkages between these bodies of knowledge and empirically test the second one: first, public-private interactions can serve as explanatory factors for institutional re-design. *Delegation* from public authorities to private actors creates principal-agent relations that can be exploited by private actors to evade the control of public

authorities. This can change the impact of existing institutions and lead to informal shifts in the institutional environment in the form of ‘drift,’ in which policy settings change in a bottom-up manner (Hacker, 2004). Moreover, non-hierarchical interactions in the form of *orchestration* can lead to consistent agreed-upon updates of existing institutional goals and create a change in the form of ‘conversation,’ in which stakeholders strategically change policy settings (Streeck and Thelen, 2005).

Vice-versa, modes of institutional change can explain public-private interactions. When new rules are introduced on top or alongside existing ones by means of layering, it implies that actors with strong veto powers but low levels of discretion are able to preserve previous institutional arrangements, and might seek to diffuse principles of public-private interactions from old to new arrangements (Thelen, 2003 & 2004; Streeck & Thelen, 2005).

Drawing on Bartley’s (2011) approach, I test three hypotheses that delineate the institutional context of the publicization of private certification bodies in the European Union. The hypotheses offer different explanations to the type of endogenous institutional change that EU and Member States had to compromise on, and consequently, discuss why public-private interactions have gravitated toward proposed institutional frameworks.

The first hypothesis tests whether the traditional dominant role of Member States in the cybersecurity policy arena and the will of nations to further influence cybersecurity certification practices can explain the addition of new layers to existing frameworks, illuminating why public-private interactions have diffused toward the proposed regime.

I follow Capano’s (2018) approach who argues that institutional layering can be conceptualized in terms of institutional design and drive stability in existing policy systems. Member States are hypothesized to push for institutional layering in order to maintain the political legitimacy of their current dominant positions in cybersecurity certification. I expect Member States’ veto powers to allow them to control the extent of proposed institutional change, thus ensuring their dominance over private governance actors persists and stabilizing existing certification frameworks.

The literature on EU cybersecurity governance confirms the willingness of nations to further legitimize their influence in this policy arena. Since cybersecurity is absent from EU treaties (as a policy field), the EU has been in a continuous conflict with Member States, trying to increase its mandate to govern cybersecurity by linking cyber-related policies to existing EU competences (Wessel, 2015). Recently, the EU has been endeavoring to make provisions for cybersecurity in the fields of national defense and security, threatening the exclusive mandate of Member States further (Odermatt, 2018).

The case of cybersecurity certification has been yet another arena for this conflict. Not supporting EU's cybersecurity initiatives as enthusiastically as smaller states do, powerful states such as Germany, France, and the UK invested heavily in national certification frameworks, potentially engendering an influential opposition to EU's policy aspirations in CSA (Backman, 2016). Since the national initiatives of strong Member States are less likely to be smoothly integrated into a comprehensive European framework (Bendiek et al., 2017), I expect significant and effective national opposition to the new certification framework. The first research hypothesis is summarized below:

***H1:** The chosen mode for institutional change, and consequently, the diffusion of public-private interactions from current to the emerging certification regime, can be explained by the veto powers of Member States in the cybersecurity policy arena and their willingness to stabilize and further legitimize their central role in cybersecurity certification.*

The *second hypothesis* tests whether the compromise that the EU was willing to make to fulfill its supranational aspirations and increase its regulatory capacities in this policy space has given rise to layering and public-private interactions.

Layering in this case was an accepted EU compromise, as long as certification schemes were developed under EU mandate and private certifiers were authorized to certify targets on its behalf.

Even though most competencies in the cybersecurity policy arena remained in the hands of Member States, the EU has been increasingly active over the years and clearly stated its ambition to play a central role in developing the regulatory framework for cybersecurity (Wessel, 2015). Initially, the EU was only influential through soft tools and promoted cooperation between actors by establishing the European Agency for Network and Information Security (ENISA) in 2004, the European Cyber Crime Center (EC3) in 2013, and the Contractual Public-Private Partnership (cPPP) in 2016. Recently, however, the EU has become more active through legislative tools. It enacted the Network and Information Security (NIS) Directive in 2016, setting minimum levels of protection in Member States by arguing that a disruption of networks in one state can have wider effects on others and create a barrier to the Internal Market (Christou, 2016). This reliance on an economic rationale is also demonstrated in the discussions over cybersecurity certification. National fragmentation in existing policies and the legal EU basis to ensure the functionality of the Single Market

lend legitimacy to EU attempts to forge a European Cybersecurity Certification Framework regardless of the opposition of Member States.

Moreover, as an international government organization (IGO), the EU is significantly constrained by Member States. Through the promotion of private certification bodies, the EU can theoretically bypass Member States and govern targets beyond its jurisdiction without states' intermediation (Abbott et al., 2015 & 2019). This is not the first time the EU uses standards-setting processes to bypass Member States. Through the EU's New Approach that harmonizes technical standards in Europe, the EU has been trying to bypass national authorities as well (Borraz, 2007). It perceives standards as instruments of supranational governance that offer the opportunity to reduce the influence of national interests and quicken the pace toward the achievement of a Single Market (Brunsson and Jacobsson, 2000).

Thus, the willingness of the EU to become more influential in the cybersecurity policy arena, along with its historical utilization of standards as tools to bypass Member States and promote its agenda, lead me to hypothesize that EU's supranational aspirations contributed to the agreement on policy comprises in the Cybersecurity Act. The second research hypothesis is summarized below:

***H2:** The chosen mode for institutional change, and consequently, the diffusion of public-private interactions from current to the emerging certification regime, can be explained by EU's supranational aspirations to increase its influence in the cybersecurity arena through the elevation of private certification bodies and the creation of EU schemes, Making concessions that allow national authorities to maintain current institutional frameworks and enjoy significant control over private certification bodies.*

The *third hypothesis* examines whether private interests had only limited influence on the rising national control over private certification bodies. Since both industry and private certification bodies significantly benefit from the (1) harmonization of certification schemes – that decreases regulatory burdens for product manufactures and service providers - and (2) the upgrade of certification bodies – that increases their market share, I expect private interests to have only marginal influence on the type of interactions between national authorities and private certification bodies.

There is a paucity of studies on the influence of private interests on the governance of certification regimes. Generally, I expect private regulators to encourage and support the publicization process to gain legitimacy and further 'lock-in' their modes of operation

(Spruyt, 2001). Traditional private interest literature points to the fact that business interests of profit maximization and market stability are likely to influence policy outcomes (Baldwin and Cave, 1999). In this case, since both industry and certification bodies are significantly better off, I expect them to pose minimal obstacles for both institutional layering and enhanced public control over private certification bodies. The third research hypothesis is summarized below:

***H3:** The chosen mode for institutional change, and consequently, the diffusion of public-private interactions from current to the emerging certification regime, can be explained by the limited influence of private interests on this chosen policy design. Since product manufactures, service providers, and private certification bodies significantly benefit from this institutional change, I expect them to pose minimal obstacles in the policy process and instead, allow strengthened national control over private certification bodies.*

3 – METHODOLOGY

In order to explain the publicization of private governance actors, I conducted an in-depth case study analysis of EU cybersecurity certification that tracks how the institutional frameworks for certification have changed with the emergence of new types of public-private interactions.

I collected 40 relevant policy documents and reports: sixteen policy documents from EU institutions (See Appendix #1), sixteen position papers from twenty-two private organizations and associations (see Appendix #2), and eight ENISA reports (see Appendix #3) that are related to cybersecurity certification. I also interviewed 18 stakeholders from different types of organizations that include – The EU Commission, Parliament, and Council, ENISA, national certification agencies, private certification bodies, private evaluation laboratories, product manufacturers, digital service providers, and industry associations (see Appendix #4). In those interviews, I asked for insights about the current and prospective certification regimes, the public-private interactions in both regimes, and main compromises in the policy process.

Data analysis was based on qualitative analysis of documents and interview transcripts based on the process-tracing methodology (George and Bennet, 2005). I traced the links between possible causes for the publicization of private certification bodies and observed outcomes, focusing on sequential processes within the legislative process.

To measure the influence of Member States, I traced stated positions by national authorities, the veto powers that Member States gained in the process, and the changes that Member States were able to incorporate in the text. To measure the influence of EU's supranational aspirations, I traced the significance of the proposed change to EU's policy standing in the field, and the battles that the Commission chose during the legislative process. Finally, to measure the influence of private interests, I traced all the arguments in the collected position papers and realized how significant was the addition of new institutional paths for certification to private groups, even if control over private certification bodies has grown.

4 – CURRENT AND PROPOSED REGIMES FOR EU CYBERSECURITY CERTIFICATION

Certification as a tool of governance refers to 'regulation through authorization' and addresses giving a quality assurance based on a successful evaluation process conducted according to standards-based certification schemes (Frieberg, 2017). Specifically, in the domain of cybersecurity, certificates can apply to services, products, or persons. They are issued to certified subjects following evaluations tests that are based on certain standards for information security in organizations or services (ISO 27001/2), and security evaluations of products (Common Criteria – CC) that evaluate the security functional requirements of products' technical designs, interfaces, communication methods, the resiliency of the product against attack heuristics, and etc.

The growth in the use of this tool reflects its promise to address complex technical issues, outsource regulatory processes to experts, allow public authorities to 'govern at distance,' increase consumers' trust, and improve the competitiveness of manufacturers (Loconto and Busch, 2010). This promise, however, is not fully utilized in EU cybersecurity certification. Current certification processes are costly, lengthy, and fragmented across Member States.

The institutional framework for certification contains four types of mutually reinforcing independent actors: (1) *standardization bodies* set the requirements for the production of certification schemes. These schemes include the methods and principles for the issuance of certificates. (2) *Certification bodies* certify products/services according to evaluation processes conducted by (3) *independent laboratories*, and based on certification schemes. The evaluation process is the assessment of the product while the certification process oversees the evaluation and ends with the actual certificate. Since certification bodies

are held accountable for the issued certificates, they are obliged to oversee the evaluation process and ensure the competences of the labs. Laboratories that perform the testing can be part of the certification body, or independent entities accredited by certification bodies. The involvement of the certification body in evaluating, auditing, and monitoring labs changes per requirements within the certification scheme. The fourth type of actors are (4) *accreditation bodies* that verify the quality and monitor the operation of certifiers.

4.1. CURRENT REGIME

These four components are executed by public and private actors in the current patchy terrain of cybersecurity certification in the EU. Certificates are issued through four distinct institutional frameworks that are differently recognized at the international, European, national, and industry levels. Each public certification path demonstrates the dominant position of national authorities and embodies interactions between public certification bodies and private laboratories.

First, *internationally recognized* certificates are provided based on the international Common Criteria (CC) standards, featuring one of seven possible hierarchical Evaluation Assurance Levels (EAL). The international community has embraced the CC standardization through the Common Criteria Recognition Agreement (CCRA) whereby signers have agreed to accept the results of CC evaluations performed by other CCRA members. Currently, fifteen Member States are part of the agreement. The object of CCRA is to enable a context where products and protection profiles that earned a CC certificate can be procured or used without the need for further evaluation.

The requirements of CC standards are developed by an international consortium known as the Common Criteria Development Board (CCDB) and Common Criteria Maintenance Board (CCMB). These are management committees consisting of senior representatives from each signatory country of the CCRA, which was established to implement the arrangement and provide guidance to the respective national bodies, including on evaluation and validation activities. The public certification body in each Member State is responsible for overseeing evaluation laboratories, whereas national intelligence and defense agencies accredit public certification bodies. Officially, only evaluations up to EAL 2+ are mutually recognized.

Public-private interactions take place between national cyber agencies that serve as public certification bodies, while certification bodies are charged with auditing and licensing

independent private laboratories. Auditing includes the monitoring of the personnel, facilities, and evaluation processes in labs, and happens on a yearly and per-project basis. In case of non-compliance, the certification body can revoke the license of the lab, but it typically issues a warning to fix non-compliance within six months before abrogating the license of a laboratory.

Second, *at the European level*, in 1997 twelve Member States + Norway concluded a mutual recognition agreement regarding CC certificates, also known as the Seniors Officials Group on Information Systems Security (SOG-IS) agreement. It is currently the main certification mechanism at the European level and was produced in response to EU Council Decision from 1992 (92/242/EEC) and a subsequent Council recommendation from 1995 (1995/144/EC) on common information technology security evaluation criteria.

The purpose of SOG-IS is to coordinate the standardization of Common Criteria and certification policies among public certification bodies in Member States. Each party to the agreement recognizes evaluations done up to EAL 7 by limited number of nations that are defined as ‘certificate issuing parties.’ Another goal was to coordinate the development of certification schemes to comply with legal requirements at the EU level. Still, the scope of mutual recognition is limited to product types that involve digital signatures, digital tachographs, and smart cards, because national authorities wanted to limit the higher levels of recognition of CC standards to only specific technical domains, where adequate agreements around evaluation methodology and laboratory requirements have been in operation.

Public-private interactions under the SOG-IS are similar to interactions under the CCRA. Labs are mostly independent private companies and need to be licensed. They are heavily monitored by public certification bodies and can be blocked from being licensed in multiple countries. Certification bodies accredited by national intelligence and defense agencies have to ensure that all laboratories follow SOG-IS criteria in addition to CCRA requirements.

A third path for certification in the EU is national. Public certification bodies provide *nationally recognized* certificates in several Member States for two purposes: (1) They set high-level cybersecurity requirements for national security in components of traditional infrastructure under the CC, and (2) create efficient alternatives to CC for low assurance levels. With the lack of mutual recognition agreements, these certificates are recognized only within national boundaries. Like in previous certification paths, public-private interactions take place between national agencies that serve as public certification bodies and the private

laboratories they work with. Public authorities authorize private labs, review their processes, and audit them on a periodic basis.

While Germany, France, and the UK enjoy high amount of expertise in this domain, not all Member States hold public certification capacities. The Commercial Product Assurance (CPA) scheme in the UK is an example of a national scheme that provides low assurance levels. The scheme is open for application to all vendors with a UK sales base and has no mutual recognition agreement. UK's national authorities also support Common Criteria certificates. The national accreditation body in the UK accredits Commercial Evaluation Facilities (CLEFs) as testing laboratories based on ISO 17025. UK's national cyber agency authorizes CLEFs, keeping their operations under review.

Another example is the French cybersecurity agency, that offers two types of evaluations – local, and CC. Its local certification scheme - Certification Securitaire de Premier Niveau (CSPN) - was established by the National Cybersecurity Agency of France (ANSSI) in 2008, with the purpose of providing a faster and cheaper alternative to CC. Like UK's CPA, this scheme has no mutual recognition agreement. The French Prime Minister is in charge of licensing private laboratories, whereas the French Accreditation Committee accredits them (COFRAC) in keeping with the ISO 17025 standard.

In Germany, the national cybersecurity authority – Federal Office for Information Security (BSI) – has developed a baseline approach for low-level assurance to improve the efficiency of CC evaluation. The technical evaluation has been performed by an evaluation facility approved by BSI and monitored by its certification body. BSI also uses the CC approach for certification, developing schemes to define national security requirements in the evaluation of critical components. Emerging national certification initiatives are also developing in Italy, Sweden, Norway, the Czech Republic, Ireland, and Poland (EU Commission Impact Assessment, Part 6, 2017).

The fourth path for certification is completely *private*, where private actors drive standardization, certification, and evaluation. Industry associations adopt certain standards and deploy certification schemes that are recognized within industrial sectors. Product manufactures apply for certificates through private certification bodies that work with private laboratories. The need for accreditation varies according to the private scheme. Examples of such schemes include: ISASecure certification program in the industrial automation sector, EMVCo and the Payment Card Industry (PCI) schemes, and MIFARE scheme by NXP Semiconductors for ticketing solutions. Most cybersecurity certification is currently based on

private rather than public schemes and operates through this path (Interview with an EU Commission policymaker, 2019).

To summarize, public-private interactions in current certification paths between public certification bodies and private laboratories demonstrate significant control of public authorities over the operation of private labs, which have to be licensed by the public bodies, and their personnel, processes, and facilities are constantly audited by public authorities in the international, European, and national paths of certification. In case of non-compliance, public certification bodies can repeal the license of labs after appropriate warnings. Under the SOG-IS agreement, private laboratories can even be banned from licensing with multiple national authorities.

The figure below illustrates the four paths for cybersecurity certification in the EU before the Cybersecurity Act (pre-CSA).

<FIGURE 1 HERE>

4.2. EMERGING REGIME

The need to develop a European cybersecurity certification framework was firstly raised in a 2016 EU Commission Communication that recognized the urgency of harmonizing national evaluation practices and certification schemes. In September 2017, the Commission proposed the Cybersecurity Act (CSA), a regulation that strengthens the mandate of ENISA and establishes a new EU Cybersecurity Certification Framework. The trialogue negotiations successfully ended in December 2018, and the EU Parliament had voted to adopt the Act on March 12th, 2019.

One of the main pitfalls of current paths for certification is the lack of cooperation among Member States. This creates nationally separate testing and evaluation procedures in ways that might protect indigenous industries and increases the regulatory burden for manufacturers that operate in several states. The process of certification is long, expensive, and not suitable to the dynamic lifecycle of high-tech products.

The EU has undertaken to address these gaps by setting up a new framework for EU-recognized certificates that tries to find the balance between time to market and security quality. Through the CSA, three new European certification paths were generated, upgrading the role of private certification bodies. Moreover, the act establishes public accreditation, monitoring, and enforcement mechanisms over private certification bodies.

According to EU Commission policymakers, the elevation of private certification bodies ensued from reasons of scale and resources. Since these bodies already enjoy capacities to certify, they can cope with the expected surge in the demand for certificates and fulfill gaps for Member States with no certification capacities (Interview with EU Commission policymaker, 2019).

Still, this elevation of private governance actors indicates an intriguing type of public-private interaction to explore. The paragraphs below render an account of the creation of the three new paths for EU certification, delineating the overall institutional changes in the certification framework to realize how public authorities elevate and control private certification bodies. As opposed to current public certification paths, public-private interactions in the new framework take place among cyber agencies, national accreditation bodies, and private certifiers.

Tracing the institutional change

The European framework for certification was established on top of existing institutional frameworks, introduced three new certification paths for different assurance levels – Basic/Low, Substantial, and High. All types of certificates are currently voluntary and should be issued by an independent third party. The low/basic assurance level also allows self-assessment models of first party certification. Each certification body has to register with a national authority, and its status can be revoked in cases of non-compliance with accreditation and regulatory requirements.

Certificates issued at the assurance level of *basic/low* are defined as providing a limited degree of confidence. Evaluation should include a review of the technical documents of the product. For this assurance level, CSA opens the possibility of a conformity self-assessment by industry actors in addition to third-party assessment. The first-party certification process permits manufacturers to voluntarily issue a statement of conformity to requirements laid down in the scheme. They assume responsibility for the compliance of their products and carry all evaluation checks by themselves.

Certificates issued at the assurance level of *substantial* are defined as providing a higher degree of confidence. Verification of the security functionalities with the product's technical documentation informs the evaluation. Both public and private certification bodies are allowed to issue certificates at this level. This allows private certification bodies to work with market actors from several Member States and produce recognized certificates without the need to go through SOG-IS or CCRA mechanisms. Evaluation is done in private labs, and

accreditation is conducted through national cyber agencies and traditional accreditation bodies.

Certificates issued at a *high level* of assurance are defined by the Act as providing the highest degree of confidence. Efficiency testing that assesses the resistance of the security functionalities of evaluated object against high-level cyber-attacks guides evaluation. Only public certification bodies can issue certificates at this assurance level.

New governance frameworks that apply to all assurance levels support these emergent certification paths, addressing the (1) development of European certification schemes, (2) the accreditation of private certification bodies, and (3) the monitoring and enforcement practices over certification bodies and certified products. These institutional changes create new interactions between private certification bodies and public authorities.

First, the CSA defines an overall framework of rules governing the adoption of European certification schemes pertaining to cybersecurity. The governance processes involve multiple stakeholders from Member States, industry, and certification bodies to decide upon new schemes to embrace. Stakeholders come together and influence the process through two different groups – (1) the EU Cybersecurity Coordination Groups (ECCG), headed by the Commission and ENISA, which comprises heads of national cyber agencies, and the (2) Stakeholder Cybersecurity Certification Group that includes small, medium, and big businesses, digital service providers, standardization bodies, accreditation bodies, certification bodies, consumer organizations, and academia. The schemes detail the specification of cybersecurity evaluation requirements including the level of assurance they provide, methods to evaluate, rules for surveillance and compliance, and consequences for non-compliance. Once a need for a scheme is identified, the request is submitted via the Commission and/or ECCG to ENISA, which works with all stakeholders for transparently drawing the scheme. Thus, through the development and deployment of certification schemes, EU and Member States set the regulatory framework for private certification bodies, including monitoring requirements and sanctions for non-compliance.

Second, the CSA creates a new framework of accreditation to assess the quality and ensure the capacities of certification bodies. This is based on both national accreditation bodies that operate according to regulation EC 765/2008 and national cybersecurity agencies that act as both public certification bodies and accreditors in the process. The national cyber agencies should actively assist national accreditation bodies in monitoring and supervising certification bodies based on their expertise. For each EU scheme, national authorities ought to notify the Commission of the accredited certification bodies that are allowed to certify. In

cases of non-compliance, national authorities can restrict, suspend, or withdraw existing authorizations of private certification bodies.

Third, the CSA forges a new framework for monitoring and enforcing the compliance of certification bodies and certified products in the post-certification process. This is an often-neglected aspect of certification regimes (Loconto, 2017). Post-certification, compliance of certified products is going to be tested through information gathering based on current Market Surveillance Authorities in Member States, as defined in EC 765/2008. These are periodic checks on certified products to ensure that the certification is still valid. In addition, the operation of private certification bodies has been also under comprehensive monitoring. National cyber agencies can revoke non-compliant certificates and withdraw certification bodies from the list of authorized entities. National cyber agencies are authorized to supervise private certification bodies, conduct investigations, impose penalties, and handle complaints regarding their operation. They are empowered to request information from certification bodies on their performance and compliance practices, and obtain access to any premises of the certification body or certificate holders.

Another significant monitoring mechanism is the newly established ‘peer-review’ arrangement. This arrangement allows national authorities to cooperate by sharing information on possible non-compliance of labs or certification bodies with the schemes. The new mechanism serves two purposes – it increases control of public authorities over private certification bodies and ensures equivalent standards and practices throughout the Union to prevent a race-to-the-bottom in the quality of issued certificates. Information sharing covers the procedures for supervising the compliance of products, services, and processes with certificates, and verifies the appropriateness of the expertise of the personnel in certification bodies. The ECCG should draw up a summary of the peer review results that may be made publicly available and include recommendations on actions to be taken by entities covered.

Overall, the newly emerged institutional frameworks for EU cybersecurity certification take over the market practice of certification by bolstering voluntary enlisted private certification bodies while strengthening public control over their operations. While in previous arrangements, private certification bodies only had a role in certifying according to private schemes that were recognized within specific industries, the new regime allows them to certify based on EU schemes across Member States. Previously, these private certification bodies worked without significant levels of public control over their operations. In the new framework, however, they are under the auspices of public authorities. Each private certification body has to be registered and approved by a Member State; it is accredited by a

joint effort of the national accreditation body and cybersecurity agency, and comprehensively monitored by the national cyber agencies. This enhanced public control is carried forward through three new governance arrangements for (1) the creation of EU schemes that includes monitoring and enforcement principles over private certification bodies by public authorities, (2) an accreditation framework that monitors and can suspend or restrict the operation of private bodies, and the (3) post-certification monitoring and information sharing mechanism among national agencies that empowers public authorities to monitor and sanction private certifiers. In the next section, I test to what an extent my three hypotheses can explain the emergence of these public-private interactions in the context of the broader institutional change in EU cybersecurity certification.

The figure below illustrates the three new additional paths for cybersecurity certification in the EU.

<FIGURE 2 HERE>

5. HYPOTHESES TESTING

The publicization of private certification bodies takes place in a context of endogenous institutional change, in which certification paths are established on top of, rather than in lieu of existing ones. The EU added a new institutional layer, bringing about a change in the form of ‘layering’ whereby new elements are attached to existing institutions and do not replace the old ones (Thelen, 2003 & 2004; Streeck & Thelen, 2005). The chosen policy path does not only keep current frameworks intact, but also engenders mechanisms to control private certifiers in line with existing public control patterns over private labs.

In both current and proposed institutional arrangements, private actors need public authorization to operate, work under a regulatory framework that is designed by public actors, accredited by public authorities, constantly audited and monitored by national agencies, and face the threat of sanctions from public bodies. Table 1 below compares public-private interactions in the current and emergent regimes. It seems that prospective interactions evolve from previous institutional arrangements. This is the dependent variable I aim to elaborate below.

<TABLE 1 HERE>

5.1. **Hypothesis #1:** Member States' Powerful Influence on this Policy Space

To examine the influence of Member States on the way private certification bodies are controlled in the forward-looking regime, I analyze Member States' official positions, their veto points in the new framework, and the changes they were able to incorporate in the agreed CSA text.

The voice of Member States in this policy process was dominantly led by nations with certification capacities and expertise – Germany, France, and the UK. Policy documents and interviews with key stakeholders reveal the willingness of these states to further legitimize their central role in the cybersecurity certification ecosystem and limit significant changes to current practices. According to a senior ENISA official: 'Cybersecurity, especially as a component of critical infrastructures and national assets protection, remains a national responsibility within EU treaties.' In the current public certification paths, national representatives lead the development of schemes, because it touches upon core national security and sovereignty issues. National authorities argue that the different designs of traditional infrastructures across nations require fragmented certification and a continuous influence of Member States on these processes (EU Commission Impact Assessment, Part 4, 2017). France and Germany argued that the prospective framework should extend rather than replace existing successful national tools and processes. They asserted that the EU Commission should not detract from Member States' competencies, suggesting taking advantage of existing national certification capabilities (Schabhuser, 2017; French Senate, 2017). A private lab owner described how 'national authorities care about security, not about business,' and this is where they diverge from EU's approach to cybersecurity. Subsequently, they would like 'private certification bodies to be very controlled...and these bodies should worry about their levels of independence under the new Cybersecurity Act.' He perceives cybersecurity as 'a sensitive topic,' for which national authorities are imposing their mandate and will over other actors. This skepticism towards other actors is evident within national boundaries as well. According to an EU Commission policymaker, 'national cyber agencies do not trust national accreditation bodies to properly accredit private certifiers.'

Member States were eventually able to promote significant changes during the legislative process and enjoy significant veto points and monitoring capacities in the proposed framework. According to a senior ENISA representative, 'the power shift in the agreed text is towards Member States – they get to control the Commission in every step of the way, enjoy discretion to act as they please, and retain full operational capacities in the

aftermath of the proposal in terms of accreditation and supervision over certification.’ The veto points of national authorities include the declaration of an issue as a national security issue that should be kept under their sovereignty, their authority to accredit and approve every certification body, the authorization to monitor the operation of certification bodies and revoke their accredited status, and the ability to vote against recommended EU schemes during the comitology process.

Pro-national changes in the CSA text include, *inter alia*, provisions to the development process of certification schemes, where the Commission, which had been initially empowered to state annual priorities, lost that prerogative to the ECCG group consisting of Member States’ representatives, after an amendment by the Council vested it with the authority to request a new scheme.

In terms of certification paths, national schemes have not been excluded, and based on an amendment by the Parliament, the SOG-IS arrangement still holds. Furthermore, a Council amendment suggests that national agencies can still issue national certificates that are valid only within their borders. This can happen in cases where an EU scheme is not provided, or when issues of national security arise.

Several amendments by the Council incorporated some provisions meant to increase the capacity of monitoring through accreditation and national agencies into the extant framework, including the authority of accreditation bodies to suspend and restrict certificate authorities, the double-accreditation requirements – from both a national accreditation body and a national cyber agency, and the strengthened monitoring capacities over private certification bodies.

In terms of CSA’s implementation, Member States got significant veto powers as well. Even though implementation is going to take place through an implementing rather than delegating act that leaves less discretion for Member States during the implementation process, national representatives still need to approve the Commission’s activities. According to an ENISA representative: ‘Member States will have the final word, as these committees control the Commission in this policy implementation. Therefore, Member States enjoy veto powers on every scheme that will be produced, which means they can block the adoption of a scheme as they desire.’ At the same time, a Parliament amendment to increase the discretion of Member States in adopting an EU scheme was discarded.

Two additional changes in the text permit significant national influence on the post-certification process: (1) The introduction of the peer-review mechanism, that was jointly

promoted by Parliament and Council, and the (2) use of Market Surveillance Authorities, as added by the Parliament.

Ultimately, Member States were able to pose on the EU a policy compromise, preventing a significant divergence from current institutional paths. They were able to push for enhancing their control over private certification bodies, maintaining their powerful position through several veto points and further legitimizing their status as central actors for cybersecurity certification. Therefore, I do find that their dominant role affected the type of institutional change and the diffusion of public-private interactions from current to the future certification regime.

5.2. **Hypothesis #2:** EU's Supranational Aspirations in the Cybersecurity Arena

To examine how EU's passion to increase its role in the cybersecurity policy arena bore on the agreement concerning national control over private certification bodies, I traced the new powerful position that the EU gained, and clarify how important was this change for its aspirations, even if the price was a compromise with national authorities.

Eventually, the EU was able to create a new institutional framework on top of the existing one to influence cybersecurity governance in Member States considerably. Through the development of EU schemes and the elevation of private certification bodies, the EU can indirectly govern targets in Member States. These are both significant changes to the balance of power in EU cybersecurity policy space. CSA's text specifically stipulates, following an amendment by the Council, that national schemes will cease to apply. Member States are not allowed to introduce new schemes in case they are already covered by an approved EU one. This is likely to create a situation in which gradually, EU certificates will replace national ones. According to a senior representative from ENISA: 'The main novelty of the CSA is the fact that the EU is taking responsibility over cybersecurity certification schemes and implements them in a European fashion.' Even though the Act allows the continuation of national paths of certification, national agencies have to communicate their desire to develop a new scheme and get an approval from the Commission and ECCG to do so.

In the governance processes of developing new schemes, ENISA enjoys leading roles of facilitation and coordination, while the Commission is authorized to approve every new scheme. Hence, the EU casts a central role for its institutions, and is responsible for the operation of the whole process.

Another substantial achievement for the EU is the authorization of private certification bodies to operate and be recognized by several Member States. Previous institutional arrangements blocked private actors from operating in several nations, but following an amendment added by the Parliament, private certifiers can now voluntarily enlist themselves with any Member State.

EU's passion to pass CSA and elevate its capacities is demonstrated by the Commission's decision to couple the strengthening of ENISA with the new certification framework under a single proposal for consideration by EU institutions. This coupling is not a coincidence. ENISA is a valuable agency for Member States as it allows them to get assistance and support at a low cost. According to an ENISA representative: 'the agency is weak to stand up against Member States, but can still support, assist, and advise them. Therefore, Member States would not want to explain to their tax payers why they did not agree to the strengthening of ENISA,' and by that, 'The Commission wanted to increase its opportunity of success, so it moved in an area where Member States did not agree before – certification, together with a popular proposal to strengthen ENISA. By putting two seemingly different things together, the Commission increased the chances that Member States will accept everything as a package.'

Moreover, in the initial consideration of policy options, the Commission chose the only policy option that elevated private certification bodies to certify based on EU schemes. All other options relied on existing frameworks, leaving the EU with the same levels of influence as before. Previous policy options included the development of non-binding EU cybersecurity standards, the turning of SOG-IS to a mandatory framework, and the use of EU's New Legislative Framework (NLF) for harmonizing standards in the internal market. These options were rejected because they were perceived as either burdensome for market actors or unlikely to solve the current national fragmentation. Most importantly, none of them boosted EU's influence as the chosen policy option.

In terms of CSA implementation, the Commission was able to prevent significant discretion from Member States in the process. Member States pushed to implement CSA through a delegated act based on a Parliament amendment in order to gain additional room for discretion in the implementation stage. This was not approved in the agreed text, leaving the Commission to produce implementing acts that refer to practical implementation of rules that already exist in the original legislation. The Parliament was also unsuccessful in adding to the text requirements to include justifications for a new EU scheme based on Member States' opinions.

Thus, the EU was able to strategically improve its standing in the cybersecurity policy arena in ways that make national control over private certification bodies and the maintenance of existing institutional frameworks marginal to the long-term EU interest. CSA allows parts of EU's supranational aspirations to be fulfilled in manners that motivate the EU to make a compromise, even if it allows national authorities to continue controlling private certifiers and develop existing paths. Therefore, I do find that EU's supranational aspirations had led to policy compromises, the upshot of which was the diffusion of public-private interactions from the current to the proposed regime.

5.3. **Hypothesis #3:** Private Interests influence on the New Certification Framework

To examine the influence of private interests on this policy process, I rely on CSA's stakeholder's engagement documents and trace how the different interests were divided between the groups, and which interests were eventually expressed in the agreed text. More than twenty different interest groups were involved, including product manufacturers, service providers, certification bodies, and standardization bodies.

I found that industry actors favored the proposed certification framework from the very beginning. According to an ENISA representative: 'Industry and private certification bodies pressured national policymakers to agree on the harmonized certification framework. They used the current fragmentation and consequent regulatory burden to push their public officials to agree on CSA. Since the EU has many export-oriented industries, the companies realized that a strong EU brand is a more desirable selling point than national brands.' This approach was expressed through a Parliament amendment that recognized how manufacturers face increased costs due to fragmentation, and why mutual recognition among national certification bodies should be promoted.

I compared the agreed act with the positions of different private groups and found that unanimous issues were added to the text. For instance, the need to allow self-assessment through first-party certification was promoted by the Parliament and Council, stressing the importance of keeping certificates voluntary, or the decision that the validity of schemes should be decided on a case-by-case basis - all added as amendments to the text.

Issues where private groups were less successful include the requirement that certification for high assurance will remain national rather than turn European, the idea of extending SOG-IS instead of establishing a new framework, keeping issuance of certificates in the hands of public authorities, and the insistence of certification bodies on establishing

mandatory certification requirements. The common denominator of all these issues is the fact that only few private groups promoted them.

Therefore, industry groups that benefit from decreased fragmentation in certification requirements and private certification bodies that significantly increase their market opportunities under the proposed regime were able to attain additional provisions, tipping the balance in their favor. It seems that they were not busy with issues of national control over private certification bodies. Thus, I do find that private actors significantly capitalized on the proposed regime change, and therefore offered little resistance to institutional layering practices and enhanced national control over private certification bodies.

6 – DISCUSSION & CONCLUSION

This study traces the institutional change in EU cybersecurity certification from the pre- to post-CSA era. Pre-CSA, I found that the current certification regime has operated through four distinct institutional paths that have been recognized by international, national, or industry actors to various degrees. Private certification bodies only certify on behalf of industry actors based on private schemes that are recognized contingent on market decisions. Public-private interactions among national certification bodies and private laboratories demonstrate significant public control over the operations of private labs through public licensing, auditing, and sanctioning. Post-CSA, this type of public-private interaction diffused to new certification paths, which characterizes how national agencies control private certification bodies. Based on the new act, the EU has integrated new European certification paths into existing ones, and advanced the publicization of private certification bodies; on the one hand, the EU has upgraded their role to certify based on European schemes across Member States. On the other hand, it strengthened public control over their operations through national registration requirements, public accreditation measures, and comprehensive monitoring and enforcement mechanisms, including sanctions and public disclosures of their flaws.

I use Arcuri's (2015) term - publicization - to describe the elevation of voluntary enlisted private governance actors under increased public control measures. This type of interaction challenges the dichotomous understanding of public control over private governance actors. Rather than full or no control by public authorities, publicization embodies a notion whereby voluntary enlisted governance actors are free to choose whether they become subordinate to enhanced public control over a market-driven governance

practice. Such strict control measures and aggressive public involvement, along with substantial public elevation in the status of private certifiers, cast doubt on the "privateness" of this market-driven governance practice.

To explain this rather unexplored type of state interaction with private regulators, I delved into the institutional context of the newly crafted interactions, arguing that they do not evolve in a void. I studied them as part of the entire institutional change in EU cybersecurity certification, which was designed in the wake of a compromise between EU, Member States, and private interest groups.

I first described how EU policymakers created the new certification paths on top of existing ones, adding new layers to current institutional frameworks. Then, I found that Member States that enjoy strong veto powers but low discretion in the interpretation of new rules led to policy changes in the proposed framework, increasing public control over private certification bodies along similar lines as nations currently control private laboratories. Even though the strong states did not beget new institutional layer for certification, they were able to dictate the type of public-private interactions it will embody, and diffused public control patterns from current to the planned institutional framework. This demonstrates Capano's (2018) argument that the practice of institutional layering can also serve to stabilize and further legitimize the balance of power in existing institutional frameworks. I also found that the boost to EU's supranational aspirations, along with the decrease in regulatory burden for industry actors and the new market opportunities for private certification bodies, allowed all these parties to come to terms on national control measures over private certification bodies.

Thus, the publicization of private governance actors was a political compromise led by actors with strong veto powers and low discretion capacities, which were able to diffuse current public control practices over private governance actors to the prospective framework. This highlights a rather unexplored link between private governance and the institutional change literature, demonstrating how the causes for certain modes of institutional change hold explanatory powers for understanding why certain types of public-private interactions have emerged.

This study also contributes to our understanding of political battles in the cybersecurity policy arena. On the one hand, I find that Member States pushed for layering practices in order to increase the stability and legitimacy of current, nationally dominant institutional frameworks for certification. I show how dominant Member States are in current paths for certification, and why they were able to impose a policy compromise on the EU, preventing substantial divergence from current institutional paths and maintaining their

central role in this policy arena. The EU, on the other hand, was also successful in promoting the link between cybersecurity issues and its Single Market approach, further legitimizing its intervention in this policy field. As an IGO, the EU had also broadened previous political tactics that were used in EU's New Approach for harmonizing standards to circumvent Member States by governing through certification. The EU was willing to agree on national control over private certifiers in exchange for securing a long-term EU interest of increased involvement in cybersecurity governance. The CSA is another round of conflict between EU and Member States over influence in the cybersecurity arena.

Bringing together the literature on private governance with research on standardization, certification, endogenous institutional change, and cybersecurity governance, this study is conducive to three important elements. First, it increases our understanding with respect to the development of a rarely explored form of public-private interaction – the publicization of private governance practices by public authorities. Second, it contributes to the sparse literature on the governance of standards implementation through certification. While most studies address standard setting processes, this study highlights how and why standards are implemented through certification. Third, it contributes to the literature on endogenous institutional change by considering how modes of institutional change can explain interactions between public and private actors in newly created institutional frameworks.

The increasing publicness of market-driven governance practices casts doubts on the story line that tells us that we are witnessing a transformation from hierarchical governance to modes of soft governance, where multitude of public and private actors from different policy levels govern society through horizontal and soft instruments. This case-study shows that this framing does not particularly hold. The promise of horizontal governance, sometimes even without the government, has been replaced with new forms of control of public authorities over private governance actors. Initially, many market-driven regimes emerged as a reaction to the lack of state actions. Once public authorities had become involved, hierarchical or horizontal dynamics soon followed. This case study, however, allows us to broaden our understanding of post-market governance dynamics, setting forth a new form of state intervention in contemporary governance arrangements.

The limitations of this study relate to the challenge of understanding how and why a complex and rather under studied ecosystem of security certification operates. I was able to interview representatives from most involved sectors, but a larger sample of interviewees would have helped me to make even better sense of certification as a tool of governance.

While this study certainly adds to the body of knowledge on certification, this policy domain merits further research.

Looking ahead, future research avenues can further explore the explanatory power of modes of institutional change for realizing how and why public-private interactions emerge. In addition, comparative studies that assess different forms of publicization across sectors or nations would boost our understanding of what drives this new type of presence of the state in market-based governance mechanisms.

REFERENCES

- Abbott, K., Genschel, P., Snidal, D., and Zangl, B. (2015). 'Orchestration.' In: K. Abbott, P. Genschel, D. Snidal, & B. Zangl (Eds.), *International Organizations as Orchestrators* (pp. 3-36). Cambridge: Cambridge University Press. doi:10.1017/CBO9781139979696.002
- Abbott, K., Levi-Faur, D. and Snidal, D. (2017). 'Introducing Regulatory Intermediaries', *The ANNALS of the American Academy of Political and Social Science* 670(1): 6-13
- Abbott, K., Genschel, P., Snidal, D., Zangl, B. (2019). 'Competence Versus Control: The Governor's Dilemma.' *Regulation & Governance*. doi:10.1111/rego.12234
- Ackrill, R., Kay, A. (2006). 'Historical-institutionalist Perspectives on the Development of the EU Budget System.' *Journal of European Public Policy* (13): 113-33
- Arcuri, A. (2015). 'The Transformation of Organic Regulation: The Ambiguous Effects of Publicization.' *Regulation & Governance* 9: 144-59
- Backman, S. (2016). 'The Institutionalization of Cybersecurity Management at the EU-level.' *Master Thesis in the program of Politics & War, The Swedish Defense University*
- Baldwin, R. and Cave, M. (1999) *Understanding Regulation: Theory, Strategy and Practice*, Oxford: Oxford University Press.
- Bartley, T. (2007). 'Institutional Emergence in An Era of Globalization: The Rise of Transnational Private Regulation of Labor and Environmental Conditions.' *American Journal of Sociology* 113, 297-351.
- Bartley, T. (2011). 'Transnational Governance as the Layering of Rule: Intersections of Public and Private Standards.' *Theoretical Inquiries in Law* 12(2) : 517-542
- Bendiek, A., Bossong, R., and Schulze, M. (2017). 'The EU's revised cybersecurity strategy: half-hearted progress on far reaching challenges (SWP Comments, 47/2017).' *Berlin: Stiftung Wissenschaft und Politik – SWP- Deutsches Institut für Internationale Politik und Sicherheit*
- Bernstein S., B. Cashore. (2007). 'Can non-state Global Governance be Legitimate? An Analytical Framework.' *Regulation & Governance* 1(4): 347-71.
- Borraz, O. (2007). 'Governing Standards: The Rise of Standardization Processes in France and EU.' *Governance* 20(1):57-84
- Borzel, T. A., Risse, T. (2010). 'Governance without a state: Can it work?', *Regulation & Governance* 4:113-134
- Brunsson, Nils, and Bengt Jacobsson, (eds.) (2000). *A World of Standards*. Oxford: Oxford University Press.
- Bruszt, L. (2008). 'Multi-level Governance – the Eastern Versions: Emerging Patterns of Regional Developmental Governance in the New Member States.' *Regional and Federal Studies* 18: 607-27
- Büthe, T. and Mattli, W. (2011) *The New Global Rulers: The Privatization of Regulation in the World Economy*, Princeton: Princeton University Press.
- Capano, G. (2018). 'Reconceptualizing layering—From mode of institutional change to mode of institutional design: Types and outputs.' *Public Administration*. DOI: 10.1111/padm.12583
- Cashore, B. (2002). 'Legitimacy and the Privatization of Environmental Governance: How Non-State Market-Driven (NSMD) Governance Systems Gain Rule-Making Authority.' *Governance* 15 (4): 503-529.
- Christou, G. (2016). *Cybersecurity in the European Union. Resilience and adaptability in governance policy*. London: Palgrave.
- Donahue, J. and Zeckhauser, R.J. (2008). 'Public-Private Collaboration.' In: Goodin, R., Moran, M. and Rein, M. (Eds.). *The Oxford Handbook of Public Policy*, Oxford University Press, Oxford, 509-510.
- Egan, M. (2001). *Constructing a European Market – Standards, Regulation, and Governance*. Oxford: Oxford University Press.
- Fouilleux E., A. Loconto. (2016). 'Voluntary Standards, certification, and accreditation in the global organic agriculture field: a tripartite model of techno-politics.' *Agriculture and Human Values* 34(1):1-14.

- Frankel, C. and E. Hojbjerg. (2007). 'The Constitution of a Transnational Policy Field: Negotiating the EU Internal Market for Products.' *Journal of European Public Policy* 14(1): 96-114
- Freiberg, A. (2017) *Regulation in Australia*, Sydney: Federation Press
- French Senate. (2017). 'Draft resolution on the proposal for a regulation on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act").' *Commission des Affaires Europeennes*.
- George, A. L., & Bennett, A. (2005). *Case studies and theory development in the social sciences*. Cambridge: MIT Press.
- Grabosky, P. (2013). 'Beyond Responsive Regulation: The Expanding Role of non-state Actors in the Regulatory Process.' *Regulation & Governance* 7: 114-123.
- Grabs, J. (2018). 'Assessing the Institutionalization of Private Sustainability Governance In a Changing Coffee Sector.' *Regulation & Governance*. <https://doi.org/10.1111/rego.12212>
- Gulbrandsen L. H. (2014). 'Dynamic Governance Interactions: Evolutionary Effects of State Responses to non-state Certification Programs.' *Regulation & Governance* 8: 74-92.
- Hacker, J. S., (2004). 'Privatizing Risk without Privatizing the Welfare State: The Hidden Politics of Social Policy Retrenchment in the United States. *The American Political Science Review* (98): 243–60.
- Havighurst, C. (1994). 'Foreword: The Place of Private Accrediting among the Instruments of Government.' *Law and Contemporary Problems* (57): 1-14
- Hysing, E. (2009). 'From Government to Governance? A Comparison of Environmental Governing in Swedish Forestry and Transport.' *Governance* 22 (4): 647-72.
- Knill C. and D. Lehmkuhl. (2002). 'Private Actors and the State: Internationalization and Changing Patterns of Governance.' *Governance* 15(1): 41-63.
- Loconto, A. and Busch, L. (2010). 'Standards, techno-economic networks, and playing fields: Performing the global market economy', *Review of International Political Economy* 17(3): 507–536
- Loconto, A. M. (2017). 'Models of Assurance', *The ANNALS of the American Academy of Political and Social Science* 670(1): 112–132
- Lytton T. D. (2014). 'Competitive Third-Party Regulation: How Private Certification Can Overcome Constraints that Frustrate Government Regulation.' *Theoretical Inquiries in Law* (15)2: 539-71.
- Odermatt, J. (2018). 'The European Union as a Cybersecurity Actor.' In: S. Blockmans and P. Koutrakos (Eds.), *Research Handbook on the EU's Common Foreign and Security Policy (chapter 17)*. Edward Elgar Publishing.
- Schabhusser, G. (2017). 'The Cybersecurity Act and the Future Role of ENISA from a German National Perspective.' *Federal Office for Information Security (BSI)*
- Spruyt, H. (2001). 'The supply and demand of governance in standard-setting: insights from the past.' *Journal of European Public Policy* 8 (3): 371-391
- Streeck, W., Thelen, K. (2005). *Institutional Changes in Advanced Political Economies*. Oxford University Press, Oxford.
- Thatcher, M., Coen, D. (2008). 'Reshaping European Regulatory Space: An Evolutionary Analysis.' *West European Politics* 31: 806–36.
- Thelen, K. (2003). 'How Institutions Evolve: Insights from Comparative-historical Analysis. In: Mahoney J, Rueschemeyer D (Eds.) *Comparative Historical Analysis in the Social Sciences*, pp. 208–240. Cambridge University Press, New York, NY.
- Thelen, K. (2004). *How Institutions Evolve: The Political Economy of Skills in Germany, Britain, the United States and Japan*. Cambridge University Press, New York, NY.
- Wessel, R. A. (2015). 'Towards EU Cybersecurity Law: Regulating a New Policy Field.' In N. Tsagourias, & R. Buchan (Eds.), *International Law and Cyberspace* (pp. 403-425). (Research Handbooks in International Law series). Edward Elgar Publishing.

Table 1: Public-Private Interactions in EU’s Cybersecurity Certification Regimes pre- and post-CSA

	<u>Pre-CSA</u> [Private Labs ↔ National Authorities]	<u>Post-CSA</u> [Private Certification Bodies ↔ National Authorities]
<i>Public Authorization to Operate</i>	Private labs have to be publicly licensed and can be denied licensing in multiple states.	Private certification bodies have to be registered by Member States.
<i>Public Deployment of Regulatory Frameworks</i>	National authorities predominantly prompt Common Criteria and national certification schemes that set evaluation requirement.	EU schemes developed by EU institutions and Member States set the framework for monitoring and enforcing requirements from private certification bodies.
<i>Public Accreditation of Private Actors</i>	Private labs are accredited by national certification bodies.	Accreditation takes place through a joint effort of national accreditation bodies and national cyber agencies.
<i>Public Audit of Private Operations</i>	Personnel, facilities, and processes of labs are constantly audited.	National agencies across the Union monitor private certification bodies comprehensively through post-certification, information sharing mechanisms between public agencies. Public investigations of complaints also take place.
<i>Public Sanctions over Private Actors</i>	Public certification bodies can revoke the license of labs.	Public accreditation bodies can suspend and restrict the operation of private actors. National agencies can sanction and publicly undermine the reputation of private certification bodies.

Figure 1: Pre-CSA Cybersecurity Certification Paths in the EU

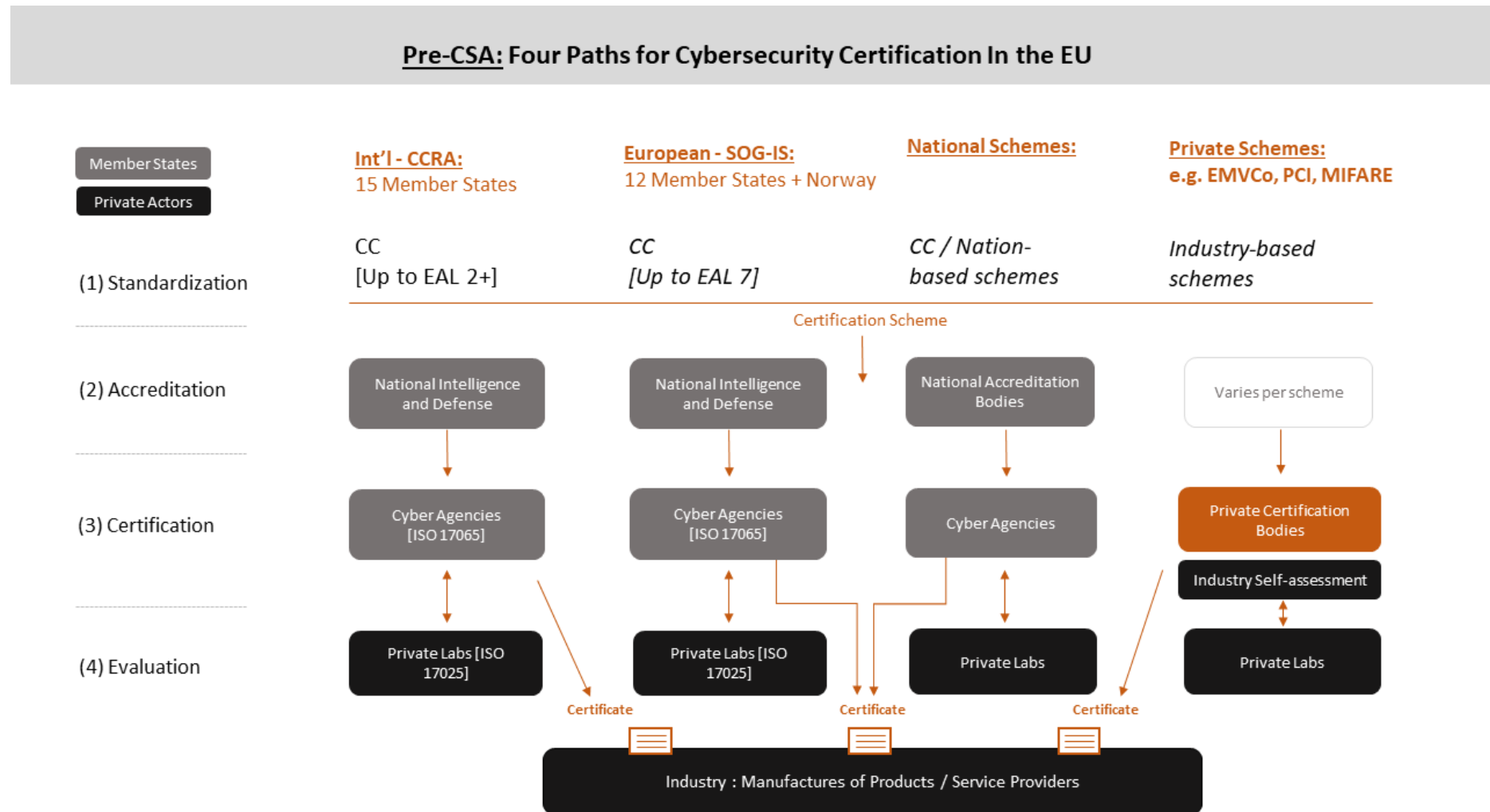
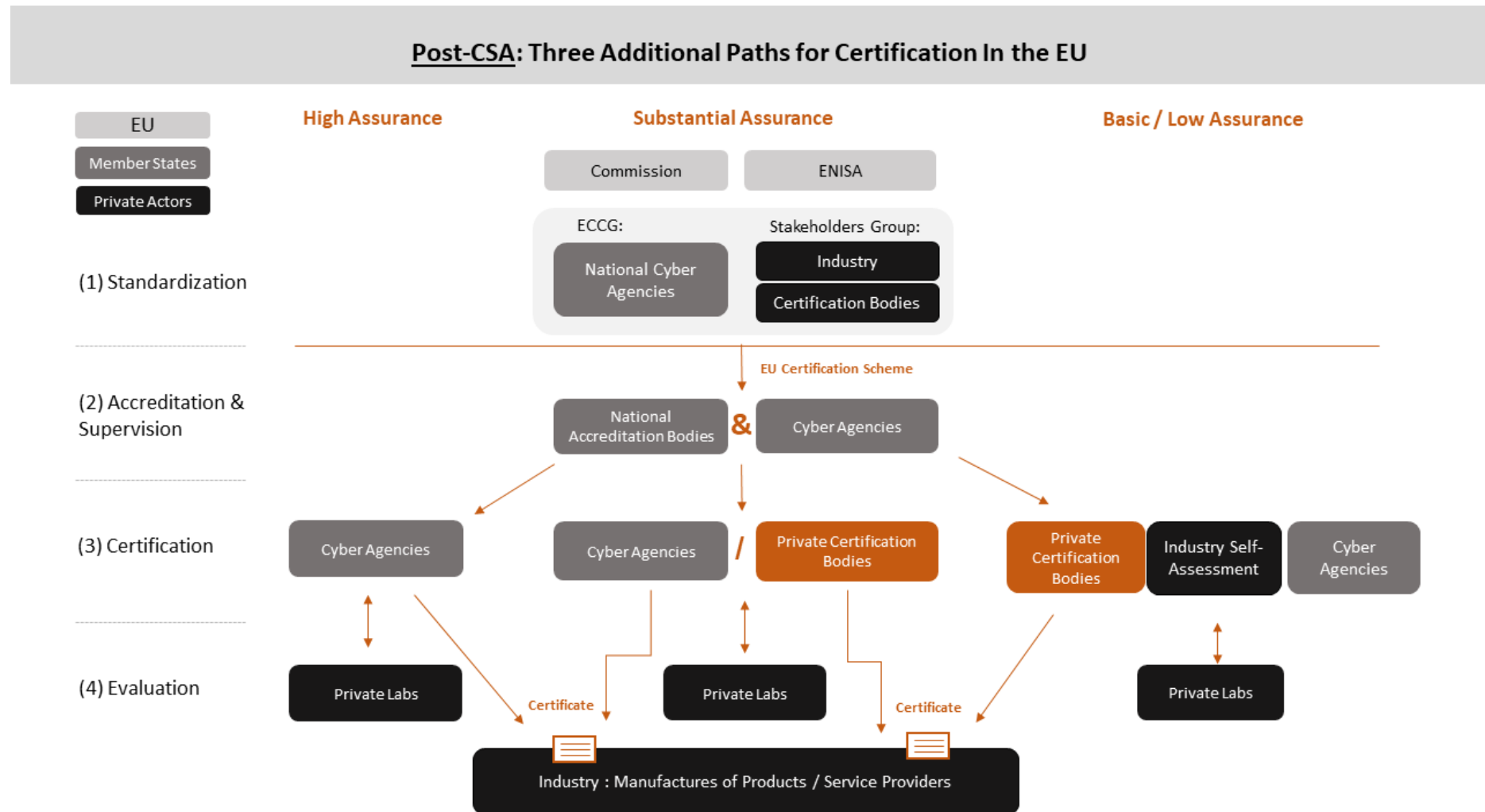


Figure 2: Post-CSA's Additional EU Cybersecurity Certification Paths



APPENDIX #1: Analyzed Policy Papers on CSA from EU Institutions

	Document Name	Organization(s)	Date
1	Commission Communication on Strengthening Europe's cyber resilience systems and Fostering a Competitive and Innovative Cybersecurity Industry	EU Commission	July 2016
2	State of the Union 2017: The Commission scales up its response to cyberattacks	EU Commission	September 2017
3	CSA Impact Assessments Parts 1 - 6	EU Commission	September 2017
4	Regulation Proposal: The Cybersecurity Act	EU Commission	September 2017
5	Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU	EU Parliament & Council	September 2017
6	EPRS Briefing: EU Cybersecurity Agency and cybersecurity certification	EU Parliament	December 2017
7	Draft Opinion on the Cybersecurity Act - Civil Liberties, Justice, and Home Affairs Committee	EU Parliament	January 2018
8	Draft Opinion on the Cybersecurity Act - IMCO Committee	EU Parliament	February 2018
9	Draft Opinion on the Cybersecurity Act - ITRE Committee	EU Parliament	March 2018
10	Draft Opinion on the Cybersecurity Act - Civil Liberties, Justice, and Home Affairs Committee	EU Parliament	March 2018
11	Draft Opinion on the Cybersecurity Act - IMCO Committee	EU Parliament	May 2018
12	CSA Amendments	EU Council	May 2018
13	CSA Amendments	EU Parliament	July 2018
14	EPRS Briefing: ENISA and the New Cybersecurity Act	EU Parliament	September 2018
15	CSA Agreed Text	EU Commission	December 2018
16	EPRS Briefing: ENISA and the New Cybersecurity Act	EU Parliament	February 2019

APPENDIX #2: Analyzed Position Papers on CSA by Stakeholders

	Document Name	Organization(s)	Date
1	Security certification and labelling	EUROSMART	July 2017
2	Joint FIEEC-ZVEI Position on Cybersecurity	FIEEC & ZVEI	October 2017
3	Position Paper: Initial Position on the EU Cybersecurity Package	EC SO	October 2017
4	Clusit and Information Security & Privacy	Clusit	November 2017
5	The proposal for a Cybersecurity Act - a BusinessEurope position paper	BusinessEurope	November 2017
6	DIGITALEUROPE's position paper on the European Commission's Proposal for a European Framework for Cybersecurity Certification Scheme for ICT products and services	DIGITALEUROPE	December 2017
7	SAFECode perspective on Cybersecurity Certification	SAFECode	January 2018
8	Cybersecurity – A Strategic Task for Europe	VDMA	February 2018
9	The EU Cybersecurity Act proposal	AmCham EU	February 2018
10	Industry Challenges & Opportunities in Future Cybersecurity Certification Schemes	STMicroelectronics	March 2018
11	Toward EU Cybersecurity Certification Framework: Statement as Manufacturer and Service Provider	G+D Mobile Security	March 2018
12	AIOTI position on the EU Cybersecurity Act Proposal	AIOTI – Alliance for Internet of Things Innovation	May 2018
13	Cross-industry and standards development organisations open letter on the EU Cybersecurity certification framework proposal	Eight associations from industry and standards development sectors	June 2018
14	SAFECode Comments on EU Cybersecurity Legislation	SAFECode	October 2018
15	The International TIC Sector Welcomes the Proposed Measures by the European Commission	IFIA & CIOC International	No date
16	ETSI Position Paper on draft Regulation 2017/0225 “Cybersecurity Act”	ETSI	No date

APPENDIX #3: Analyzed ENISA Reports on Cybersecurity Certification

	Document Name	Date
1	Security Certification Practice in the EU	October 2013
2	Smart Grid Cybersecurity Certification: Minutes of the Workshop	September 2014
3	Definition of Cybersecurity: Gaps and Overlaps in Standardization	December 2015
4	Governance framework for European standardization	December 2015
5	Challenges of security certification in emerging ICT environments	December 2016
6	Considerations on ICT security certification in EU: Survey Report	August 2017
7	Improving recognition of ICT security standards	December 2017
8	Overview of ICT certification laboratories	January 2018

APPENDIX #4: Interviews Conducted

Organization Type	Number of Interviews
EU Commission	2
EU Council	1
EU Parliament	1
ENISA	1
National Certification Agency	1
Private Certification Bodies	2
Private Evaluation Laboratories	4
Product Manufacturers	4
Digital Service Providers	1
Industry Associations	1

CONCLUSION: POLICY DESIGN FOR DIGITAL TECHNOLOGY RISKS

Over the past decades, policymakers across the globe are trying to produce policies that would properly govern the alarming risks that arise from digital technologies. Nevertheless, the constant failures in preventing data breaches and protecting against cyber threats, along with massive privacy infringements that erode core values such as liberty, anonymity, and freedom of speech, create a sense of urgency in understanding how and why cybersecurity and privacy risks are governed. Insecure digital systems and the lack of effective checks and balances on personal information flows destabilize societies and question the ability of policymakers to properly handle continuous technological development. The understanding of how and by whom policy regimes are shaped to mitigate such risks is crucial for better coping with these policy failures. Furthermore, the analysis of such under-studied policy domains in the public policy literature holds a promise for advancing theories on the policy process and policy regime design further. By understanding how policy regimes for cybersecurity and privacy are constructed, and uncovering drivers for policy change in these spaces, we can better assess the development of public policies in regimes that are fragmented, where policies are developed in different levels of government, with a variety of government agencies involved, and through institutional structures that develop over time in a patchy nature.

Previous research devoted disjointed and fragmented efforts to the study of these pressing problems. Scholars have yet to apply the policy regime perspective to understand how and why the governance of cybersecurity and privacy develops. In this dissertation, I addressed these gaps by conceptualizing, theorizing, and empirically studying the drivers for the development of three policy regimes that govern cybersecurity and privacy-related policy problems in two central political systems – the US and the EU.

Summary of the research project and the work process

I have started my work on this project without realizing the plural dimensions in the relationships between privacy and national security, and with little understanding of how cybersecurity governance is designed. The scholarly works that did address privacy or cybersecurity provided only a glimpse on these regimes, with no up-to-date understanding of their development (e.g. Etzioni, 2011; Quigley and Roy, 2012; Hiller and Russel, 2013).

Coming from a computer science background, I mainly attached the cybersecurity challenge to technological complexity and the vulnerable nature of software and hardware appliances. I did not fully realize the disturbing impacts of insecure digital systems and the massive flows of personal information on vital principles such as privacy, anonymity, and liberty.

The surprising revelations in 2013 by whistle-blower Edward Snowden (Macaskill and Dance, 2013) motivated me to further explore how the design of massive surveillance infrastructures was promoted in the US without significant checks and balances. I realized that this would require research on historical policy patterns over national security and privacy dynamics, but there were only few existing works in the public policy literature that I could rely on. I further understood that in contrast to existent literature (Regan, 1995; Diffie and Landau, 2007; Solove, 2011), these relations have more than two dimensions, and in order to fully comprehend them I need to broaden the regime boundaries applied by existing studies.

The dissertation's first paper, entitled *Complementaries and Contradictions: National Security and Privacy Risks in U.S. Federal Policy, 1968–2018* (Sivan-Sevilla, 2018) was, to the best of my knowledge, the first attempt to empirically explore the plurality of dimensions between national security and privacy as constructed by US federal policies. This yielded novel results on the development of these dynamics over time and across policy arenas.

I found that federal policies design contradictory dynamics between national security and privacy in a rarely punctuated policy equilibrium. It takes severe security crises or significant privacy scandals to create the unusual political conditions for change in this policy regime. Moreover, the paper underscored newly captured independent variables that influence the construction of different types of relationships between the two goals. These include: the instrumental use of technological changes to frame policy problems, framings of policy issues and their associated policy arenas, characteristics of the policy process, and convergence of interests between commercial and governmental actors.

For the cybersecurity policy arena that mostly promotes complementary, but also contradictory dynamics between national security and privacy, the paper found high actor variance and significant influence from private interest groups. Still, this policy arena was the most packed and complex one. I was able to recognize different approaches taken by policymakers to the cybersecurity problem but could not realize how they affect policy outcomes and shape governance arrangements in this policy arena.

This motivated me to further dive into the cybersecurity policy arena and realize how and by whom cyber risk governance is shaped. In the second dissertation's chapter, entitled *Framing and Governing Cyber Risks: comparative analysis of US federal policies [1996-2018]*, I put forth a novel typology for realizing how cyber risks are governed by public policies and how shared ideas within this policy regime and different perceptions of the cybersecurity problem are translated into distinct governance frameworks across private sectors. To the best of my knowledge, this is the first attempt since Hood et al. (2001) to conceptualize public policies as risk governance frameworks and uncover the disconnection between risk framings and policy outcomes in cybersecurity governance arrangements.

The paper originally detected three distinct sub-regimes across private sectors based on policymakers' understandings of the cybersecurity problem that perceived cybersecurity as a problem of traditional infrastructure, data protection, or as a tool to safeguard financial interests. This finding empirically validates Science and Technology Scholars' (STS) arguments about the importance of meanings and framings to policymakers' choices (Nissenbaum, 2005; Fichtner, 2018). I found that policymakers were bound to certain framings, assessments, and evaluations of cyber risks that informed their risk management policy decisions. The role of the government and the extent to which it dictated coercive risk management steps was loosely related to how risks were framed and were mostly designed based on early decision-making structures.

Moreover, while previous works on cybersecurity governance considered policies as one-dimensional (Weiss and Jankauskas, 2018), the novel typology for appreciating public policies as risk governance frameworks revealed how public policies shaped different categories in the cyber risk management process. Still, the government has been responding to the dynamic threat landscape only within the boundaries and paradigms of the decision-making structures that were decided upon during early regime development. For each regime, the government tried to improve risk management practices without considerably diverging from previous policy paths.

The results of this paper also revealed the different role of private actors across the three sub-regimes. The industry either collaborated with the government while being regulated by top-down hierarchical structures, or else it developed self-regulatory mechanisms. While private actors were perceived by policymakers as holding the expertise to assist and

complement governmental capacities in the field, I recognized different paths of influence of private authorities on cyber risk governance.

This had encouraged me to explore the operation of private regulators for cybersecurity in additional political systems. In the third dissertation paper, entitled *EU Publicization of Private Certifiers for Cybersecurity: explaining public-private interactions through the context of institutional change*, I studied the institutional frameworks for cybersecurity certification in the EU and traced their development over time. This paper recognized a rather less familiar interaction between public and private authorities: EU policymakers has been elevating voluntary enlisted private certification bodies, but at the same time increased public control over them. I framed this type of interaction as ‘publicization’ to capture the turning of private regulation to public one. To explain the evolvement of such interaction, I relied on the institutional context of regime change, and discovered the political contexts that designed such multi-level public-private arrangements within the EU cybersecurity policy regime.

This paper adds to our understanding of public-private interactions in the era of increasingly popular indirect governance arrangements (Abbott et al., 2017). The dichotomous understanding of public control over private governance actors implies either full control through delegation interactions or lack thereof in orchestration interactions. Contrariwise, EU policymakers have built a cybersecurity certification framework where public authorities increase their monitoring and enforcement capacities over voluntary enlisted private certification bodies, giving rise to an intriguing form of state intervention in market-driven governance practices.

Furthermore, this paper highlights how such soft but hierarchical public-private interaction can be explained based on the influence of regime actors with strong veto powers and low discretion in interpreting new institutional rules. Even though Member States did not initiate the creation of the new institutional layer for certification, they were able to dictate the type of public-private interactions it will embody, and diffused public control patterns from current to the newly proposed institutional framework. This demonstrates Capano’s (2018) argument that the practice of institutional layering can also serve to stabilize and further legitimize the balance of power in existing institutional frameworks.

This creates a novel link between the literature on endogenous institutional change and private governance. In contrast to scholars of institutional change that mostly ignore the public

or private nature of institutional frameworks and do not link modes of change with the distribution of public or private authorities, this paper found that causes for institutional change can throw light on why policymakers choose certain public-private interactions when designing a regime change.

The paper also questions the transformation from hierarchical governance to modes of soft governance. New forms of control of public authorities over private governance actors has superseded the promise of horizontal governance, even without government at times. Initially, many market-driven regimes emerged as a reaction to the lack of state actions. Once public authorities had become involved, hierarchical or horizontal dynamics soon followed. The EU cybersecurity certification regime, however, allows us to broaden our understanding of post-market governance dynamics, suggesting a new form of state intervention in private governance arrangements.

Going back to the dissertation's objectives

Overall, the aims of this dissertation have been fulfilled. *First*, by embracing a policy regime approach, the three dissertation papers were able to capture complex dependent variables that incorporate: (1) variance in national security and privacy dynamics over time and across federal arenas in US federal policymaking, (2) variance in US cyber risk governance frameworks across sectors, and (3) temporal variance in public-private interactions between public authorities and private certification bodies in EU cybersecurity certification regime.

Second, the policy regime perspective allowed me to identify the micro-mechanisms that explain policy outcomes and advance theory of policy change: national security and privacy outcomes are predicated on the level of convergence of commercial and governmental interests and the characteristics of the policy process. This emphasizes the importance of policy arenas to types of policy outcomes. Furthermore, chosen policy paths for cyber risk governance are contingent on policymakers' decision-making structures that were institutionalized in early phases of regime development, rather than on risk framing in these policy spaces. This questions the importance of risk framings to policy outcomes and validates the significance of historical institutionalism to cybersecurity risk governance outputs. Finally, actors that drive certain types of institutional change are instrumental in determining the type of public-private

interactions in regime development, especially when they face little opposition from other groups.

Third, based on the captured variables in each regime, new research questions can be generated to further develop public policy theories and advance the study of contemporary governance frameworks in the era of continuous technological change. For instance, the analytical framework for studying national security and privacy dynamics can be applied to study dimensions of these dynamics in additional political systems. This would allow us to test whether similar independent variables across political systems account for national security and privacy outcomes. This is especially appealing in the age of increasing information collection practices by state and commercial authorities. Moreover, cyber risk governance can be compared across political systems based on the disconnection between risk frames and policy outcomes. The significance of early institutional structures can be compared within the same political systems, or more generally, across risk issues. This could increase our understanding of how cyber risks are framed in different political systems and how significant are historical policy decisions regarding the development of risk regimes. New research questions can also test the explanatory power of modes of institutional change for realizing how and why public-private interactions emerge. Further research on the publicization of private governance frameworks can help us draw conclusions on what drives this new type of presence of the state in market-based governance mechanisms.

The contribution of the dissertation to existing public policy research

This dissertation represents the first attempt, to the best of my knowledge, to study cybersecurity and privacy-related policy problems from a regime perspective, opening a promising opportunity for policy scholars to further engage in studying the governance of risks that arise from digital technologies. It highlights the significance of new factors when it comes to the design of policies for risk governance. These include the characteristics of the policy process, policymakers' risk perceptions, historical decisions on institutional structures, and the interests of actors with historically determined veto points. We learn that policies that accumulate in a patchy manner govern digital technology risks, and contextual settings and traditional drivers for institutional stagnation or change influence decision-making.

The dissertation contributes to the literature on risk regulatory regimes. Risk scholars tend not to focus on cybersecurity and privacy risks. They also usually delineate the political nature of risk governance decisions and pay less attention to how public policies link between stated risk perceptions and regime design (Moss, 2002; Renn, 2008; Black, 2010; Vogel, 2012; Wiener, 2013; Rothstein et al., 2013; Alemanno, 2016). By suggesting a novel typology for understanding how public policies create risk governance frameworks and through studying the link between risk frames and policy outcomes, this dissertation takes us one step closer to understanding how governments manage risks for societies. It lays out policymakers' techniques for managing cyber risks, emphasizing the difficulty to diverge from early risk governance decisions while wedding historical institutionalism theory (e.g. Pierson, 2004) and risk governance.

The dissertation also enriches contemporary debates by theorists of regulation on the development of hybrid forms of indirect governance. Policy systems were recently conceptualized as a three- rather than two-party systems that include rule maker, rule intermediary, and rule taker (Abbott et al., 2017). This describes the shift from traditional state-centric approaches with hierarchically organized government agencies to multi-level systems that distribute authority across private and public bodies (Gunningham et al., 1998; Coglianese & Lazer, 2003; Gilad, 2011; Levi-Faur, 2011; Klinke & Renn 2011). This dissertation leverages changes in intermediation strategies to study the institutionalization of regulatory-intermediaries in risk-governance frameworks. But while most scholars address private intermediation in the forms of delegation or orchestration, this dissertation highlights a rather unexplored case of taking public ownership over private governance practices. This form of state intervention questions the two-dimensional understanding of either strict top-down or collaborative relations between public and private authorities. Through soft engagement with private governance actors while exercising hierarchical control over their operations, the state is more relevant than ever, instrumentally steering private governance actors to advance its goals. The capturing of this regulatory phenomenon is important for understanding multi-level and hybrid forms of governance in contemporary arrangements.

Beyond these theoretical contributions to existing debates in the public policy literature, the dissertation's findings can travel to policy spaces with similar characteristics. The dissertation highlights the role of focusing events in domains that demonstrate difficult to change policy equilibriums such as the foreign intelligence domains, or for policy spaces that

are fragmented and disjointed such as the cybersecurity policy domain. These domains are likely to provide great influence to veto players, who can rather easily prevent changes from taking place in these arenas due to their complexity and lack of single capable change agents. This is likely to only allow a gradual institutional change at best. The dissertation also reveals the impact of the convergence of interests between commercial and government actors over issues that are directly related to state's sovereignty and powers (Genschel and Jachtenfuchs, 2013), such as the national security arena. The instrumental use of technological change is also demonstrated by the findings of this dissertation, highlighting possible attention focus to concurrent debates in policy parliaments about advancements of technology and their consequences for society. Technology is likely to be used instrumentally by different stakeholders in the policy process. For governmental attempts to manage risks for society in certain domains, over the course of several decades, this dissertation offers a unique analytical approach on how to study public policies as risk governance frameworks and examine the possible disconnection between framing and policy outputs. In addition, policy fields that experience gradual institutional change under national and supra-national tensions can be studied from the perspective of veto players attempts to legitimize old structures in the attempts of policymakers to 'take-over' market-driven governance structures.

This research project also has a significant methodological contribution that can 'travel' across nations and contexts. It employs a novel analytical framework for studying the plurality of dynamics between national security and privacy. Rather than framing them as contradictory, this dissertation shows the full spectrum of contradictory and complementary relations between the two goals, allowing for better understanding of the influence of conflicting political forces in these policy arenas and highlighting the importance of policy context to policy outcomes. This novel typology can be applied to study dimensions of these dynamics in additional political systems. In addition, this research also develops a novel typology for studying public policies as risk governance frameworks. As policymakers are increasingly occupied with governing risks for society, this can help advance future risk governance studies across nations and issues.

The implications of the dissertation for other audiences

Whilst the dissertation is rooted within the academic public policy literature, it can be of interest to additional audiences. For instance, the policy regime perspective on cybersecurity and privacy governance can be appealing for sociology scholars who are interested in the

balance of power within institutional structures (e.g. Mayer, 2002) and study isomorphism to realize how institutional practices diffuse over time and across organizations (DiMaggio and Powell, 1983). The present dissertation features these diffusion patterns that stem from power struggles and are comparable to isomorphism patterns in organizational settings.

Moreover, political scientists who are interested in the balance of power in political systems (e.g. Bachrach and Baratz, 1963; Clegg, 1989; Lukes, 2005) might be interested in comparing power struggles over policy change in the governance of digital risks with more traditional security studies domains (e.g. Jervis, 2004). Similar policy actors are influential in both domains, but the dissertation allows us to appreciate the role of commercial interests, and the ability of private interests to significantly influence security-related decisions by the state.

Finally, this research project has important practical implications and may also appeal to policy practitioners. Policymakers are currently wrestling with cybersecurity and privacy issues, and mostly address the technical rather than the political contexts of these challenges (Clark, 2014; Siboni and Sivan-Sevilla, 2018). Nonetheless, they may utilize insights from this research to understand how such policy regimes are designed and what to pay heed to in considering future policy developments. They can also choose strategic approaches for changing the identified equilibriums in the studied policy regimes. For instance, the rarely punctuated policy equilibrium that set certain contradictory dynamics between national security and privacy necessitates the development of guidelines for checks and balances in controversial national security decisions that bear uncertain privacy implications. Following the findings of this dissertation, we realize that such checks and balances are less likely to be coded via policies, but should be developed by other actors in the ecosystem to overcome the stagnation of current policy regimes. Moreover, the limited response by governments to cyber threats might require enhanced incentives for private actors to develop more flexible governance solutions.

Proposed directions for future research

This dissertation leaves several avenues for future research. First, it informs the studying of the broader context of indirect governance arrangements in governing systemic risks across political systems. While the risk governance literature frames cyber risks as one example of systemic risks (Goldin and Mariathan, 2014; Renn et al., 2019), future research

can suggest broadening the study of indirect governance across systemic risks to assess the role of intermediaries in risk governance. These intermediaries are embedded in institutional settings and work based on their private interests. They might introduce bias and subjectivity in key functional capacities of the risk-governance process. Comparatively assessing the operation of such intermediaries can contribute to understanding additional political contexts of indirect governance arrangements.

Since the dissertation reveals the role of industry associations in the field of private cybersecurity certification, their role could be further studied with regard to privacy issues as well. Following the ubiquities tracking and targeting of individuals in the online advertising ecosystem, industry associations such as the Interactive Advertising Bureau (IAB) adopt different consumer protection and empowerment mechanisms (Dwyer et al., 2017; ENISA, 2018). Absent significant policy regimes, industry associations take the role of regulators. Future research can assess when and how a standardization body such as IAB becomes an effective regulator, emphasizing how policy regimes for digital technology risks are constructed in a bottom-up manner.

Last but not least, future research can realize the impact of policy regimes design on innovation. It can assess whether policy regimes for cybersecurity affect innovation capacities of regulated companies differently. As policymakers endeavor to balance between coercing and incentivizing cybersecurity protections, the dissertation in question reveals several paths for cyber risk governance via private actors. I found different contextual and operational factors for certification across different institutional paths in the EU; future research can assess whether and how working through different certification process impacts the innovation possibilities of certified producers. This will contribute to the current literature that pays only little attention to the link between certification and innovation and is generally ambiguous on how regulation influences innovation (Ashford et al., 1985; Pelkmans and Renda, 2014).

Bibliography

- Abbott, K. W., Levi-Faur, D. and Snidal, D. 2017. "Introducing Regulatory Intermediaries", *The ANNALS of the American Academy of Political and Social Science* 670(1): 6–13.
- Aleman, A. 2016. "Risk and Regulation." In: Burgess A., Aleman A., Zinn J. (eds.), *Routledge Handbook of Risk Studies*, pp. 191-203.
- Ahford N. A., Ayers C., and Stone R. 1985. "Using Regulation to change the market for innovation." *Harvard Environmental Law Review* 9(2): 419-66.
- Bachrach P. and Baratz, M. S. 1963. "Decisions and nondecisions: An analytical framework." *American political science review* 57(3): 632-42.
- Black, J. 2010. "The Role of Risk in the Regulatory Process", In: Baldwin R., Cave M., and Lodge M. (eds.) *The Oxford Handbook of Regulation*, pp. 302-48.
- Capano, G. (2018). 'Reconceptualizing layering—From mode of institutional change to mode of institutional design: Types and outputs.' *Public Administration*. DOI: 10.1111/padm.12583
- Clark D., Berson T., and Lin Herbert S. 2014. "At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues." *Committee on Developing a Cybersecurity Primer: Division on Engineering and Physical Sciences: National Research Council*
- Clegg, S. R. 1989. *Frameworks of power*. New York: Sage Publications.
- Coglianes, C. and Lazer, D. 2003. "Management-Based Regulation: Prescribing Private Management to Achieve Public Goals." *Law & Society Review* 37(4): 691–730.
- Diffie, W., and S. Landau. 2007. *Privacy on the Line: The Politics of Wiretapping and Encryption*. Updated and Expanded Edition. Cambridge: MIT Press.
- DiMaggio, P. J. & W. Powell, "The iron cage revisited: institutional isomorphism and collective rationality in organizational fields", *American Sociological Review*, 48 (1983), 147-60.
- Dwyer, C., and Kanguri, A. 2017. "Malvertising: A Rising Threat to the Online Ecosystem." *Journal of Information Systems Applied Research (JISAR)* 10 (3): 29-37.
- The European Agency for Network and Information Security (ENISA). 2018. "The Value of Personal Online Data." Available here: <https://www.enisa.europa.eu/publications/info-notes/the-value-of-personal-online-data>
- Etzioni, A. 2011. "Cybersecurity in the Private Sector." *Issues in Science and Technology*, Vol 28, Issue 1.
- Fichtner, L. 2018. "What Kind of Cyber Security? Theorising Cyber Security and Mapping Approaches." *Internet Policy Review* (7)2.
- Genschel P., and M. Jachtenfuchs. 2013. *Beyond the Regulatory Polity?: The European Integration of Core State Powers*. New York: Oxford University Press.
- Gilad, S. 2011. "Process-Oriented Regulation: Conceptualization and Assessment." in D. Levi-Faur (ed.). *Handbook on the Politics of Regulation*. Edward Elgar Publishing.
- Goldin, I. and M. Mariathasan. 2014. *The Butterfly Defect: How Globalization Creates Systemic Risks, and What to do About it*. Princeton: Princeton University Press.
- Gunningham, N. and Sinclair, D. 1998. "Smart regulation." in P. Drahos (ed.): *Regulatory theory: foundations and applications*. Acton, Australia: The Australian National University Press, pp. 133–48.
- Hiller, J. S., and Russel, R.S. 2013. "The challenge and imperative of private sector cybersecurity: An international comparison." *Computer Law & Security Review* 29: 236-45.
- Hood C., Rothstein H., Baldwin R. 2001. *The Government of Risk: Understanding Risk Regulation Regimes*. Oxford, Oxford University Press.
- Jervis, R. "Cooperation Under the Security Dilemma." 2004. in Karen A. Mingst and Jack L. Snyder (eds.) *Essential Readings in World Politics*, 2nd edition, New York: Norton, pp. 309-322.
- Klinke A. and Renn O. 2011. "Adaptive and Integrative Governance on Risk and Uncertainty." *Journal of Risk Research* (15)3: 273-92
- Levi-Faur, D. 2011. "Regulation and regulatory governance." in D. Levi-Faur (ed.): *Handbook on the Politics of*

- Regulation*. Edward Elgar Publishing.
- Lukes S. 2005. *Power: A Radical View*. Basingstoke: Palgrave Macmillan.
- Macaskill, E. and Dance, G. 2013. "NSA Files: Decoded. What the Revelations Mean to You." *The Guardian*. Available here: <https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded>
- Mayer, N. Z. 2002. "Spinning disciplines: Critical management studies in the context of the transformation of management education." *Organization* 9(3): 365-385.
- Moss, D. 2002. *When all else fails: Government as the Ultimate Risk Manager*. Harvard University Press
- Nissenbaum, H. 2005. "Where Computer Security Meets National Security." *Ethics and Information Technology* 7, pp. 61-73.
- Pelkmans J. and Renda A. 2014. "Does EU Regulation hinder or stimulate innovation?" *Center for European Policy Studies*, Special Report No. 96.
- Pierson, P. 2004. *Politics in Time: History, Institutions, and Social Analysis*. Princeton, NJ: Princeton University Press.
- Quigley, K., & Roy, J. 2012. "Cyber-Security and Risk Management in an Interoperable World: An Examination of Governmental Action in North America." *Social Science Computer Review* 30(1): 83-94
- Regan, P.M. 1995. *Legislating Privacy: Technology, Social Values, and Public Policy*. Chapel Hill: UNC Press.
- Renn, O. 2008. *Risk Governance: Coping with Uncertainty in a Complex World*. Earthscan, London:UK
- Renn O., K. Lucas, A. Haas, and C. Jaeger. 2019. "Things are Different Today: The Challenge of Global Systemic Risks." *Journal of Risk Research* 22(4): 401-15.
- Rothstein, H. Borraz, O. Huber, M. "Risk and the limits of governance: Exploring varied patterns of risk-based governance across Europe." *Regulation & Governance* 7: 215-35.
- Siboni G. and Sivan-Sevilla I. 2018. "The role of the State in the Private-Sector Cybersecurity Challenge." *Georgetown Journal of International Affairs blog*. Available here: <https://www.georgetownjournalofinternationalaffairs.org/online-edition/2018/5/27/the-role-of-the-state-in-the-private-sector-cybersecurity-challenge>
- Sivan-Sevilla, I. 2018. "Complementaries and Contradictions: National Security and Privacy Risks in U.S. Federal Policy, 1968-2018." *Policy & Internet*. DOI: [10.1002/poi3.189](https://doi.org/10.1002/poi3.189)
- Solove, D. 2011. *Nothing to Hide: The False Tradeoff Between Privacy and Security*. New Haven: Yale: University Press
- Vogel, D. 2012. *The Politics of Precaution: Regulating Health, Safety, and Environmental Risks in Europe and the United States*. New Jersey: Princeton University Press.
- Weiss, M., V. Jankauskas. 2018. "Securing Cyberspace: How States Design Governance Arrangements". *Governance* 32(2): 259-75.
- Wiener, J. 2013. "The Politics of Precaution, and the Reality", *Regulation & Governance* 7: 258-65.

הפרטיות לטובת הבטחון הלאומי ומסבירות את המקורות לתופעה. כמו כן, הן מבליטות לראשונה את השפעתן של זירות המדיניות, מאפייני הליך המדיניות, ושונות השחקנים המעורבים בתהליך קבלת ההחלטות להבניית מערכת היחסים בין בטחון לאומי ופרטיות עבור החברה.

המאמר השני עוסק באופן בו קובעי מדיניות ציבורית בארה"ב ממסגרים סיכוני סייבר וכתוצאה מכך מעצבים ומסדירים את ניהולם. על בסיס ניתוח טקסט שיטתי וטופולוגיה חדשנית, מאמר זה מנתח 30 מופעי מדיניות משני העשורים האחרונים ומקודד מתוכם כ – 463 משפטי מפתח. המאמר מוצא כי ניהול סיכוני סייבר משתנה על פני מגזרים ולאורך זמן, על בסיס תפיסות סיכון שונות וכתוצאה ממבני ממשל אשר מוסדו בתחילת הדרך, וחושף באופן מפתיע קשר מאוד רופף בין האופן בו קובעי מדיניות ממסגרים סיכוני סייבר למדיניות שהם מכוננים בנושא.

המאמר השלישי מנתח דינמיקה שאיננה שכיחה בספרות המחקרית בין שחקנים מדינתיים לפרטיים. על ידי התבוננות בתחום ההתעדה והתקינה להגנת הסייבר באיחוד האירופי, המחקר משווה לאורך זמן בין תשתיות מוסדיות למתן תעודות אבטחה משני העשורים האחרונים. תוך התבססות על 58 מסמכי מדיניות וראיונות, המאמר בוחן כיצד שחקני מדיניות פרטיים זכו למקום מרכזי בזירה על ידי קובעי מדיניות, אך הפכו נתונים תחת שליטתם. תוצאות המחקר מעשירות את הידוע אודות הקונפליקט הפוליטי בין האיחוד האירופי למדינות החברות בתחומי מדיניות הגנת הסייבר. בנוסף, המאמר מחדש בכך שהוא מסביר את הדינמיקה בין שחקנים פרטיים למדינתיים על ידי ספרות של שינוי מוסדי שלרוב איננה עוסקת ביחסי הגומלין בין הפרטי לציבורי בעיצוב תשתיות מוסדיות חדשות. בכך, המאמר מערער את הקביעה הדו-קוטבית אודות המעבר מ'ממשלה לממשלות', חושף יחסי גומלין רכים אך היררכיים בין שחקני משילות פרטיים וציבוריים, ומלמד על תפקידה העדכני של המדינה במיגור סיכונים טכנולוגיים עבור החברה.

שלושת המאמרים יחדיו מאירים כיצד סיכונים הנובעים מטכנולוגיה מוקדרים על ידי המדינה דרך מאמצים נרחבים, שאינם מסונכרנים לרוב, ומתווספים כטלאי על גבי טלאי. המאמרים מביאים לקדמת הבמה את הקונטקסט המוסדי והפוליטי של החיבור בין טכנולוגיה למדיניות ציבורית. הם ממחישים תבניות מדאיגה אודות אובדן הזכות לפרטיות, קבעון מדיניות וחוסר הלימה עם מרחב האיומים הדינמי, והחלטות אינטרסנטיות בכל הנוגע לטיפול בסיכונים מרכזיים אלו. חשיבות המאמרים הללו נובעת גם מן העבודה כי הם מהווים תשתית עבור חוקרים נוספים לחיזוק הקשר האנליטי בין תאוריות של מדיניות ציבורית לסיכונים הנובעים מהתפתחותה של הטכנולוגיה.

תקציר

ההתפתחות הטכנולוגית בעשורים האחרונים הביאה עמה התקדמות ניכרת. יישומים טכנולוגיים ותשתיות מידע הפכו אינהרנטיים למהלך חיים תקין, שמירה על הבטחון, רווחה כלכלית, ושגשוג. מחד, פירות הטכנולוגיה מאפשרים כוח חישוב חסר תקדים, זרימת מידע גלובלית בין כל קצוות העולם, אספקת שירותים חיוניים, והתפתחות יוזמות חדשניות לקידום האנושות. מאידך, התלות הגוברת בטכנולוגיה מביאה עמה סיכונים הנובעים מאי-ודאות בנוגע לעמידותן, אמינותן, ושלמותן של תשתיות טכנולוגיות ומערכות מידע רגישות, יחד עם תאבון מתגבר לאיסוף מידע באופן שפוגע בזכות הפרטיות.

על אף מאמצייהם הגורפים של קובעי מדיניות ציבורית ברחבי העולם למגר סיכונים אבטחה במרחב הדיגיטלי, אנו עדים לעלייה מתמדת במספר הפריצות למערכות ולניצול תשתיות טכנולוגיות על ידי פֶּצְחָנִים למטרות רווח, גניבה של קניין רוחני, ופגיעה בתשתיות קריטיות כגון חשמל, מים, ותחבורה. בנוסף, כמויות המידע הנאספות באופן לא מפקח במרחב הדיגיטלי מאפשרות למדינות ושחקנים מסחריים לאסוף, לעבד, ולעשות שימוש במידע אישי ללא הרשאה מתאימה מצד בעלי המידע. מעבר לפגיעה אנושה בפרטיות, הסרת האיזונים והבלמים מתהליכי איסוף מידע פוגעת בזכויות בסיסיות נוספות כגון הזכות לחירות, אנונימיות, וחופש הביטוי.

באופן מפתיע, חוקרי מדיניות ציבורית עסקו מעט מאוד באופן בו קובעי מדיניות מנסים למגר סיכונים אלו. השדה המחקרי בתחום חסר הן עבודות אימפריות העוסקות באופן בו מערכות המדיניות הללו מתעצבות לאורך זמן ועל פני מגזרים שונים, והן הבנה תאורטית המאפשרת להסביר מדוע המערכות הללו פועלות בדרך מסוימת ומהם הגורמים המכריעים לעיצוב שינוי מדיניות בתחום. מעט המחקרים שכן עוסקים בנושא, מנתחים מופעי מדיניות בנקודות מסוימות בזמן, אשר אינם נתפסים כחלק ממכלול רחב יותר. החוקרים אינם מאמצים גישת ניתוח כוללת המאגדת את כל מאמצי המדיניות סביב בעיה מסוימת לכדי 'משטר מדיניות' אחד. גישה זו מאפשרת לקחת בחשבון את האינטרסים, המִבְּנִים המוסדיים, והרעיונות המשותפים המתפתחים על ידי שחקנים שונים בזירה לאורך זמן.

מחקר זה שואף למלא את החלל המתואר על מנת להבין כיצד ומדוע מתעצבים משטרי מדיניות ציבורית לקידום הגנת מרחב הסייבר ומיגור הפגיעה בפרטיות בשתי מערכות פוליטיות מרכזיות – ארה"ב והאיחוד האירופי. מטרות המחקר הן ראשית, המשגת משתנים תלויים מורכבים אודות ההתפתחות של משטרי המדיניות הללו לאורך זמן ועל פני מגזרים שונים. שנית, זיהוי המנגנונים אשר מובילים לשינויים במשטרי המדיניות על פני מערכות פוליטיות שונות. ושלישית, יצירת שאלות מחקר חדשות, על בסיס המשתנים התלויים והבלתי תלויים שנמצאו בכל משטר, על מנת להסביר התפתחות מדיניות ציבורית בעידן של קידמה טכנולוגית.

על כן, שלושת המאמרים הכלולים בדיסרטציה מתחקים אחר היווצרותם של משטרי מדיניות סביב בעיות העוסקות בהגנת הסייבר והפרטיות. המאמרים בוחנים את השחקנים, הוויכוחים, והתפתחות המשטרים לאורך זמן, וחוקרים מה מוביל לשינוי מדיניות בכל אחת מהזירות הללו. **המאמר הראשון** חוקר כיצד מערכת המדיניות הפדרלית בארה"ב מִבְּנָה את מערכת היחסים בין בטחון לאומי ופרטיות בחמשת העשורים האחרונים בראי ההתפתחות הטכנולוגית. המאמר מנתח 63 מופעי מדיניות לאורכן של שלוש זירות מדיניות, על בסיס מסגרת אנליטית חדשנית, על מנת להבין כיצד הליכי מדיניות ציבורית פוגעים, מייצרים פשרה, או משלימים בין בטחון לאומי לפרטיות. תוצאות המחקר מאוששות את אובדן

עבודה זו נעשתה בהדרכתו של

פרופ' דוד לוי-פאור

עיצוב משטרי מדיניות ציבורית להתמודדות עם סיכוני הטכנולוגיה

ניתוח היסטורי והשוואתי של מערכות מדיניות ציבורית בארה"ב
והאיחוד האירופי להגנת הסייבר ושמירה על הפרטיות

חיבור לשם קבלת תואר דוקטור בפילוסופיה

מאת עידו סיון-סביליה

הוגש מחדש לסנט האוניברסיטה העברית בירושלים

אוקטובר 2019

עיצוב משטרי מדיניות ציבורית להתמודדות עם סיכוני הטכנולוגיה

ניתוח היסטורי והשוואתי של מערכות מדיניות ציבורית בארה"ב
והאיחוד האירופי להגנת הסייבר ושמירה על הפרטיות

חיבור לשם קבלת תואר דוקטור בפילוסופיה

מאת עידו סיון-סביליה

הוגש מחדש לסנט האוניברסיטה העברית בירושלים

אוקטובר 2019