

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

Ido Sivan-Sevilla 

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

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

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

关键词： 国家安全，隐私，监控，网络安全，临时政策趋势，政策舞台

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

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

Introduction

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

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

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

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

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

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

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

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

Literature Review

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

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

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

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

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

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

Conceptual Clarifications: National Security and Privacy

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

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

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

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

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

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

Analytical Framework and Methodology

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

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

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

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

The third regulatory regime under study, cybersecurity,¹⁰ involves policies that protect vital personal information networks, including those of the federal government and of health and financial service providers. The start of this regime can be pinpointed to the passage of the National Security Directive (NSD) #145 and the Comprehensive Crime Control Act of 1984, through which the government began sanctioning cyber-criminals and protecting federal networks. Most policies in this regime enhanced the protection of personal information in vital systems, but some introduced new threats to privacy.

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

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

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

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

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

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

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

Analysis Over Time

Contradictory Relationships

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

First Period: 1968–89

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

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

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

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

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

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

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

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

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

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

Second Period: 1993–2012

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Third Period: 2013–18

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

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

In 2015, Congress passed the U.S. Freedom Act. This statute, enacted after the sunset of the Patriot Act's Section 215, limited privacy-harming national security practices for the first time since 1978 by ending the direct bulk collection of phone call metadata.⁴⁸ It also required the appointment of external technical personnel to secret FISA Courts, and publication of further rulings that set new surveillance authorization precedents. The Act required security agencies to be as specific as possible when issuing NSLs, noted that the disclosure of a letter request should not conclusively be treated as a danger to national security, and allowed these requests to be challenged in court.⁴⁹

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

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

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

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

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

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

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

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

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

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

Complementary Relationships

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

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

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

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

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

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

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

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

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

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

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



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

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

Analysis Across Policy Arenas

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

Information Collection for Criminal Investigations

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

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

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

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

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

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

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

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

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

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

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

Foreign Intelligence

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

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

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

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

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

Cybersecurity

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

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

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

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




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

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

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

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

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

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



Conclusion

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

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

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

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

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

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

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

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

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

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



Notes

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

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

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

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

64. The 1996 Clinger–Cohen Act mandated this assignment.
65. As outlined in OMB’s policy memos—M-07-16 (2007), M-08-23 (2008), M-10-28 (2010), M-17-05 (2016)—the agency (i) posed breach notification requirements in 2007; (ii) required the deployment of the more secure DNSSEC protocol in 2008; (iii) expanded the operational role of DHS in federal networks in 2010; and (iv) published a policy to increase its oversight capacities over information security in federal agencies in 2016.
66. DOC’s strategy document, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework*, argues that “many key actors, due to the sectorial privacy and cybersecurity approach of the U.S., operate without specific statutory obligations to protect personal data” (p. 12; see https://www.ntia.doc.gov/files/ntia/publications/iptf_privacy_greenpaper_12162010.pdf). The strategy addresses the privacy and security problems of “non-critical” sectors and recommends the adoption of privacy standards and federal breach notification rules, after a decade of failed attempts to do so. These are rules that require companies to report and face financial consequences in case of a data breach. Currently, the United States has 47 versions of breach notification laws across states and was unable to pass unified federal legislation despite many attempts since 2003. There is controversy over issues like federal preemption, desired policy goals, scope of notification, and effectiveness of policy (Thaw, 2015).
67. The strategy document is the *Cybersecurity Risk Management and Best Practices Working Group 4: Final Report March 2015*, FCC. See https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf.
68. The new FCC chairman, Ajit Pai, blocked FCC requirements from ISPs to apply common sense security practices and protect personal information. More on this policy process is available at <http://stlr.org/2016/12/12/the-fccs-latest-privacy-regulations-a-new-stance-on-private-sector-protections/>.
69. James X. Dempsey’s testimony before the Subcommittee on Crime in the Committee on Judiciary, 1997. See https://fas.org/irp/congress/1997_hr/h971023d.htm.
70. For example, NSA wiretapping of an AT&T facility and Microsoft’s, Yahoo!’s, Google’s, Facebook’s, and Apple’s data centers through the PRISM program. See <https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>.
71. See Note 57.
72. For a summary of these failed attempts, see <https://www.accessnow.org/no-more-waiting-its-time-for-a-federal-data-breach-law-in-the-u-s/>.
73. See the June 21, 2016 meeting minutes from the Commission on Enhancing National Cybersecurity on private sector cybersecurity challenges at https://www.nist.gov/sites/default/files/june_21_2016_uch_meeting_minutes.pdf. Also see an overview of the role of the state in the private-sector cybersecurity challenge: <https://www.georgetownjournalofinternationalaffairs.org/online-edition/2018/5/27/the-role-of-the-state-in-the-private-sector-cybersecurity-challenge>.
74. See CRS 2012 report by Eric A. Fischer on the numerous failed attempts to pass a federal information sharing legislation in Congress at <https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-073.pdf>.

References

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

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

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

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

Appendix: Methodological Annex

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

Data Collection and Sources

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

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

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

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

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

Data Classification

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

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

Continued

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

Continued

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

Continued

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

Continued

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

Copyright of Policy & Internet is the property of Wiley-Blackwell and its content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder's express written permission. However, users may print, download, or email articles for individual use.