2017 9th International Conference on Cyber Conflict
Defending the Core
H. Rõigas, R. Jakschis, L. Lindström, T. Minárik (Eds.)
2017 © NATO CCD COE Publications, Tallinn

Trading Privacy for Security in Cyberspace: A Study Across the Dynamics of US Federal Laws and Regulations Between 1967 and 2016

Ido Sivan-Sevilla
The Federmann School of
Public Policy and Government
The Hebrew University of Jerusalem
Jerusalem, Israel
sivan018@umn.edu

Abstract: How does the legislative and regulatory agenda in the US trade between security and privacy in cyberspace? How can we explain the shift in the agenda towards more security and less privacy in the past 20 years? In order to answer these questions, I use an original dataset (N=85) of US federal laws and regulations on security and privacy between 1967 and 2016. Within the database, each policy event is classified according to the extent that security and privacy compete or complement each other. The findings indicate: (1) a shift in US federal policies towards greater security at the expense of privacy since the mid-1990s; and (2) a consistent lack of mandatory cyber security and privacy protections in the private sector. I explain this shift through emphasising: (1) the broken interest alliance over privacy between businesses and civil society organisations; (2) the increased power of the executive vis-à-vis Congress; and (3) the institutional position of security agencies and internet monopolies in the online environment. The contribution of this study stems from its empirical focus on the ambivalent role of the state in cyberspace over time. I trace the way the state promotes cyber security and privacy while increasingly collecting information or allowing others to do so at the expense of privacy and cyber security. Understanding how the state chooses between security and privacy increases our understanding of how governments manage cyberspace risks in the digital age.

Keywords: *cyber security, privacy, surveillance, resilience, regulation*

1. INTRODUCTION

This study asks how and why the US federal government has traded security and privacy over the past fifty years. The promotion of these goals complements and contradicts at the same time, and reveals the dual role of the state. Indeed, the growing dominance of cyberspace in modern life[1] requires the state to protect digitally stored personal information against new security and privacy threats. At the same time, emerging technologies and the reliance of modern societies on functioning digital systems allow the state and private actors to use cyberspace to collect personal information for security and economic purposes. This undermines privacy and threatens data security. Despite the puzzling nature of these two conflicting policy goals, little attention has been paid to the policy processes that decide between security and privacy in cyberspace.

I explore federal legislation, Executive Orders, Presidential Directives, federal register rules, federal policy guidelines, strategy documents, and novel court rulings (N=85) in the US federal arena between 1967 and 2016 and classify them to three distinct categories in which security and privacy compete with or complement each other. The findings indicate a policy shift towards greater government and privacy sector surveillance since the mid-1990s. This trend is evident throughout all branches of the federal government: (1) *the executive*, which was under close scrutiny by Congress over domestic surveillance issues in the 1970s, has been authorising surveillance without proper checks and balances and through 'temporary' tools that quickly became permanent. In the private sector, the executive led the way for unregulated market actors that rely on commodification of personal information for revenue; (2) *the legislature* has shifted from promoting policies that compromised between security and privacy during the 1970s and 1980s to passing legislation that encourages government information collection and letting private actors to collect personal information as they please; (3) and *the judiciary*, which was able to set the policy tone of restricting government surveillance in the 1970s, has been mostly unsuccessful in influencing the agenda in the same direction since.

The literature on the policy processes behind the conflicting roles of the state in cyberspace is surprisingly narrow. While only a few scholars address this discrepancy, they provide very limited explanations for the causes of each policy trend (Mendez and Mendez 2009; Deibert and Rohozinski 2010). Other policy scholars address either privacy (Flaherty 1989; Regan 1995) or cyber security (Etzioni 2011; Hiller and Russel 2013; Harknett and Stever 2011), but provide a limited and rather outdated empirical analysis. This study, however, considers both security and privacy as important elements of the whole, and traces them over the course of fifty years to reveal policy trends.

This paper challenges the common wisdom that emphasises the 9/11 terrorist attacks as the main significant cause for policy-makers to choose security over privacy in cyberspace. Indeed, the US Department of Justice (DOJ) issued guidelines in 2002 that indicate a strategy shift from mitigation to prevention of security threats. In addition to minimising damages, the department has devoted much of its focus to the prevention of threats altogether through massive information collection practices. But the 9/11 explanation does not completely fit with our findings, which

1 Any attempt to function in a modern society without employing digital practices is considered to be eccentric. Zuboff (2015) argues that 'It is impossible to imagine effective social participation - from employment, to education, to healthcare - without Internet access.' She asserts that this phenomenon has 'happened quickly and without our understanding or agreement.'

recognise a policy trend of increased government and private sector surveillance already in the mid-1990s. The 9/11 explanation also assumes that all federal authorities and market players act as a single actor with a unified post-9/11 strategy of increased surveillance. By separately analysing the actions of each federal authority and assessing the policy efforts of market players over time, this study enriches our understanding of surveillance drivers. Regarding private sector surveillance, the 9/11 explanation does not address the continuous deterioration of privacy by market actors. Thus, while the war on terrorism had catalysed surveillance, it was business interests, the increased power of the executive vis-à-vis Congress, and the institutional position of security agencies and information monopolies that contributed to the distinct policy shift from a compromise between security and privacy in the 1970s and 1980s to increased surveillance since the mid-1990s.

The article is organised in four sections. The next section clarifies the interplay between the concepts of privacy, security, surveillance, and resilience for the argumentation of the paper. Next, I present the analytical framework and methodology through which I test the promotion of security and privacy via cyberspace in the US federal arena. The third section discusses the findings through two sub-sections on each role of the state: (1) using cyberspace to ensure security through undermining privacy and cyber security; and (2) protecting cyberspace through cyber security and privacy measures. The shift towards greater security and less privacy is discussed through the role of each federal authority and business group in crafting this balance. The last section concludes by assessing the implications of understanding the dual role of the state in cyberspace and discussing the limitations of this research.

2. CONCEPTUAL CLARIFICATIONS

Privacy, security, surveillance, and resilience are four fundamental concepts for the analysis and arguments in this paper. These concepts can be used and understood in many ways, and the purpose of this section is to clarify their meanings in the paper.

First, I will discuss the concept of privacy. In contrast to its insufficient promotion in the public policy arena (Regan 1995), privacy as a concept has a rich history of definitions and understandings. Some stress the importance of an isolated location and space in order to enjoy the right to privacy. Other definitions tie privacy with control over personal information. A few scholars further argue that privacy is about the body and mind of the individual, rather than its location or personal information. Bygrave (2002) provides a promising framework to understand this blend of definitions. He divides the debate over the definition of privacy into four distinct groups. The first is scholars who take non-interference as their starting point and argue that individuals cannot be exposed to the public unless they choose (Warren and Brandeis 1890). The second group includes scholars who attach privacy to the levels of control over personal information (Westin 1967; Fried 1968; Rachels 1975; Laudon 1996; Lessig 1999). Scholars who focus on the degree of access to a person argue that privacy is about the body and mind and make up the third group. Gavison (1980) defines this amount of access across three dimensions – secrecy (personal information), solitude (physical access to a person), and anonymity (attention to a person). This broader notion of privacy considers mental health,

autonomy, growth, creativity, and the capacity to create meaningful relations as fundamental to the definition of privacy. With no privacy, this approach would argue, we are no longer the primary controllers of our self-presentation and do not decide on the term of our social interactions. Finally, the fourth group is made up of scholars who attach privacy to intimate or sensitive information. Julie Innes promotes this privacy approach by claiming that privacy 'is the state of possessing control over a realm of intimate decisions which include decisions about intimate access, information, and actions' (Innes 1992, p. 140). For the purpose of this paper, I choose to follow the second group of definitions and argue that privacy is about individuals' ability to control their personal information. At the same time, I acknowledge that privacy holds broader implications and I do not assert that the four groups of definitions are independent. Some may lead to others, as privacy is a dynamic concept that is determined by social relations over time. Nevertheless, for the simplicity of the argument, I would assert that violation of privacy is practically any illegal and non-transparent collection of personal information, even without a proof of harm to the individual.[2]

Second, I will clarify my understanding of the broad concept of security. In contrast to the conception of privacy, security has long been viewed as a dominant policy concept that guides public policies, public opinion, and the distribution of money and power (Rothschild 1995). Hobbes (1642) views security as one of the traditional roles of the sovereign. Waldron (2006) broadens the definition of security beyond physical safety. According to him, security provides certainty, freedom from fear, and the assurance for individuals that they will not be harmed. It creates an essential platform through which individuals can enjoy other values. Locke (1689) was maybe the first to notice and define the tension between security and liberty. The possession of basic liberty rights is insufficient without the security to exercise them, but if security seriously compromises liberty, one might wonder whether security retains its fundamental value.

Waldron (2006) takes this one step further and distinguishes between two types of security. *Individual security* is defined as the security of fundamental human rights (such as privacy) and is exercised by state institutions. Individuals acknowledge that in order to sustain social and state structures that keep them protected, they have to pay a tax. Such individual security is not only about physical security, but also addresses the security of cultural, social, and institutional attributes that allow individuals to live the way they choose. *Collective security* addresses the security of the nation, its institutions, and the distribution of security across populations. It introduces questions to individuals regarding constrains they are willing to carry for the sake of the 'security of everyone'. To ensure collective security, individuals might have to carry burdens that would not necessarily improve their own security status, but rather contribute to the individual security of others. Waldron's distinction between individual and collective security is useful, and will be used in this paper to assess the tension between security and privacy in cyberspace.

Third, I will address the concept of surveillance. Common perception ties surveillance to modernity and uses the concept to better capture the contemporary privacy problems in society (Lyon 2001; Regan 2011; Bennett 2011). Surveillance is not attached to data capturing in a private space, but rather refers to the systematic monitoring and analysis of individuals that exists on all level across institutions, social practices, and modern life. It became a useful

2 As opposed to Hughes (2015), who argues that a privacy claim turns into privacy right only when harm is unjust.

tool for government and the private sector to develop disciplinary power and new forms of governance. It is used instrumentally by the state and justified to increase collective, individual, or infrastructural security against terrorism or other break downs of public order (Regan 2011). The effects of surveillance on individuals do not just reduce privacy, they also alter opportunities and life style. The intensity of surveillance hampers freedoms, ethical principles, and even democracy itself (Raab, Jones, and Szekely 2015). The phrase 'privacy invasion' is too limited to encompass what has become a distinguishing and disquieting feature of modern life. Privacy was suited to a time when society was moving from paper records to large computerised databases, not a time of decentralised data capturing every movement on wireless devices (Regan 2011). For the purpose of this paper, I will use the term surveillance to describe a systematic violation of privacy by state institutions and private corporations.

Finally, I will discuss the term resilience. Raab, Jones, and Szekely (2015) tried to capture this concept through an extensive overview of policy documents that use 'resilience' as their end goal. They realise that this concept is identified with 'all kinds of natural or social phenomena where threats to the integrity and identity of physical objects, social goods, ethical values, or social relationships are introduced.' (Raab, Jones, and Szekely 2015, p. 23) They further find practical implications for resilience. They describe it as a coherent set of measures that include 'protecting, detecting, and responding to the consequences of threats, attacks, disasters, and other adverse events [...] that put vital interests such as national security, food supply, and community functioning at risk.' (p. 23) Strategy to achieve resilience usually relies on planned and coordinated efforts across organisations at various levels and among participants with separate roles and responsibilities. Politically, the term enjoys a certain political appeal, possibly because it suggests strength and robustness. Following these distinctions, Raab, Jones, and Szekely (2015) suggest an important conceptual boundary between the uses of the term 'resilience.' The term can be used as a property of community, individuals, or sphere, or as a set of activities undertaken to bounce back a threat. For the latter, resilience and surveillance complement each other. Governments conduct surveillance as part of a resilience strategy. For the purposes of this paper, however, I embrace the definition of resilience as a property that reflects the integrity and robustness of the digital sphere. I view resilience as a sustained and systematic process that includes capacity-building and institutional development that increases the stability and integrity of a sphere.

3. ANALYTICAL FRAMEWORK AND METHODOLOGY

The complex relations[3] between security and privacy are a subset of a broader theoretical scholarship over security and liberty in modern Western societies (Dworkin 1977; Waldron 2003; 2006; Zender 2003). The distinction between collective and individual security reveals some of the puzzle. While collective security is perceived as the 'platform' through which individuals can enjoy their liberties (Waldron, 2006), the intrusive means that political systems tend to adopt against collective security threats undermine liberty and paradoxically, some argue, lead to individual insecurity (Zender 2003; Waldron 2003; 2006). Thus, security and privacy are not logically independent and hold a social and collective importance for societies (Waldron 2003; 2006; Regan 1995, Hallsworth and Lea 2011).

3 Waldron (2003), Zender (2003) and others argue that security and privacy are much more parallel than we tend to think. Others, like Etzioni (2014), suggest a more utilitarian approach and assert that societies should consider scenarios in which security overrides the privacy of some for the security of others.

With the expansion of cyberspace and the increasing reliance of modern societies on robust and secure digital infrastructures, it became challenging to preserve the policy goals of security and privacy. Traditional threats have evolved and adapted themselves to the characteristics of the digital sphere. Cyber criminals, commercial hacking firms, and states' cyber-espionage arms have increased cyber insecurity and required response from the state. At the same time, governments and commercial organisations have been taking advantage of new technological capacities to monitor individuals and promote security, efficiency, and economic revenue at the expense of privacy. This study focuses on these often-conflicting goals. It traces the way the state promotes cyber security and privacy, but also increasingly collects or allows the collection of information at the expense of privacy and cyber security for greater national security, law enforcement, and market goals.

Surprisingly, the dual role of the state in promoting or impeding security and privacy in the digital age has not been fully explored in the literature. We are still puzzled by how security and privacy relationships are constructed by policy-makers. Deibert and Rohozinski (2010) highlight this discrepancy by differentiating between risks 'to the security cyberspace' (hacking, cyber crime etc.) and risks 'through cyberspace' that are generated by states through cyber technologies in order to promote other policy goals. This can be achieved through political depression and the violation of privacy to ensure the stability of regimes or address security threats on the state. They recognise the contradiction between increasing cyber security and using cyberspace for surveillance, but do not take us further to understand how this discrepancy is constructed and where it comes from in the policy-making process.

Mendez and Mendez (2009) shed more light on the policy process behind these conflicting goals. They consider government laws and regulations that either protect or threaten privacy, and argue that both policy fields have experienced increased federal concentration of power. Their explanation has two limbs. They emphasise the increasing threat to US commerce posed by strict EU privacy directives in the 1990s and view it as a federal incentive for changing the sectorial 'hands-free' privacy approach of the US government towards a more centralised federal approach in the form of a privacy monitoring agency (the Federal Trade Commission). They also argue that salient policy issues with 'a dangerous external threat', like the 'war on terror' post 9/11, led to even more centralised solutions by federal actors and paved the way for federal acts that violate privacy with very little scrutiny by Congress. Their findings raise an immediate puzzle; are these contradictory roles of the state advanced equally across federal powers? Since Mendez and Mendez (2009) base their conclusions on rather narrow empirical foundations,[4] we are still puzzled regarding the paradoxical role of the state in cyberspace. The authors' empirical analysis does not address the federal arena over time, and fails to consider cyber security policies as a tool for promoting privacy as well. While the federal arena lacked any privacy promotions during the 2000s, Congress and the Executive did pass significant privacy protections before that. These empirical shortcomings do not allow explanations other than 9/11 terrorist attacks for violations of privacy, and do not fully explore the role of business interests in this contradictory policy process. If the 9/11 terrorist attacks explain the expansion of US surveillance policies, why did we witness this expansion in the 1990s? If, according to Mendez and Mendez (2009), the likelihood of passing acts for federal privacy protections is high, why do we constantly see failed attempts to pass federal privacy legislation? The role of

4 They only focus on the rise of the Federal Trade Commission (FTC) as the U.S. privacy regulator in the 2000s in light of two significant laws that violate privacy in the same post 9/11 period.

businesses in government surveillance policies, and the failed attempts to pass federal privacy protections for the private sector, are not explored despite their significance in these policy processes.

Other scholars have addressed either privacy or security to study one aspect of the state's role, but did not analyse these attempts as part of the whole. Privacy policy scholars explain lack of privacy protections by either policy-makers' perceptions of privacy as an individual value that is subordinate to other collective values[5] (Regan 1995) or the lack of institutional capacities in the US to adequately promote privacy (Flaherty 1989). While these studies enrich our understanding on the policy processes that lead to insufficient privacy protections, they are rather outdated and focus on the 1970s and 1980s in the US federal arena. What these scholars viewed as insufficient privacy protections is nowadays viewed as the 'golden age' of privacy that was followed by significant privacy erosions by the US government and the private sector. A more recent study by Newman and Bach (2004) analyses the incentives behind the self-regulation model of privacy protections in the United States. Newman and Bach (2004) argue that latent threats and the potentially costly federal regulation dictate close collaborations within industries to avoid government regulation. While Newman and Bach (2004) shed light on why this 'hands-free' federal approach over privacy persists, we still lack an understanding of how and why this approach was decided on in the first place. This self-regulatory model is not contrasted with the emerging private sector surveillance that was created from this lack of privacy scrutiny by the government.

Finally, scholars of security in cyberspace shed even less light on the policy process and the contradictory role of the state. Etzioni (2011) explains the implications behind the reluctance of private actors to accept mandatory cyber security regulations, while Hiller and Russel (2013) vaguely explain the self-regulatory model of private sector cyber security through the 'regulatory culture' in the US that is traditionally skewed in favour of businesses. None of these scholars, however, address the dual role of the state empirically over time, or link security and privacy to provide explanations on the policy processes.

To explore the relations between security and privacy in cyberspace through the US federal arena, I have created an original data set with policy events[6] (N=85) from the years 1967 – 2016 that address:

(1) Government information collection for security purposes at the expense of privacy;
(2) Limitations to government information collection that increase privacy at the expense of security; and
(3) Cyber security and data protection measures that advance security and privacy at the same time.

The methodological approach of this study does not only include components of the traditional cyber security and data protection regulation, but also covers the promotion of national

5 Such as national security, law enforcement, or business efficiency.

6 Federal Legislation, Executive Orders, Presidential Orders and Directives, National Security Directives, Federal Register Rules from federal agencies, Policy Guidelines from federal agencies that provide additional interpretation to federal statues, Strategy documents from the White House and federal agencies that provide voluntary recommendations and best practices on the related issues, novel FISA Court rulings that further advance the understanding and practices over government surveillance, and novel Supreme and District Court rulings that provide new interpretation to the regulatory regimes of security and privacy.

security and law enforcement goals that dictate the extent to which the government can collect information in cyberspace. This allows for a broad understanding on the dynamics between security and privacy and the contradictory role of the state. The starting point of the policy events was chosen to be *Katz v the United States (389 U.S. 347)*, a Supreme Court landmark ruling from 1967 which overturned a decision from 1928 and provided constitutional privacy protections from government information collection.[7] This Supreme Court decision had triggered policy-making processes over security and privacy issues that shape the regulatory arena as we know it today.

Each gathered policy event was then classified to one of three policy categories according to the relationships it dictates between security and privacy. The events were conceptually mapped according to the following table:

TABLE I. THE CONCEPTUAL MAPPING OF POLICY EVENTS ACCORDING TO THE RELATIONSHIPS BETWEEN SECURITY AND PRIVACY IN EVERY EVENT

		PRIVACY	
		+	−
SECURITY	+	Security & Privacy complements (N=33): Cyber security and data protection practices that strengthen the security of personal information systems and advance the right to privacy of the associated data subjects	Security > Privacy (N=31): National Security or Law Enforcement policies that increase the collection of personal information and weaken digital infrastructures for security purposes
	−	Privacy > Security (N=21): Privacy practices that limit government information collection for security purposes and promote privacy at the expense of potential security risks that may arise from lack of collected information	

The *first* category includes policy-making events from 1984–2016 that strengthen security and privacy in cyberspace at the same time (N=33). These are mainly cyber security and data protection measures that strengthen the security of information systems as well as the privacy of individuals whose personal information is processed by those systems. These policies reflect one role of the state as strengthening the resilience of cyberspace. The *second* category includes policy-making events from 1976–2015 that open avenues for information collection by the government to advance national security and law enforcement at the expense of privacy (N=31). The *third* category includes policy-making events from 1967–2016 that deal with limitations to government surveillance, and thus strengthen privacy at the expense of security (N=21). These latter two categories reflect the extent to which the state uses cyberspace to increase security over privacy.

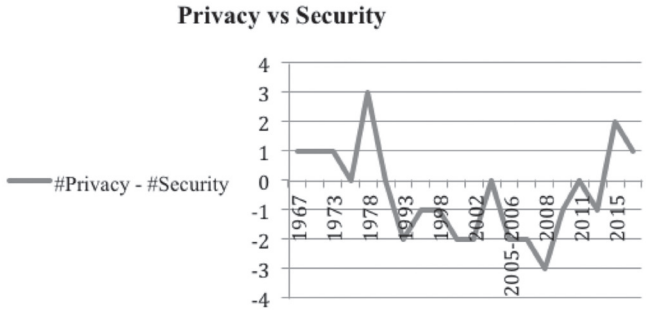
7 The court decided that using a telephone bug without a court order violates privacy according to the Fourth Amendment and determined that the right to privacy is entitled to people rather than places.

4. FINDINGS

A. Security ≠ Privacy: The State Uses Cyberspace to Advance Security Over Privacy

Figure 1 reflects the shift in the role of the state that uses cyberspace. Since the mid-1990s, the US federal arena has been crafting more laws and regulations to collect information from cyberspace, and thus, prioritise security over privacy. For each year, the figure reflects the yearly number of federal measures that *limit* government information collection minus the yearly amount of federal measures that *encourage* government information collection. While in the 1970s and 1980s the federal arena had more privacy than security measures (the blue line is above the horizontal axis), since the mid-1990s, the line is mostly under the horizontal axis, which quantitatively reflects a clear priority for national security and law enforcement measures over privacy measures in cyberspace.

FIGURE 1. ([PRIVACY MEASURES] – [SECURITY MEASURES]) PER YEAR OVER TIME [1967-2016]



In the last four decades, the government's information collection desires have been regulated through a variety of policy instruments and significantly affected the way security and privacy risks are managed in cyberspace. In the 1970s and 1980s, Congress was able to limit governmental desires for information collection. Up to the mid-1990s, Congress constructed a compromise between security and privacy, backed by public legitimacy, following political surveillance disclosures of anti-Vietnam war activists and the Watergate scandal (1974). The 1990s, however, brought the technological breakthrough of mass encryption and communication capabilities. Consequently, law enforcement agencies were worried that their surveillance capabilities would be undermined. This also changed the alliance of interests between businesses and civil society. In contrast to pro-privacy policies that were advanced by private businesses for the sake of their products, the 1990s brought close ties between government and telecoms businesses to increase surveillance. The 9/11 terrorist attacks and the official strategy of the administration, reflected in the 2001 Patriot Act, to collect anything 'tangible', was accompanied by the lack of significant pushback by Congress.

Figure 1 demonstrates a shift towards security at the expense of privacy in the use of cyberspace over time. This shift is evident throughout US federal authorities and relevant business groups. First, I will briefly summarise the actions of the executive. Since the 1990s, the executive branch had gradually eroded checks and balances over the use of government power to collect information from cyberspace. During the 1960s and 1970s, however, significant public outcries led to a rather weak executive. Congress was able to form investigative committees (the Church and Pike Committees of 1976) that eventually limited government surveillance and posed serious constraints on the ability of the executive in this area. Following demands from the American public, the executive itself initiated steps to limit surveillance through Executive Orders and Attorney General Guidelines (1976). However, since the mid-1990s, the legitimacy to exercise executive power has changed. With no major public scandals over surveillance and with the mind-set of the 'war on terror', there was almost complete federal silence over pro-privacy issues. This led to weak oversight mechanisms and lowered the standards and judicial safeguards for government information collection. This trend in the executive started in the 1981 Executive Order #12333, in which President Regan ordered the protection of privacy when collecting information, but only through self-regulation mechanisms rather than an external oversight. This trend significantly increased through several Attorney General Guidelines over the years (1983, 1989, and 2002) which broadened surveillance authority within the US with no negotiations or a complete policy process through Congress. In addition, from 2001–2007, President Bush solely relied on his own judgement to launch and then secretly continue to operate unlawful surveillance programmes, without notifying Congress. In 2001, President Bush launched these programmes on a 'temporary' basis to gain legitimacy for their use, and then extended them for seven years. Finally, the Administration had gradually expanded the authority of National Security Letters (NSLs) from the Department of Justice (DOJ). This policy instrument was originally launched as a national security exception to required data protection practices, but soon became one of the main avenues for information collection, taking the tool completely out of its original purpose.

Second, the role of Congress in the shift for greater security over privacy is quite striking. During the 1970s and 1980s, the legislature was highly active and pressured the administration to limit surveillance through its investigative committees and unprecedented legislation (Foreign Intelligence Surveillance Act (FISA) 1978 and Electronic Communications Privacy Act (ECPA) 1986[8]). However, since the mid-1990s, Congress has been unable to pass any significant legislation to limit information collection.[9] Privacy stakeholders in Congress became weak and were brought down by competing national security and law enforcement forces. Congress had shifted its role from pushing for a compromise between security and privacy, to backing the administration and supporting the collection of data at the expense of privacy. Since the mid-1990s, Congress allowed the passing of surveillance measures that were marketed as 'temporary' but soon became permanent. These include the Patriot Act 2001 provisions and the 2007 and 2008 amendments to FISA that significantly weaken privacy in favour of greater surveillance. Congress had also allowed the erosion of the legal barrier between surveillance for national security purposes and surveillance for law enforcement purposes. While national security surveillance was limited by previous laws, US intelligence agencies circumvented these limitations through collecting national security information in the name

8 Both these acts significantly limit the collection of personal information for national security (FISA) and law enforcement (ECPA) purposes.

9 The US Freedom Act that was passed in 2015 was the first legislation after 30 years that limits government bulk information collection.

of 'law enforcement purposes.' Congress approved the erosion of this 'wall' policy through the Patriot Act 2001, since it was related to one of the September 11 intelligence failures. Recently, however, following disclosures on government surveillance by Edward Snowden, Congress passed the US Freedom Act 2015 that has imposed some limitations on government surveillance after several decades.

The judiciary also had a role in the shift towards greater surveillance. Throughout the 1970s and 1980s, the courts had a significant role in promoting pro-privacy legislation to the federal policy-making agenda. This is evident through two examples: (1) the 1967 *Katz vs. United States (389 U.S. 347)* court ruling that was the basis of the Omnibus Crime Control Act 1968, which limited government information collection for the first time; and (2) the 1976 *United States vs. Miller (425 U.S. 435 1976)* case, which limited privacy rights when information was shared with third parties by individuals, was the basis for a counter-response by policy-makers in the form of the Electronic Communications Privacy Act (ECPA) 1986. At the same time, the influence of the courts on limiting government information collection since the 1990s was only expressed through amendments to restrict the use of NSLs by the FBI in the 2000s. Despite additional court rulings on the illegality of surveillance, the court was unable to influence the agenda and advance legislative measures to promote privacy over security. In fact, since the 1990s, decisions from the special Foreign Intelligence Surveillance Courts (FISC) for surveillance authorisation have contributed to the surveillance agenda of the government. These courts have secretly ruled on controversial issues without oversight from external judges. Moreover, FISC judges have also allowed controversial temporary surveillance authorisations to become permanent. Overall, the judiciary has been unable to limit surveillance in the past two decades, and in fact had a role in opening more avenues for government surveillance at the expense of privacy through FISA rulings.

Finally, the role of business groups from the telecom industry in fuelling the policy shift of security over privacy is also significant. Since privacy was viewed as an economic advantage during the 1970s and 1980s, business groups had strongly supported limiting government surveillance. An alliance over privacy between businesses and civil society was formed and successfully advanced pro-privacy legislation such as the Right to Financial Privacy Act 1978 and the Electronic Communication Privacy Act (ECPA) 1986. But in the mid-1990s, this alliance was broken after industry leaders paved the way for the Communication Assistance for Law Enforcement Act (CALEA) 1994 to pass. The government had provided a significant compensation for telecoms businesses to make their communications infrastructure 'surveillance friendly' for the government, and had weakened privacy at the expense of security. This trend of close ties between businesses and government continued throughout the 1990s and 2000s.

Most of this cooperation is hidden, but what we do know is that businesses cooperated with the government over controversial uses of National Security Letters (NSLs) to collect information. In addition, Internet Service Providers (ISPs) were allowed by law (Patriot Act 2001) to conduct surveillance based on their own judgement, while probable surveillance causes were lowered to suspicion only. Recently, however, since the Snowden disclosures, civil society and business interests have converged again. Examples include the refusal by Apple to break

iPhone encryption for national security purposes; the pushback of the industry that was able to postpone CALEA II legislative proposals by the FBI; and the opposition from Microsoft to turn in personal records of its clients from servers outside US jurisdiction. Privacy is gradually re-becoming a competitive economic advantage and a way to satisfy consumer demands.

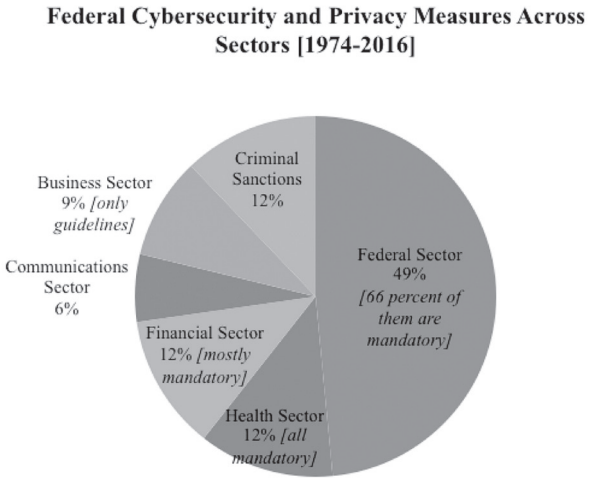
B. Security = Privacy: The State Increases the Security and Privacy of Cyberspace

At the same time, and in contrast to its efforts to undermine privacy and cyber security for national security and law enforcement purposes, the state has passed laws and regulations to increase the resilience of cyberspace. Three elements stand out from these policy efforts. First, these protection efforts are narrow in scope, mostly voluntary for the business and communications sectors, and thus do not seriously limit surveillance practices by the government or the private sector. Second, the government's agenda from the very early days of the Internet was to leave it unregulated. This had created the institutional conditions for the massive private sector surveillance for revenue we see today. Third, even within this policy category that mostly promotes security and privacy while increasing the resilience of cyberspace, we can see instances of tension over promoting cyber security through the collection of personal information and the violation of privacy.

1) Insufficient Privacy and Cyber Security Protections in the Private Sector

The advancement of security and privacy in cyberspace became a salient issue for federal policy-makers in the mid-1980s (Warner 2012). Nonetheless, despite the growth of the Internet's economy and the reliance on private networks, the promotion of security and privacy in the private sector is inefficient, sectorial, and only partially advances cyber security and privacy in cyberspace. The federal government is unable to extend its reach and regulate segments other than the federal, health and financial sectors. Most mandatory regulations pose strict requirements on critical sectors and the federal government, while non-critical private sectors are only addressed through declarative policy-making as their protection is mainly based on self-regulation models. Figure 2 demonstrates the lack of federal government efforts to increase the resilience of cyberspace for the business and communications sectors. Almost half of the regulatory effort is channelled to federal government networks, but while the federal government has to protect itself, it leaves other significant sectors to rely on voluntary practices (Newman and Bach 2004).

FIGURE 2. MANDATORY AND VOLUNTARY CYBER-SECURITY AND PRIVACY MEASURES ACROSS SECTORS [1974-2016]



Businesses were able to skip costly and mandatory regulations from the very beginning. The Privacy Act 1974 was enacted by Congress after long debates over the importance of protecting private information from federal authorities. Within these debates, private industry argued that there was little concrete evidence of abuses in the information practices of private businesses. They claimed that they were already overburdened by government regulation and the proposed regulation by the federal government was unnecessary and costly (Regan 1995, p. 78). Their strategy was to urge companies to enact voluntary protections for personal information in order to lessen the pressure for government regulation. The private sector also opposed establishing a federal agency to oversee information collection and use. A more rigorous Senate bill that included the creation of a privacy protection commission and suggested tighter restrictions on personal information was rejected in favour of a weaker House bill. In fact, the Privacy Act 1974 encompassed the minimum protection that was advocated at that time (Regan 1995).

In the mid-1990s, the federal government responded to the growth of the Internet by regulating the information security and privacy of specific private networks. Yet again, businesses were able to skip strict federal privacy regulations. In 1997, The Clinton Administration published *The Framework for Global Electronic Commerce (Clinton and Gore 1997)* which described businesses as essential to the new economy. The Administration did not want to limit businesses' expansion by posting costly and mandatory regulations over their operations. The framework also called for applying self-regulation models over privacy protections, leaving privacy decisions to the private sector. This practically mandated the private sector to set the standards of privacy protections by itself. This trend emerged in the beginning of the Internet age and

has not changed since. It allowed the business practice of the commodification of personal information to evolve, and led to extensive private sector surveillance for economic purposes by information monopolies like Google and Facebook.

Despite dozens of bills to regulate the private sector, Congress ended up passing legislation solely on the health and financial sectors. Health records were recognised as sensitive and critical in the digital age and the Health Insurance Portability and Accountability Act (HIPAA) 1996 was the first time that information security standards were codified. After long debates and the expressed concerns of private players over the cost and complexity of the regulation, the act became a binding federal register rule in 2003. The policy-makers then turned to the financial sector. Through the Gramm-Leach-Bliley Act (GLBA) 1999, federal policy-makers sought to ensure the security and privacy of information in the financial sector. The financial sector enjoyed an additional indirect boost through the Sarbanes-Oxley Act (SOX) 2002 that was introduced following the collapse of Enron and WorldCom in order to restore public trust in US corporations. The legislation changed the way publicly traded companies manage their audit, financial reporting, and internal controls. While information security is not specifically discussed in the Act, reviews of companies' controls include information security controls that have to follow the same strict restrictions.

In 2010, after a decade of federal laws and regulations that mainly dealt with the protection of federal networks and critical infrastructures, the regulatory agenda was shifted toward regulating the private sector. But instead of changing the 40-year trend towards mandatory and strict requirements, the Department of Commerce continued the trend of posing no mandatory security and privacy requirements on the private sector. The Department published two strategy documents to address the privacy and security problems of 'non-critical' sectors. The first[10] goes a long way by suggesting a baseline for consumers' privacy and security protections in the business sector. Specifically, the strategy recommends businesses to adopt the Federal Information Processing Standard (FIPS) – a privacy standard that was enacted in 1974 by the Privacy Act – and suggests that the federal government pass federal breach notification rules.[11] The strategy also calls for the establishment of a privacy oversight office under the Department of Commerce. A similar policy suggestion on the oversight of the privacy of federal networks through a dedicated office was made in the 1970s, but had been unable to get on the agenda since. The second strategy document[12] calls for collaboration between the public and private sector and the promotion of trust and multi-stakeholder processes in order to develop security best practices and make them industry standards. The suggested framework is voluntary, and the aim of the strategy was to find the proper security protection for each 'sector and sub-sector in the economy.' (Cybersecurity, Innovation, and the Internet Economy p. 2) It defines a new sector – the Internet and Information Innovation Sector (I3S) – and provides recommendations

10 The referred policy document is the *Commercial Data Privacy and Innovation in the Internet Economy: A dynamic policy framework*. The document argues that 'many key actors, due to the sectorial privacy and cyber-security approach of the U.S., operate without specific statutory obligations to protect personal data.' (p. 12).

11 These are rules that require companies to report and face financial consequences in case of a data breach. Currently, the U.S. has 47 versions of breach notification laws across its states and was unable to pass a unified federal legislation despite many attempts in the last 15 years. There is controversy over issues like – federal preemption, desired policy goals, scope of notification, and effectiveness of policy.

12 The referred policy document is the *Cybersecurity, Innovation, and the Internet Economy* by the Department of Commerce Internet Policy Task Force.

on technical security standards and incentives[13] to deal with cyber security threats that are integrated in the culture of each firm. Despite these important efforts, the cyber security and privacy of businesses remained almost completely a product of self-interest and judgement, bound only to what is considered 'fair trade practices' that could be enforced by the FTC.

Since 2013, however, we have seen a few significant steps at the federal level to ensure private sector security and privacy. The health and financial sectors are now required to adopt further protections through guidelines from federal agencies, while the Federal Communications Commission (FCC) is also increasing its role as a privacy and security regulator in cyberspace. The agency published a strategy document[14] with voluntary recommendations to communication providers on how to mitigate cyber security risks and comply with the National Institute for Standards and Technology (NIST) network security framework. Additionally, the 3rd U.S. Circuit Court of Appeals in Philadelphia had recently taken a stand on the authority of the Federal Trade Commission (FTC) to enforce cyber security protections in the private sector *(FTC vs. Wyndham Worldwide Corporation 2015)*. This was a significant ruling. Previously, the FTC had relied on the reasonableness of companies' security practices and enforced regulation based on unfair business practices. This enforcement power was authorised to the FTC by section 5 of the FTC Act 1914. Following this ruling, the FTC has a new mandate and institutional power to enforce cyber security and privacy protections. This trend continued in 2016, with the FCC moving from recommendations to actions. It published a new rule that requires Internet Service Providers (ISPs) to protect their consumers against information collection practices and require full transparency in personal information processing. However, with the recent change in the Administration and the appointment of a new FCC Chair by President Trump, these mandatory privacy guidelines have already been partially reversed.[15]

These inadequate privacy protections have paved the way for the lack of barriers for government surveillance, but more importantly, laid the foundations for the commodification of personal information and the massive surveillance practices we see today in the private sector. In its role to promote cyber security and privacy, the state does not only lack the ability to protect the private sector, but has also created the conditions that have allowed private sector surveillance to emerge and thrive.

2) Contradictions between Cyber Security and Privacy in the State's Efforts

Beyond the lack of sufficient mandatory protections for the private sector, the federal government also risks privacy to increase the security of cyberspace. Even though increasing the levels of cyber security would also increase the protection of privacy, many state initiatives include massive information collection practices. This tension between cyber security and privacy reflects a shift towards less privacy protections in cyber security measures from 2001 onward.

Concerns over the means and the potential violations of privacy to ensure information security were already evident in 1984. Through a National Security Directive in 1984, President Reagan authorised the National Security Agency (NSA) to protect all classified government

13 Such incentives can be achieved through national breach notification law, information sharing and liability protections, and insurance mechanisms.

14 The referred strategy document is the *Cybersecurity Risk Management and Best Practices Working Group 4: Final Report March 2015*, FCC.

15 The new FCC chairman, Ajit Pai, blocked FCC requirements from ISPs to apply common sense security practices to protect personal information. See more here: https://www.eff.org/deeplinks/2017/02/new-fcc-chairman-begins-attacks-internet-privacy.

networks. This decision increased surveillance concerns of US policy-makers and in 1987, Congress responded and enacted the Computer Security Act. The purpose of the Act was to assign responsibilities for the protection of federal networks and appoint the civilian National Institute for Standards and Technology (NIST) rather than the intelligence National Security Agency (NSA) as the sole body responsible for protecting federal networks. However, NIST was never powerful enough institutionally and was bound to certain arrangements with the NSA that questioned its influence over the entire process (Flaherty 1989). In 2001, an unexpected contributor to the promotion of cyber security and privacy was the passage of the Patriot Act. While the Act significantly weakens privacy protections for information collection that serves national security interests, it also increases defensive capabilities against cybercrime. The act creates, for the first time, the definition of a 'computer trespasser'. It also allows law enforcement officials to trace the communications of computer trespassers and improves their ability to track cybercrime activities. Section 220 allows a single court order with jurisdiction over the cybercrime offence to issue a search warrant for electronic evidence anywhere in the country. These increased cybercrime capabilities threaten privacy. The types of collected data on computer trespassers is broad; section 210 expands the information that can be obtained from communications providers to include means and sources of payments as well as session times and temporarily assigned network addresses, while section 216 applies tracking devices of meta-data (e.g. pen registers and trap-and-trace devices) to any communication facility in the country.

Tension between the right to privacy and promoting cyber security was also expressed in the 2008 *Comprehensive National Cyber Security Initiative (CNCI)*. The White House published this strategy in order to ensure that federal networks are resilient to the dynamic nature of cyber-attacks. The initiative encourages the use of intelligence and advances information collection of foreign intelligence. It also encourages the use of decryption capabilities by the NSA that risk privacy. Another instance of tension between cyber security and privacy is the recent passage of the Cyber Information Sharing Act (CISA) 2015. This allows non-transparent information collection from the private sector on cyber threats for the sake of greater cyber security. It signals a new phase in the tension between privacy and cyber security as it removes liability from businesses that choose to share information, and thus encourages information collection by the government without a court order. To conclude these trends, even in its role as protecting cyberspace, the US has undermined privacy in cyber security at an increasing rate since 2001.

5. CONCLUSION

Over the course of fifty years, the US federal government has held a contradictory role with regards to the promotion of security and privacy in cyberspace. In the past twenty years, the power of the executive branch vis-à-vis Congress and the close cooperation between businesses and security agencies have increased surveillance and weakened the privacy and cyber security of cyberspace. At the same time, the reluctance of businesses to accept mandatory regulations and the power of the executive and security agencies to advance cyber security at the expense of privacy have led to lax cyber security and privacy protections. This has encouraged the

trend of deteriorating privacy and created the institutional conditions for massive private sector surveillance by powerful information monopolies that undermine privacy for economic revenue.

While the US excels in undermining privacy and cyber security to achieve 'greater' security goals, it is less successful in strengthening the resilience of cyberspace as a common good. After thirty years of policy experience with regards to cyberspace, this paper illustrates the urgency of changing the policy discourse on cyber security. In order to advance cyberspace as a common good, the current policy framing that places cyber security as a property of systems rather than people has to change.

Traditional definitions of cyber security usually involve the protection of digital systems against hackers, and the dominant actors in this policy domain are security agencies and private interests. This creates a discourse over cyber security according to which 'surveillance powers are expanded, encryption is limited, backdoors are installed, and accountability structured are weakened' (Puddephatt and Kaspar 2015 p. 3). This dramatically opposes individual security and questions the move towards greater reliance on digital practices that weakens the fabric of society.

As demonstrated empirically in this paper, the overarching policy trends over security and privacy in cyberspace are a source of concern. The policy discourse over those issues should emphasise the security rights of end users rather than just the security of systems or the promotion of national interests. This might mean giving ownership back to data subjects, guarantee end-to-end encryption and public education over privacy, and include stronger accountability and oversight mechanisms for necessary data collection by ensuring that the scope of such powers is narrowly defined. Voices other than those of the security agencies should be involved in the policy debate to ensure that individual and collective cyber security are jointly advanced.

Finally, it is worth mentioning the limitations of my research conclusions. There is a tension in this paper between the amount of the data (85 policy events) and the explanatory power of my arguments that relies on general trends in regulation over time. The next logical step would be to focus on three or four cases that provide a representative sample of the data and analyse them comparatively to reveal the mechanisms of business influence and executive power over the way the US government manages risks in cyberspace.

REFERENCES

Bennett, C.J., 'In Defense of Privacy: The Concept and the Regime', *Surveillance & Society*, 2011, Vol. 8, No. 4.

Bygrave, L.A., *Data Protection Law – Approaching its Rationale, Logic, and Limits*, 2002, Kluwer Law Intl.

Clinton, W.J., and Gore, A., *A Framework for Global Electronic Commerce*, 1997, Washington, DC.

Deibert, R.J., and Rohozinski, R., 'Risking Security: Policies and Paradoxes of Cyberspace Security', *International Political Sociology*, 2010, Vol. 4, Issue 1, 15-32.

Doyle, C., 'The USA Patriot Act: A Legal Analysis', *Congressional Research Services (CRS) Report for Congress*, 2002.

Dworkin, R., *Taking Rights Seriously*, 1977, Harvard University Press.

Etzioni, A., 'Cybersecurity in the Private Sector', *Issues in Science and Technology*, 2011, Vol 28, Issue 1.

Etzioni, A., 'A Cyber Age Privacy Doctrine: A Liberal Communitarian Approach', *Journal of Law and Policy For the Information Society*, 2014, Vol 10, Issue 2.

Federal Trade Commission, 'Protecting Consumer Privacy in an Era of Rapid Change', *Preliminary FTC Staff Report*, 2010.

Flaherty, D.A., *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States*, 1989, UNC Press.

Fried, C., 'Privacy', *Yale Law Journal*, 1968, Vol. 77, 475-93.

Gavison, R., 'Privacy and the Limits of Law', *Yale Law Journal*, 1980, 89: 442.

Hallsworth, S. and Lea, J., 'Reconstructing Leviathan: Emerging contours of the security state', *Theoretical Criminology*, 2011, 15(2), 141-157.

Harknett, R.J., and Stever, J.A., 'The New Policy World of Cybersecurity', *Public Administration Review*, 2011, 455-460.

Hiller, J.S., and Russel, R.S., 'The challenge and imperative of private sector cybersecurity: An international comparison', *Computer Law & Security Review*, 2013, Vol. 29, 236-245.

Hobbes, T., *De Cive*, 1642.

Hughes, D.R.L., 'Two Concepts of Privacy', *Computer Law & Security Review*, 2015, Vol. 31, 527-537.

Innes, J., *Privacy, Intimacy, and Isolation*, 1992, New York: Oxford University Press.

Laudon, K.C., 'Markets and Privacy', Association for Computing Machinery, 1996, *Communications of the ACM*, Vol 39, Issue 9.

Lessig, L., *Code and Other Laws of Cyberspace*, 1999, Basic Books.

Locke, J., *Two Treatises of Government*, 1689, London.

Lyon, D., *Surveillance Society: Monitoring Everyday Life*, 2001, Open University Press.

Mendez, F., and Mendez, M., 'Comparing Privacy Regimes: Federal Theory and the Politics of Privacy Regulation in the European Union and the United States', *The Journal of Federalism*, 2009, Vol. 40, Issue 4, 617-645.

Newman, A.L., and Bach, D., 'Self-Regulatory Trajectories in the Shadow of Public Power: Resolving Digital Dilemmas in Europe and the United States', *Governance*, 2004, Vol 17, No. 3, 387-413.

Puddephatt, A., and Kaspar, L., 'Cybersecurity is the new battleground for human rights', *OpenDemocracy.net*, 2015, access: https://www.opendemocracy.net/wfd/andrew-puddephatt-lea-kaspar/cybersecurity-is-new-battleground-for-human-rights.

Raab, C., Jones, R., and Szekely, I., 'Surveillance and Resilience in Theory and Practice', *Media and Communication*, 2015, Vol. 3, Issue 2, 21-41.

Rachels, J., 'Why Privacy is Important', *Philosophy & Public Affairs*, 1975, Vol. 4 No. 4, 323-333.

Regan, P., Legislating Privacy: *Technology, Social Values, and Public Policy*, 1995, UNC Press.

Regan, P., 'Response to Bennett: Also in defense of privacy', *Surveillance & Society*, 2011, Vol. 8, No. 4.

Rothschild, E., 'What is Security?' *Daedalus*, 1995, Vol. 24, No. 3, 53-98, MIT Press.

Waldron, J., 'Security and Liberty: The Image of Balance', *Journal of Political Philosophy*, 2003, 11 (2): 191-210.

Waldron, J., 'Safety and Security', *Nebraska Law Review*, 2006, 85: 454-507.

Warner, M., 'Cyber Security: A Pre-history', *Intelligence and National Security*, 2012, Vol 27, Issue 5, 781-799.

Warren, S.D., and Brandeis, L.D., 'The Right to Privacy', *Harvard Law Review*, 1890, 4: 193-220.

Westin, A., *Privacy and Freedom*, 1967, New York: Atheneum.

The White House, 'National Strategy for Trusted Identities in Cyberspace', *White House Strategy*, April 2011.

Zender, L., 'Too Much Security?', *The Journal of Sociology of Law*, 2003, Vol. 31, Issue 3, 155-184.

Zuboff, S., 'Big Other: Surveillance Capitalism and the Prospects of an Information Civilisation', *Journal for Information Technology*, 2015, Vol 30, 75-89.