The State as a Double Agent: National Security Versus Privacy and the State's Role in Cyberspace in the United States

Ido Sivan-Sevilla

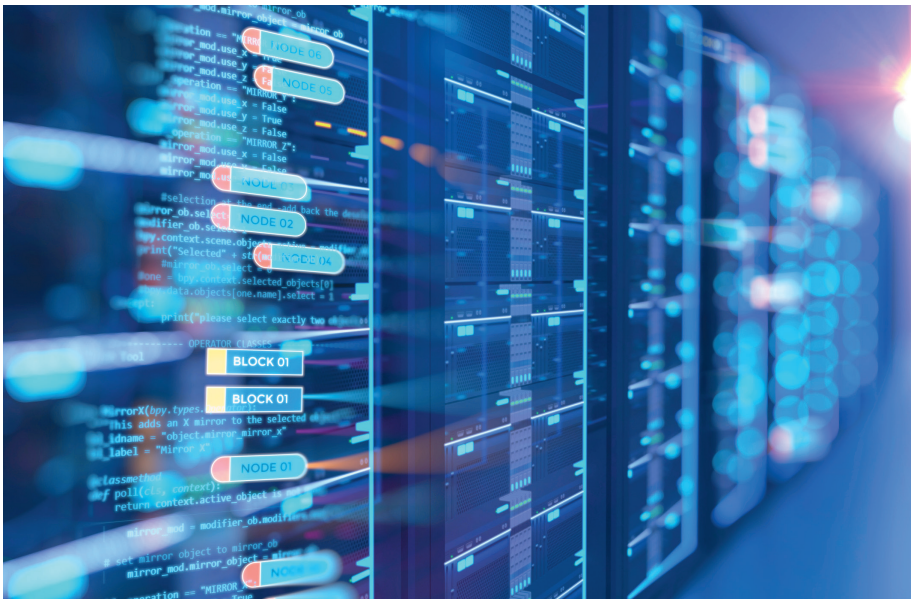
How does legislation and regulation in the United States structure the relationship between national security and privacy in the digital era? To answer this question, a database was created, consisting of all relevant federal laws and regulations (86 in all) issued between 1967 and 2016. Each one was classified by the degree to which it represented a contradiction or congruence between national security and privacy. The findings reveal changes favoring national security over privacy in three different timespans before and after the digital era and indicate significant gaps in promoting national security and privacy in the civilian business sector. These findings may be due to three factors: 1) the changing role of business in promoting national security and privacy in cyberspace, including the lack of overlapping interests between the business sector and civil society; 2) asymmetrical power relations favoring the executive branch of government over that of Congress; and 3) the decisive effect of security agencies and technology monopolies hindering the advancement of cyberspace policies that would strengthen both national security and privacy. This article empirically tracks the dual and paradoxical role of the state in cyber issues; on the one hand, the state goes to great lengths to promote cybersecurity, safeguard privacy, and protect national security. On the other hand, the state exploits cyberspace to gather information while it violates privacy in order to attain "higher" national security goals.

Keywords: National security, privacy, cybersecurity, regulation, risk management

Introduction

This article focuses on the way the federal government in the United States structures the relationship between national security and privacy in the digital era. On the one hand, technology allows a country to undertake mass surveillance and deepen the conflict between national security and privacy. On the other hand, technology provides an infrastructure through which it is possible simultaneously to promote national security and privacy by strengthening the cybersecurity of federal government systems and sensitive systems in the financial and healthcare sectors, which contain massive amount of private, personal information. This article finds that national security and privacy both clash and complement one another, thus making it possible to expose the state's dual role, which, in the digital era, promotes and violates privacy at the same time. A review of the literature indicates that state efforts to promote privacy protection in cyberspace and the measure of control over the executive's power in the digital era have yet to be studied in-depth and empirically. This research strives to fill some of this lacuna and examines when there is congruence or contradiction between the two objectives over time. The purpose of this article is to clarify how two complementary yet contradictory objectives relate to one another over time in public policy processes within a democratic nation.

Methodologically, the article tracks federal legislation, executive orders, state agency instructions, state strategies, and important court decisions in the US federal arena between 1967 and 2016 (86 manifestations in all), classified by the degree to which each one represents a contradiction or congruence between national security and privacy. The article then explains the definitions of national security used herein and the methodology for measuring congruence and contradiction. It should be clarified that the article examines both state efforts in promoting cybersecurity and privacy as important factors in advancing national security as well as information gathering at the expense of privacy ostensibly carried out in order to increase national security. The findings indicate that since the 1990s, policy changes have placed greater emphasis on national security than on privacy. These changes in policy have been observed in each branch of the federal government. In the 1990s, the executive branch, which was significantly restricted by Congress in the 1970s, began allowing state surveillance to the detriment of privacy thanks to controversial court decisions in camera and by means of



iStock

intervening in the architecture of technological products to allow constant state surveillance while the checks and balances were ineffective.[1] The executive branch changed its role from being a balancing party trying to mediate between national security and privacy in the 1970s and 1980s to one that passes laws encouraging the state to gather data without adequate enforcement in the business sector, which also relies on the same gathering of data. The judiciary, whose rulings in the 1970s and 1980s led to important laws strengthening privacy, has not had any fundamental impact since then.

The literature on policy and regulations related to cybersecurity and security in general and information gathering designed for national security in particular is surprisingly sparse and does not track decision making on the subject. Some researchers refer to the state's contradictory role, although their explanations of the factors affecting this trend in policy are limited.[2] Other researchers deal with only one state function, either in the field of cybersecurity[3] or cybersecurity and national security,[4] and provide limited explanations covering a short time frame of decision making on the issue. By contrast, the present research considers national security and privacy as important parts of the whole and tracks policy processes that shape the contradiction and congruence over a period of five decades. Furthermore, it contributes to an understanding of the role of the state in the digital era

and provides an analytical framework through which one may understand the wealth of regulations and laws structuring the relationship between national security and privacy in society. Despite the repeated claims of the retreat of the state in the neoliberal era, we can see, in fact, significant state intervention in the shaping and regulating of this important relationship.

The findings presented herein challenge the assumption that the 9/11 terrorist attack was the major reason why national security was given priority over privacy in the United States. Even though the US Department of Justice announced a change in its policy strategy after the attacks—from the minimizing of criminal damage to overall prevention through systematic surveillance and information gathering[5]—the trend to prioritize national security over privacy had already emerged in the 1990s. While the war on terrorism certainly supported this trend, other factors, such as business interests, power struggles between the executive and legislative branches of government, and the rising influence of intelligence agencies and the technology monopolies on the privacy of citizens from the mid-1990s, affected this imbalance.

This article is divided into four parts. The first offers a conceptual framework for understanding the relationship between privacy and national security by conceptualizing privacy, security, and surveillance. The second part surveys the theoretical literature about the state as a risk manager that structures the relationship between national security and privacy, including a discussion of the methodology for measuring this relationship over time. The third part presents the findings themselves and discusses the state's dual roles in using cyberspace for promoting national security at the expense of privacy and for defending cyberspace, thus promoting both privacy protection and national security at the same time. The fourth part discusses the findings and gives recommendations for the future.

Defining Basic Concepts

Security, privacy, and surveillance are fundamental concepts for structuring the article's analysis and discussion. As these terms may be understood in different ways, this section aims to clarify the definitions used. Let us begin with the term "privacy." In stark contrast to the insufficient way in which privacy is promoted in US public policy[6] —that is, in a sectorial manner, using models of self-regulation with only partial enforcement—privacy as a

right appears in the Fourth Amendment of the US constitution and much has been written about it. Some conceptualize privacy through the importance of the physical location that allows it to be obtained; that is, privacy is a function of location. According to this definition, people are entitled to absolute privacy in their homes. Others view privacy as the measure of control people have over their own private, personal information. Some feel that privacy is a matter of freedom over one's body and thoughts rather than an individual's location or private data. Bygrave tried to make sense of these different definitions of privacy by putting them in four major groups. The first group focuses on non-intervention, determining that privacy is the ability to respect the desire of an individual not to be exposed (the first to state this were Warren and Brandeis in 1890).[7] The second group define privacy by addressing how much control the subjects of the information have over their own data.[8] The third group conceptualizes privacy by the way of access to an individual, claiming that privacy has to do with bodily intimacy and freedom of thought. Gavison defines these ways of access using three parameters: the confidentiality of personal information, the level of isolation matching the individual's desire, and anonymity.[9] This group broadly conceptualizes the term so that it also extends to mental health, autonomy, growth, creativity, and individuals' ability to create meaningful relationships. Based on this definition, individuals cannot, in the absence of privacy, control their ability of self-presentation or the ways they manage social relationships. The fourth group conceptualizes privacy through intimate information. Innes claims that privacy is the ability to control intimate decision making at the individual level.[10] This article focuses on the second group, which conceptualizes privacy through control of private information. Nonetheless, as a concept, privacy has a much broader framework when the above definitions are not independent of one another. For the sake of simplification, it will later be claimed that the violation of privacy is the illegal or non-transparent gathering of personal data and does not require proof of damage by the subject of the information collected.

"Security" is no less elusive or broad. Unlike privacy, security is traditionally understood as the goal of the dominant policy around which the domains of public policy, public opinion, power relations, and public budgets are shaped.[11] The political philosopher Thomas Hobbes viewed security as the sovereign's uppermost objective. Waldron expands the definition to include

more than just physical safety. He claims that security allows certainty, freedom from fears, and mental peace and quiet for individuals. According to Waldron, security is the infrastructure through which individuals may enjoy other rights.[12] The political philosopher John Locke may have been the first to define the tension between security and liberty. Ensuring liberties, he wrote, is insufficient unless there is a sense of security that makes it possible to enjoy them. But if security itself violates liberty, the rationale for its promotion in the first place is undermined. Waldron goes on to distinguish between two types of security. The first is security at the individual level, which he defines as human rights generally attained by state intervention. In this case, in order to ensure state and social structures that safeguard their security, individuals understand that they must pay some sort of tax. This type of security goes beyond physical safety to include both cultural and social security and the individual's ability to lead his life as he wishes. The second type of security is at the group level and refers to the security provided by the state, its institutions, and the distribution of security among the population. This type of security raises questions about the constraints an individual is willing to accept for the purpose of collective security. Individuals may be forced to pay a price that does not necessarily improve their personal security but rather enhances the security of others in the population. This article adopts the definition of security at the group level, as this distinction between personal and collective security is useful and will reappear in the conclusion.

Having covered privacy and security, we now turn to surveillance, which, in practice, is one of the routine methods for increasing national security at the expense of privacy. The widespread approach links surveillance to modernity and uses the concept to explain the problems of privacy in the digital era.[13] Surveillance is not necessarily connected to personal information in the private sphere but rather to systematic information gathering and analysis of individuals' behavior in order to predict their future actions. In the technological era, surveillance has become a tool for states and private players to discipline citizens and create new forms of governance. Justifications for surveillance include personal and collective safety and security in the face of terrorism and public disorder. Surveillance of citizens affects not only their privacy but also their opportunities and the lifestyle they choose. When it comes to surveillance, privacy suddenly seems to become a limited

concept that does not properly describe the systematic information gathering that occurs now. The concept of privacy was more suitable to the era when society shifted from paper to computerized databases but irrelevant to an era in which systems are amassing data about all of our daily activities. The concept of surveillance in this article reflects the systematic violation of privacy by state institutions and private companies without the consent of those subjected to surveillance.

Literature Review and Methodology

The complex relationship between security and privacy is a function of the broader theoretical literature on security and liberty in the West.[14] The distinction between personal and collective security reveals only some of the complexity. While collective security is the infrastructure through which individuals may enjoy liberty, state systems are aggressive in dealing with threats to collective security, which is the antithesis of liberty and also contradicts security. Therefore, security and privacy are not independent of one another, and both are of social and collective value to society.[15] With the expansion of cyberspace and modern society's dependence on the digital sphere, the challenge of preserving and safeguarding privacy has only intensified. In terms of physical safety, the traditional threats simply have adapted themselves to the new environment. Cybercrime, commercial hacking companies, and state espionage have all contributed to insecurity in the new sphere. At the same time, governments and commercial companies exploit technological abilities to gather information and surveil, as well as promote security, efficiency, and commercial interests at the expense of privacy. This article tracks these clashing and complementary objectives and tries to understand the dual role of the state as an entity that promotes both national security and privacy through cybersecurity and cyber data while also gathering information for the purpose of national security at the expense of privacy.

The state's dual role as society's risk manager in the field of public policy during the digital era surprisingly has barely been studied. These two objectives of the state have not been properly conceptualized nor are the decision-making processes understood. Deibert and Rohozinski refer to this contradiction and distinguish between risks to "security cyberspace," which are handled by standards and protection of data integrity and reliability, and risks related

to "use of cyberspace" for promoting other aims. They describe how states tend to commit political oppression and violate privacy and data security of individuals in order to ensure stability and the preservation of the existing social order and point out an important distinction about the contradiction in the different roles of the state in the digital era.[16] Nonetheless, this distinction does not help us understand the source of the contradiction in policy processes and regularization of these issues. Mendez and Mendez provide more concrete explanations about policy processes behind the conflict in the state's role.[17] They consider laws and regulations that simultaneously promote and threaten privacy, claiming that both roles manifest the concentration of state power. In their explanations, they emphasize the commercial threat to the United States posed by European privacy laws, seeing it as the incentive for changing the permissive privacy policy in favor of restraint and enforcement in the form of the Federal Trade Commission. They then try to explain privacy violations in the name of national security by referring to new threats, such as the war on terrorism, which led to solutions that violate privacy without any congressional oversight. While the focus on the contradiction inherent in the state's role is important, their work relies on a limited empirical study. They do not refer to changes in the federal arena over time and they do not examine cyberspace policy as one that promotes both privacy and national security. This narrow perspective prevents the authors from considering factors other than the 9/11 terrorist attacks that led to violations of privacy, and they fail to deal with the role of commercial interests in the digital sphere. If the terrorist attacks in 2001 were, in fact, the primary factor in disrupting the balance between national security and privacy, why do we observe the dominance of national security over privacy already in the mid-1990s? What was the role of the various federal authorities in instituting policy on the issue?

In addition to these studies that focus on the dual roles of the state as safeguarding privacy and national security on the one hand and gathering information to protect national security on the other, a lot of research focuses only on one aspect of the state's role in the digital era and not on a more comprehensive relationship. Those who study privacy and data protection explain the lack of privacy by claiming that decision makers understand privacy as an individual value rather than a public one or as a result of the institutional inability to promote privacy at the federal level.[18] Although

these studies have contributed to our understanding of policy processes, they are now dated, as they focus only on the 1970s and 1980s. What these researchers viewed as insufficient data protection is understood now as being the golden era of privacy protection in the United States, as it was followed by serious privacy violations by both the state and the commercial sector. A later study, by Newman and Bach, analyzes the incentives for establishing self-regulation of data protection in the United States.[19] They claim that the lack of significant threats and the high cost of regulation led to frequent partnerships in industry in order to avoid state regulation. While Newman and Bach shed light on US market access, it is not clear why the approach was adopted in the first place. The researchers do not address the serious ramifications that the self-regulatory model by commercial companies had on privacy, which led to the commercialization of personal information that we are witnessing today.

Finally, researchers dealing with cybersecurity as a means of promoting privacy do not advance our understanding of the related policy processes. Etzioni explains the ramifications stemming from the private players' unwillingness to assume regulatory commitments.[20] Hiller and Russell provide a vague explanation for the self-regulation model by referring to the US regulatory culture, which traditionally tends to favor businesses.[21] By contrast, Bamberger and Mulligan's important study, which tries to study what lies behind the regulatory directive, discovers that, in practice, the regulatory flexibility and the vacuum even in information protection has led to a fascinating discourse and the protection of data by Data Protection Officers that goes beyond state requirements.[22] Still, the subject of that study is the state and the research approach advocated is the attempt to understand how a state, as an entity unto itself, structures the relationship between national security and privacy. While some companies may take advantage of regulatory flexibility to impose more stringent directives, others exploit this flexibility to invest the bare minimum in their customers' information protection and privacy. Therefore, examining the state directives and regulations is the basis for understanding the state's role in cyberspace.

A review of the literature shows the lack of studies about the state's dual function in the digital era over time. Absent is any reference to national security and privacy as two pieces comprising the whole, contradicting and complementing one another at the same time. Therefore, in order to

track the relationship between national security and privacy at the federal level in the United States, this article is based on original data containing 86 policy manifestations, defined as the sum total of all relevant legislation and regulation documents from 1967 to 2016, including primary legislation, secondary legislation, executive orders, important court decisions, decisions by the National Security Council, and strategy documents. Each policy manifestation refers to data gathering by the state for the intent of national security at the expense of privacy; limitations on the way states can gather information because of privacy protection; and possible ways to promote information and cybersecurity, which would advance both national security and privacy in the digital era. Therefore, the article's methodological approach is broad and includes issues of national security, law enforcement, and cybersecurity, which together comprise the way the state structures the relationship between national security and privacy in the digital era. This approach allows a wide understanding of the dynamics between national security and privacy and the state's dual role. The starting point selected for examining the relevant events is the Supreme Court ruling of 1967 (Katz v. the United States), which, for the first time, granted constitutional protection to the right to privacy.[23] The decision created a chain reaction leading to the establishment of policy on national security and privacy that has shaped the regulatory landscape as we know it today.

Every policy manifestation in the database was classified according to three different categories reflecting the relationship between national security and privacy, as shown in table 1 below. The first category consists of 33 policy manifestations between 1984 and 2016 that simultaneously strengthened national security and privacy in the digital era through cybersecurity and information protection. These are primarily laws and regulations promoting cyberspace and information protection in government, healthcare, and financial systems. The second category consists of 31 policy manifestations between 1976 and 2015 that expanded the state's ability to gather information for the purpose of national security at the expense of privacy. These are primarily directives and laws helping security and intelligence agencies exploit cyberspace for other security needs. The third category consists of 21 policy manifestations between 1967 and 2016 that limited the state, representing a compromise between national security and privacy. More precisely, they mainly are policies from the 1970s and 1980s that limited the

Table 1: Classification of policy events according to the conceptual relationship between national security and privacy

		Privacy	
		+	-
National security	+	**Congruence between national security and privacy (33 manifestations):** Regulation and policy dealing with cybersecurity and information protection, which strengthen national security and privacy simultaneously (e.g., setting standards for protecting healthcare, financial, and government systems).	**National security at the expense of privacy (31 manifestations):** Mostly national security and law enforcement policy promoting data gathering, which weakens the technological infrastructures for the sake of national security at the expense of privacy (e.g., the 2001 Patriot Act, permitting extensive information gathering in the name of national security at the expense of privacy).
	-	**Compromise between national security and privacy (21 manifestations):** Policy manifestations limiting state information gathering for the intent of national security (e.g., a 1978 law creating a system of checks and balances for intelligence agencies' information gathering).	

way national security and intelligence agencies could exploit cyberspace. Despite what was said in the literature, these policy manifestations are not on the same axis or level. Each category is important for understanding the overall relationship between national security and privacy in the digital era in which the state is both the solution for strengthening regularization in cyberspace and privacy protection and also the problem, as it represents a constant threat to privacy as it seeks to strengthen national security.

Findings

The State's First Function: National Security ≠ Privacy

The state exploits cyberspace for information gathering for the sake of strengthening national security at the expense of privacy

Figure 1 below describes the change affecting the relationship between national security and privacy as it is structured by the state before and after the digital era. Starting in the mid-1990s, it is possible to identify a clear trend at the federal level of preferring national security over privacy. By

counting the policy manifestations each year, figure 1 presents the quantitative difference between policy that limits information gathering by security and intelligence agencies for the sake of protecting privacy and policy that encourages information gathering for strengthening national security at the expense of privacy. Restrictions on information gathering include new arrangements and laws creating accountability, reporting obligations, and limiting criteria that must be considered when information is gathered for the purpose of national security. Encouraging information gathering includes reducing or bending these limits or demanding technological changes, such as reduced encryption for information gathering by intelligence agencies. The key weakness of this figure is that it only describes quantitative change in the trend and ignores the significance of each of the regulations and laws examined. Nonetheless, a bird's-eye-view of the federal regulations can indicate a changing trend. In the 1970s and 1980s, the federal arena was characterized by many more policy manifestations that struck a compromise between national security and privacy (the line above the X axis), but, from the mid-1990s, the line has been generally below the X axis, representing a quantitative preference for national security over privacy.

Figure 1: (Policy promoting privacy) – (policy promoting security) every year, 1967–2016

In order to understand and explain what was behind the post-1990s trend evident in figure 1, it is necessary to examine the functioning of the relevant federal authorities and business groups. From the mid-1990s, the executive branch began to remove obstacles to information gathering and

successfully used its political clout to exploit cyberspace for its needs. During the 1960s and 1970s, the executive branch had lost its public legitimacy to violate privacy for the purpose of national security, following the discovery of espionage cases for political purposes that involved American citizens. Congress appointed investigating committees, such as the Church Committee, which, by the time they had completed their hearings, recommended imposing significant limitations on information gathering in order to increase privacy. These recommendations turned into legislative bills that became law in the 1970s and 1980s and greatly limited information-gathering methods. Even the executive branch itself, by means of executive orders issued by Presidents Ford and Carter in the late 1970s, imposed limits on information gathering due to privacy concerns.

Beginning in the mid-1990s, however, the legitimacy for information gathering changed. Public protest over privacy protection had died down and the war on terrorism gradually took center stage, justifying violations of privacy for the sake of national security. The executive lifted constitutional obstacles and rendered mechanisms for supervising information gathering irrelevant. This trend started as early as 1981 when President Reagan issued a controversial executive order (No. 12333), which authorized information gathering beyond US borders, including information about American citizens, without any significant oversight. While the directive applied to events outside the United States, it had a major impact on the privacy of American citizens in the global internet environment that grew exponentially in the mid-1990s.

The digital era blurred sovereign borders. Companies such as Google and Yahoo began storing personal information wherever it was economically most convenient for them, without regard for their customers' sovereign nations. Thus, information about American citizens may be stored in Asia or Europe and therefore—based on that executive order—be subject to search. The permissive nature of the executive order granted the National Security Agency (NSA) the legitimacy to create internet surveillance programs and to gather information about many American citizens. In practice, that executive order allows unsupervised information gathering also by Congress and the judiciary, without requiring the consent of the commercial company that originally had collected the information. The information gathered includes not just headlines but also content, without requiring that the intelligence agencies provide any evidence indicating the need for intelligence gathering.[24]

Furthermore, the attorney general's directives of 1983, 1989, and 2002 expanded the states' mandate to gather information without any orderly state discourse or procedure and without the necessary checks and balances. An extreme example of preferring national security over privacy was the surveillance programs that operated between 2001 and 2007 under President George W. Bush. On his own initiative, the president decided to approve and execute surveillance of US citizens in stark contravention of existing privacy laws. The programs were secretly operated by various intelligence agencies and were partly stopped only after the *New York Times* exposed them in 2005.[25] Over the years, the US administration also expanded the use of the so-called National Security Letters, unique policy tools that could gather information from civilian companies during emergencies. As is often the case, the use of "emergency" tools became almost routine in state information-gathering efforts, exceeding the legislator's intent that established them within the context of financial information through the Financial Privacy Act of 1978.

Since the mid-1990s, the legislative branch has also been an important player in the changing trend of privileging national security over privacy. In the 1970s and 1980s, the US Congress actively limited information gathering on US citizens for the purpose of national security. Most activity was carried out through specially appointed committees, such as the Church Committee and the Pike Committee, and the important legislation that followed their recommendations, such as the 1978 Foreign Intelligence Surveillance Act (FISA), and the 1986 Electronic Communications Privacy Act (ECPA). However, starting in the mid-1990s, Congress started passing laws that breached the limits imposed in previous years. Only in 2015, for the first time in three decades, Congress passed the USA Freedom Act that limits information gathering for the sake of national security. Over the last twenty years, those who championed privacy in Congress were weakened and subordinated to national security decision makers. Congress shifted from mediating between privacy and national security to backing the administration by supporting information gathering at the expense of privacy. For example, starting in the mid-1990s, Congress allowed very aggressive legislation on surveillance and green-lighted "temporary" practices that rapidly became permanent. The Patriot Act following 9/11 may have been the most conspicuous of such laws, but it was not alone. The amendments to FISA in 2007 and 2008 also

reflected the trend of weakening the limitations on information gathering and preferring national security over privacy. The trend is manifested, inter alia, in a blurring of boundaries between information gathering for national security and information gathering for crime prevention. While the latter used to be closely supervised and required good reason demonstrating that the information would help an ongoing investigation, the former was never subject to such limits and had always been conducted more freely. But, starting in the 2000s, the boundaries between the two were blurred by the Patriot Act, leading to privacy violations for the sake of national security. Information gathering on behalf of national security in order to enforce the law allows surveillance of US citizens without appropriate checks and balances.

Finally, since the mid-1990s, even the judiciary in the United States has preferred national security over privacy. Throughout the 1970s and 1980s, the courts paved the way for several laws through important rulings that either promoted or violated privacy. One key example is the precedent-setting 1967 decision (Katz v. the United States 389 US 347), which determined that the right to privacy is embedded in the Fourth Amendment and applies to any person regardless of physical location. This ruling was the basis for the first privacy protection law, passed in 1968, and was binding during the gathering of information in order to prevent crime (The Omnibus Safe Streets and Crime Control Act). A second ruling from 1976 (The United States v. Miller 425 US 435) harmed privacy, which in turn led to legislation that reigned in that violation. The ruling stated that people are not entitled to privacy protection by a third-party supplier if they provided them with information on their own free will. In response, in 1968, Congress passed the ECPA to strengthen privacy in the emerging tech-based communications channels.

In contrast, by the 1990s and 2000s, the role of the court had been marginalized. Through a number of cases, the judiciary imposed limitations on information gathering using practices reserved for emergencies, such as the National Security Letters, but these limitations were few. Most of the time, the courts were unsuccessful in limiting privacy violations or stopping intensive state information gathering during the onset of the war on terrorism. On the contrary, through the Foreign Intelligence Surveillance Courts (FISC)—courts specifically designated to approve information-gathering orders—the judiciary helped the state in its surveillance efforts. In these discussions, the judges—lacking the technological knowledge

needed to understand the issues at hand—approved unusual and controversial NSA requests for information gathering. These approvals allowed other intelligence agencies to further expand their own surveillance. Looking at the last four decades through a wide-angled lens, one can sweepingly conclude that the judiciary shifted from delivering important decisions that affected legislation to advance privacy in the 1970s and 1980s, to issuing marginal rulings or those that encouraged surveillance to advance national security in the 1990s and 2000s.

Beyond the actions of the various branches of government in structuring the relationship between national security and privacy, the business interests of data communications companies had a decisive effect on the new trend. In the 1970s and 1980s, privacy protection by these companies was considered a commercial advantage in a developing market. Lobbyists for the communications companies worked with civil society representatives to help pass legislation that would limit surveillance and protect customer privacy. Privacy protection laws that passed with the support of these groups included the Financial Privacy Act of 1978 and ECPA in 1986. Starting in the 1990s, however, the partnership between civil society representatives and company lobbyists dissolved as their interests diverged. The turning point was in 1994, when Congress, led and pressured by the FBI, passed the Communications Assistance for Law Enforcement Act (CALEA). The law demanded that commercial companies allow law enforcement agencies to gather information from their communications infrastructures by changing working interfaces so that states now had access to all US citizens' communications data. The legislature provided business owners with handsome compensation, and they fell in line and acceded to state demands for information. The close relationship of the security establishment—including the intelligence agencies—with business owners in the United States intensified through the 1990s and 2000s. Most of this cooperation is not done openly. What we do know is the high number of joint ventures around the use of the National Security Letters for information gathering and the mandate that internet providers were given thanks to the Patriot Act to surveil their customers based on minimal justification.

In recent times, thanks to Edward Snowden's revelations, we have seen the emergence of a new trend. The interests of commercial companies and civil society over privacy are once again aligning. For example, we can

point to Apple's refusal to crack the encryption on the cell phone belonging to the San Bernardino terrorist and Microsoft's rebuff of law enforcement demands to reveal customer information stored in servers in Ireland, outside US jurisdiction. In both instances, privacy considerations outweighed state desire to gather information on behalf of increasing national security. In 2013, there was an attempt to pass CALEA II, named after the first law on the subject from 1994, but it encountered fierce opposition from the communications industry, as privacy has once again become a business and competitive advantage for commercial companies and a way of winning over consumers.

The State's Second Function: Congruence Between National Security and Privacy

The state promotes cybersecurity and privacy protection, simultaneously strengthening national security

Parallel to the state's efforts to exploit cyberspace to gather information for the purpose of national security while also violating individuals' privacy, the state has also carried out extensive regulation and legislation to jointly promote national security and privacy through the strengthening of cybersecurity. This work is limited and only partly advanced, however, due to the predominance of business interests in this field. From a broader perspective based on three decades, three key components can be discerned: First, national security and privacy protection efforts through the strengthening of cybersecurity are focused on very specific sectors. As part of the traditional American approach of regulatory non-intervention in business, commercial companies and communications services are bound only by voluntary guidelines that do not sufficiently strengthen neither national security nor privacy. Second, the administration's attitude to the internet economy, since its inception, has been one of non-intervention, making it possible to gather private information for commercial purposes. This generated the institutional conditions for today's massive commercialization of private information by the giant data monopolies, such as Google and Facebook, and the mortal blow dealt by commercial companies to consumer privacy. Third, some examples of regulation whose purpose is to strengthen cybersecurity also violate privacy. The Cybersecurity Information Sharing Act (CISA) of late 2015 permits information gathering without a court order in order

to concentrate information about cyber threats in the business sector and generate a defensive response ahead of time.

The following section is divided into two parts, explaining the limited protection of privacy and national security through data system protections and the inherent contradiction between cybersecurity and privacy in the role of the state.

Preserving national security and privacy by sector and in a limited fashion

The need to secure computerized systems and digital data has been a major concern for federal decision makers in the United States since the mid-1980s.[26] Despite the tremendous growth of the internet economy, however, the state promotes national security and privacy on a sector-by-sector basis limited to healthcare, financial services, and the federal government itself, while increasing society's dependence on a stable, functioning cyberspace. While most regulatory obligations imposed by the state affect the sectors viewed as critical to state functioning, the other industries—representing the bulk of cyberspace—are handled by self-regulation and a policy that does not pose a hardship to industries. Figure 2 below describes the federal government's ineffectiveness to promote a robust cross-sector cyberspace, which would in turn ensure better national security and greater privacy. While the government does a great job protecting itself, it abandons industry and commercial companies to their own voluntary protective practices.[27]

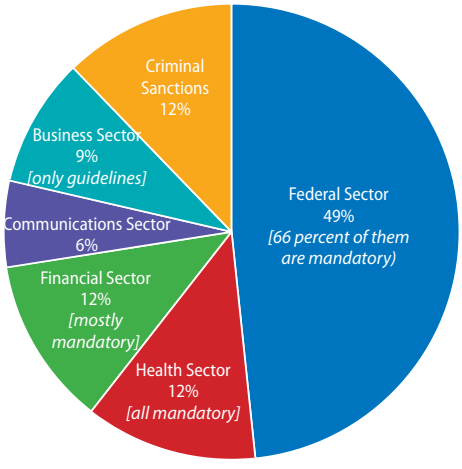


Figure 2: Federal policy on privacy protection and cybersecurity (1974–2016)

Business owners managed to avoid being included in binding data protection regulation at a very early stage. The Privacy Act of 1974 was passed by Congress based on the understanding of the importance of preserving personal information in state hands. During the debates preceding the passage of the law, commercial companies claimed there was no real evidence that they had committed privacy violations. Their working assumption was that they were already collapsing under the burden of regulatory demands; the bill was not needed and would only further add to that burden.[28] Their strategy was to urge commercial companies to adopt self-regulation, thus reduce the burden of government regulation on business owners. The business sector also opposed the establishment of a federal agency to enforce customer privacy. In fact, the Senate bill, which included the establishment of such an enforcement agency, was shelved. Finally, the law that was passed in 1974 included minimal privacy protection discussed at the time. The trend continued until the mid-1990s, when the federal government responded to the growing internet economy by establishing regulation for the protection of privacy and cyberspace—and thus also national security—in only some of the branches of the business sector (healthcare, finances, and so forth), leaving most of it without any binding regulation. In 1997, President Bill Clinton and Vice President Al Gore issued their policy paper, "Framework for Global Electronic Commerce," in which cyberspace was described as critical for economic growth and should not be subject to regulatory limitations that would impede economic development. The paper called for adopting self-regulatory models and left the process of decision making about privacy protection in the hands of commercial companies. Since that framework was issued, commercial companies have been the sole decision makers of their customers' privacy level, paving the way to the unbridled practice of commercializing customer information for profit.

Over the years, Congress has looked at dozens of bills aimed at increasing supervision and protecting citizen privacy, which has long been at the mercy of business interests, but only a few in healthcare and financial fields were passed into law. Personal health information, which was deemed sensitive, was assured protection by the Health Insurance Portability and Accountability Act (HIPAA) of 1996. It was the first time that any sort of privacy was enshrined in law. The private sector was adamantly opposed, as it worried about costs and regulation not aligned with reality. But, after seven

years, in 2003, compliance to the law became obligatory. In the financial sector, the Gramm-Leach-Bliley Act was passed in 1999 to protect financial systems and citizens' privacy. And, in 2002, after the collapse of Enron and WorldCom, the Sarbanes-Oxley Act (SOX) was passed to tighten control of commercial companies, which included various information protection practices. In 2010, after two decades or so of selective attention, the US Department of Commerce began to take an interest in cybersecurity and privacy protection in the private sector. But rather than change the voluntary approach of regulation to one that is fully binding and enforced, two policy papers were produced, advocating for the implementation of information and privacy protection strategies that exempt private companies. The first paper suggested adopting federal standards that are binding upon federal agencies and were passed into law in 1974 and applying them to the private sector. The paper also called for the establishment of a federal privacy protection agency as part of the Department of Commerce. In a certain sense, the policy papers sought to revive failed bills from the 1970s, while also exempting the business sector from protecting customer privacy. The second paper defined a new sector, the Internet and Information Innovation Sector (I3S), and it contained technical recommendations for companies facing threats to privacy and cyberspace. Nonetheless, despite that the papers offered much needed remedies, the level of customer privacy protection in commercial companies continues to be at the mercy of the companies themselves and are only subject to fair trade principles enforced retroactively by the Federal Trade Commission.

Since 2013, the regulatory agencies have themselves become quite active in cybersecurity and privacy protection. The Federal Communications Commission (FCC) issued a strategy paper with practical recommendations for system and user privacy protection. Moreover, in 2015, the US Court of Appeals for the Third Circuit determined that the Federal Trade Commission (FTC) has enforcement authority also when it comes to cybersecurity and not only in cases of privacy violations (FTC v. Wyndham Worldwide Corporation). The ruling was significant because prior to it, the FTC's enforcement authority had been focused on privacy violations and relied on fair trade practices. Now, thanks to the court, the FTC had a new institutional standing. The increasing influence of regulatory agencies was again evident in 2016, when the FCC shifted from recommendations to action and issued a binding law requiring

internet service providers to protect their customers' data and privacy. The new law also requires full transparency on how ISPs use personal information. However, with the current US administration, in January 2017, President Trump appointed Ajit Pai as the FCC's new chairman who hurried to strike the new laws off the books.

In the state's attempt to promote both privacy protection and national security by enhancing cybersecurity, we witness only sectorial actions, an absence of a central, independent enforcement agency, and the creation of conditions that allow companies to profit from private information and violate privacy even further. Binding cybersecurity regulation is not adopted, because it is seen as being costly to business. Thus, privacy protection regulation is adopted only sporadically so as not to impact the earnings of those who have based their business model on making money from private, personal information.

Cybersecurity, the right to privacy, and the contradiction between the two

Beyond the limited capacity of promoting privacy protection and national security by applying binding cybersecurity regulation, the state, paradoxically, sometimes promotes cybersecurity while violating privacy. Recently, a new concept—SIGINT cybersecurity—has come into vogue and it describes the use of gathering information about cyber threats in order to defend cyberspace.[29] While the term is new, the practice has been in use for very many years, with state support, especially since 9/11.

As early as 1984, there was concern about privacy violations for the sake of information protection. Thanks to National Security Directive No. 145, President Reagan granted the NSA the authority to protect all government databases. The decision, made after the discovery of surveillance by US security services—especially by the Church Committee in 1976—worried many legislators; in response, Congress passed a law granting the National Institute for Security Standards (NIST), a civilian agency, the authority also granted to the NSA. Still, the institutional standing of NIST compared to that of the NSA was weak. In 1989, both agencies signed a memorandum of understanding according to which the NSA would not lose any of the authority that it had been granted by President Reagan. These circumstances continued until 2001, when the Patriot Act allowed law enforcement agencies to surveil the communications data of possible suspects in order to root out

cybercrime. The law allows judges to impose sweeping orders on suspects anywhere in the United States and to gather extensive information—including technological data—needed to identify and track suspects. The tension between protecting privacy and protecting data was also manifested in the Comprehensive National Cyber Security Initiative (CNCI) issued in 2008. The strategy was published to ensure that federal authorities are impenetrable to cyberattacks. The way to do so was, in part, by encouraging information gathering and using the intelligence agencies' encryption breaking capabilities (which obviously involved privacy violations) for the purpose of defending federal data. In 2015, the Cybersecurity Information Sharing Act (CISA) was passed, making it possible to gather information from the private sector in a non-transparent manner for the sake of promoting cybersecurity, increasing the tension between privacy protection and cybersecurity. According to CISA, commercial companies that previously chose to share information with the state have no third-party accountability in the case of a cyberattack. This represents a significant incentive for the state to gather information without a court order or clear justification.[30]

Conclusion

Over the last five decades, the United States has played a dual, contradictory role when it comes to promoting national security and protecting privacy in the digital sphere. In the state's first role—exploiting cyberspace to gather information for the purpose of national security but at the expense of privacy—all federal authorities foster and promote a trend privileging national security over privacy. Since the mid-1990s, there has been an asymmetrical balance of power between the executive and legislative branches of government on the one hand and close cooperation between the state and private commercial companies possessing vast amounts of personal data on the other. In the state's second role of promoting cybersecurity to increase both national security and privacy, we are witnessing the fierce opposition of commercial companies to binding regulation for promoting cybersecurity. These trends have created a digital sphere that is not only exploited by the state while violating privacy but is also insufficiently secure against external threats to privacy. Cyberspace came into being as dependence on technological systems in all economic branches expanded. It was a completely new sphere that the state had to police. But thanks to a neoliberal regulatory culture

and the state's supposedly hands-off approach, the public interest has been subsidiary to the power of both intelligence agencies and the business world. While the United States is guilty of many violations of its citizens' privacy in order to promote its goals of national security, it has failed to promote regulation that would secure cyberspace itself and thus also both national security and privacy, just as it secures public assets in other areas of life.

After several decades of public policy structuring the relationship between national security and privacy, this article has highlighted the urgency of changing the discourse and actions of the current policy. The framing of the discourse on cyberspace policy—i.e., referring to cybersecurity as a systems component rather than a component of the security and privacy of individuals—must change. While the traditional definitions of cybersecurity deal with securing systems against hackers and grants intelligence agencies, security institutions, and the business sector the mandate to gather information, the emerging discourse expands the surveillance capabilities, limits encryption, and allows backdoors to be installed without appropriate accountability. These practices significantly harm individual security and privacy and present the social dependence on cyberspace as a factor that weakens society.

Based on the empiric examples in this article, state actions in cyberspace are cause for concern. The discourse must change so that the security of individuals is emphasized. This means giving subjects of personal information full ownership over that information, the sweeping use of encryption, and the establishment of supervision and accountability mechanisms over state information gathering in order to rein in the power of the state and of business monopolies. We must consider civil interests, and not only security or intelligence ones, and make sure that the public interest promoted appropriately in cyberspace.

Using the literature on regulation as a tool for managing risk and analyzing the findings in cyberspace enables us to discern the flaws stemming from the state's role as society's manager of such equivocal risks. In reviewing the literature, the article asked the key question that has preoccupied scholars who have adopted the approach that the state's function is to act as society's risk manager: Are state actions of risk management a consequence of new risks emerging around us, which make it necessary to ensure that the public interest is promoted given the new circumstances? Or is the state, first and foremost, interested in its own institutions and less careful about ramifications

of its risk management policy on the public? Findings from cyberspace indicate that both are true to an extent. When the state exploits cyberspace to its own ends, it significantly violated privacy in a way that ensures the promotion of security and intelligence agencies' goals at citizen expense. When the state tries to promote cybersecurity, it does so in a way that fails to promote the public interest; beyond the sectors defined as sensitive, the state is subject to pressure from business. Risk management in two partially congruent regimes—national security and privacy—challenges the existing literature and sheds lights on the complexity of the role of the state as society's risk manager.

The limitations of this research are primarily the result of its broad perspective and the conceptualization of a new analytical framework for studying public policy across five decades. Given the far-ranging description, this article did not address the mechanisms that are behind national security and privacy preferences in every area of policy and did not analyze in-depth the public policy processes that affect a single case. Therefore, future research focusing on a single area of policy in the context of the relationship between national security and privacy could allow a better understanding of the state's risk management in a given sphere.

Notes

1 The checks and balances of the executive branch of government include specially designated courts established to handle state surveillance requests by state and the congressional committees to which federal intelligence authorities must periodically report. Still, despite the long-established institutional ability, the 2013 papers leaked by Edward Snowden revealed how these mechanisms are generally a rubber stamp, failing to carry out effective monitoring and control of the government's bulimic appetite for data. The limited and slanted interpretation of the NSA of the regulatory infrastructure supervising it is especially troublesome. For the lack of effective supervision of information gathering, see some 3,000 cases in which the NSA admitted its "mistakes" at https://goo.gl/hFGmsj; for the inability to supervise complex NSA technological requests, see a judge's testimony at https://goo.gl/XEWHCZ.

2 Fernando Mendez and Mario Mendez, "Comparing Privacy Regimes: Federal Theory and the Politics of Privacy Regulation in the European Union and the United States," *The Journal of Federalism* 40, no. 4 (2009): 617–645; Ronald Deibert and Rafael Rohozinski, "Risking Security: Policies and Paradoxes of Cyberspace Security," *International Political Sociology* 4, no. 1 (2010): 15–32.

3 David Flaherty, *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States* (Chapel Hill: University of North Carolina Press, 1989); Priscilla Regan, *Legislating Privacy: Technology, Social Values, and Public Policy* (Chapel Hill: University of North Carolina Press, 1995).

4 Amitai Etzioni, "Cybersecurity in the Private Sector," *Issues in Science and Technology* 28, no. 1 (2011); Janine Hiller and Roberta Russell, "The Challenge and Imperative of Private Sector Cybersecurity: An International Comparison," *Computer Law & Security Review* 29 (2013): 236–245; Richard Harknett and James Stever, "The New Policy World of Cybersecurity," *Public Administration Review* 71, no. 3 (2011): 455–460.

5 See the attorney general's directives of May 30, 2002, spelling out a new strategy that includes information monitoring and gathering to prevent terrorism after 9/11: https://fas.org/irp/news/2002/05/ag053002.html.

6 This was despite the common procedures for privacy protection in Europe, which were instituted in the 1980s in the OECD. The peak was 1995 with the institution of strict, binding information protection regulations in all EU nations.

7 Lee Bygrave, *Data Protection Law – Approaching its Rationale, Logic, and Limits* (Kluwer Law Intl, 2002); Samuel Warren Louis Brandeis, "The Right to Privacy," *Harvard Law Review* 4 (1890): 193–220.

8 Alan Westin, *Privacy and Freedom* (New York: Atheneum, 1967) Charles Fried, "Privacy," *Yale Law Journal* 77 (1968): 475–493; James Rachels, "Why Privacy is Important," *Philosophy & Public Affairs* 4, no. 4 (1975): 323–333; Kenneth Laudon, "Markets and Privacy," *Communications of the ACM* 39, no. 9 (1996): 92–104; Lawrence Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books, 1999).

9 Ruth E. Gavison, "Privacy and the Limits of Law," *Yale Law Journal* 89, no. 3 (1980): 421–471.

10 Julie Innes, *Privacy, Intimacy, and Isolation* (New York: Oxford University Press, 1992).

11 Emma Rothschild, "What is Security?" *Daedalus* 24, no. 3 (1995): 53–98.

12 Jeremy Waldron, "Safety and Security," *Nebraska Law Review* 85, no. 2 (2006): 454–507.

13 David Lyon, *Surveillance Society: Monitoring Everyday Life* (Buckingham and Philadelphia: Open University Press, 2001); Priscilla M. Regan, "Response to Bennett: Also in Defense of Privacy," *Surveillance & Society* 8, no. 4 (2011): 497–499; Colin J. Bennett, "In Defense of Privacy: The Concept and the Regime," *Surveillance & Society* 8, no. 4 (2011): 485–496

14 Ronald Dworkin, *Taking Rights Seriously* (Cambridge: Harvard University Press, 1977); Jeremy Waldron, "Security and Liberty: The Image of Balance," *Journal*

of Political Philosophy 11, no. 2 (2003): 191–210; Lucia Zedner, "Too Much Security?," *Journal of Sociology of Law* 31, no. 3 (2003): 155–184.

15 Simon Hallsworth and John Lea, "Reconstructing Leviathan: Emerging Contours of the Security State," *Theoretical Criminology* 15, no. 2 (2011): 141–157.

16 Deibert and Rohozinski, "Risking Security."

17 Mendez and Mendez, "Comparing Privacy Regimes."

18 Regan, *Legislating Privacy*; Flaherty, *Protecting Privacy in Surveillance Societies*.

19 Abraham Newman and David Bach, "Self-Regulatory Trajectories in the Shadow of Public Power: Resolving Digital Dilemmas in Europe and the United States," *Governance* 17, no. 3 (2004): 387–413.

20 Etzioni, "Cybersecurity in the Private Sector."

21 Hiller and Russell, "The Challenge and Imperative of Private Sector Cybersecurity."

22 Kenneth Bamberger and Deirdre Mulligan, "Privacy on the Books and on the Ground," *Stanford Law Review* 67 (2011):247–316.

23 The Supreme Court decided that audio surveillance of phone calls violates the right to privacy as established by the Fourth Amendment and determined that the right to privacy is a right extended to all people regardless of their physical location.

24 In July 2014, John Napier Tye, a former State Department employee, published an opinion piece in the *Washington Post*, which provided a clear explanation of the relevance of this executive order to the violation of the balance between national security and privacy in the United States. See John Napier Tye, "Meet Executive Order 12333: The Reagan Rule that Lets the NSA Spy on Americans," *Washington Pos*t, July 18 2014, https://wapo.st/2Ttlqti.

25 See the leak and the 2005 report in the *New York Times*: James Risen and Eric Lichtblau, "Bush Let U.S. Spy on Callers Without Courts," *New York Times*, December 16, 2005, https://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html.

26 Michael Warner, "Cyber Security: A Pre-history," *Intelligence and National Security* 27, no. 5 (2012): 781–799.

27 Newman and Bach, "Self-Regulatory Trajectories in the Shadow of Public Power."

28 Regan, *Legislating Privacy*.

29 See the discussion of the concept in Dennis Chow, "Using Signals Intelligence within Cyber Security," *Eforensics*, November 12, 2015, https://eforensicsmag.com/dennis-chow.

30 See the article by a private investigator on the issue in Jennifer Granick, "OmniCISA Pits DHS Against the FCC and FTC on User Privacy," *Just Security*, December 16, 2015, https://www.justsecurity.org/28386/omnicisa-pits-government-against-self-privacy.