3rd International Conference

on Public Policy (ICPP3)

June 28-30, 2017 – Singapore

Panel P11

Policy Regime Framework: Towards Better Theories of the Policy Process

Title of the paper

Dynamic Tradeoffs:
Security and Privacy in Cyberspace in U.S. Laws and Regulations 1968-2017

Author(s)

Ido Sivan-Sevilla, The Hebrew University of Jerusalem, Israel, sivan018@umn.edu

Date of presentation

June 28th

ABSTRACT

How does the U.S. trade security and privacy in cyberspace? In order to answer this question, we created a dataset of the relevant federal laws and regulations (N=70) for the years of 1968 and 2017 aiming to give a longitudinal, arena-based, and wide perspective on the development of federal policies. We then classified each law and regulation according to the extent that security and privacy compete or complement each other. This classification yields an analytical framework that provides a broad understanding of the policy trends, actors, and debates that shape the dynamics between security and privacy in cyberspace. The existing literature only partially tackles these dynamics. It also usually works within one of three issue domains: law enforcement, national security, or cyber-security, and focuses on a certain interaction between security and privacy over a limited time period. By contrast, this study brings these distinct policy domains together to reach a comprehensive understanding of the policy relationships between two desirable goals, security and privacy, at the U.S. federal arena. The findings shed light on varying policy dynamics of security and privacy across three time periods. We also find how different policy arenas mediate varying degrees of importance to security and privacy. By embracing a broad yet refined perspective, over time and across issues, this paper takes us one step further in understanding the trends and drivers behind the polymorphic role of the state in cyberspace. In the age of digital technologies, governments do not only advance but also undermine cyber-security and privacy to achieve 'greater' law enforcement and national security goals.

Key Words: Cyber-Security, Privacy, Regulatory Frameworks, United States

Dynamic Tradeoffs:
Security and Privacy in Cyberspace in U.S. Laws and Regulations 1968-2017

Security and privacy are two important goals. The extent to which these goals complement each other, however, is dynamically determined through laws and regulations in processes that take decades to unfold. History shows that attacks on privacy in the name of security happen all the time.[1] Whereas security is a fundamental goal and a platform to enjoy all other liberties (Waldron 2006), advancing it at the expense of privacy comes with a public cost. A loss of privacy means an erosion of essential values like anonymity, liberty, and free speech. Privacy poses constrains on abuses of government power and creates a boundary between the public and the private. The importance of properly advancing both security and privacy is significant to the democratic and liberal nature of society.

Technological developments have not only further skewed this balance in favor of security, but also created a platform for complementary security and privacy relationships. Indeed, the advancements in computer processing, networking, and storage capacities removed most technical limits for mass government surveillance. Instead of hand-picking its surveillance targets, the government can easily spy on everyone on a regular basis. Mass-surveillance is not only a result of new capacities, but also a product of the increasing social trend of voluntary sharing personal information in online environments. Societies are heavily invested in digital practices and flood cyberspace with publicly available personal information ready to be collected. This makes privacy a goal that is ever-more controlled by states and private companies.[2] At the same time, the essential role of digital technologies in our lives enhances complementaries between security and privacy. By increasing the security of cyberspace, we also safeguard the privacy of individuals whose personal data is processed online. These advancements in technology make cyberspace a promising sphere to consider when studying security and privacy dynamics in liberal

[1] Such attacks include FBI domestic surveillance practices from the 1960s and 1970 on Vietnam war activists and socialist movement, including extensive surveillance over Martin Luther King Jr. on a political basis. Later in history abuses of power were evident through NSA mass surveillance programs and backdoor installations on widely used digital technology. Another recent example is President's George W. Bush unlawful domestic surveillance programs from 2001 – 2007.

[2] Only laws and regulations, rather than technological capacities, stand between desires to abuse government power and the privacy of individuals.

democracies. As human society migrates to digital communications, the construction of these relationships becomes challenging but no less essential to liberal societies.

Looking at two desirable goals across time and space is rarely done in the public policy literature. It allows a better assessment on the extent to which both aims are promoted or downgraded by the state. It also reveals how the status-quo between security and privacy is dynamically assigned. A compromise constructed by policymakers at a certain point in time becomes irrelevant in new technological contexts. For example, the U.S. assigns low levels of importance to privacy of communications that take place overseas. They are solely governed by the Executive with lax internal oversight mechanisms. Within the U.S., however, privacy of communications is protected by the courts. Nonetheless, this dichotomy is no longer valid in a world of global communications. Regional borders have practically no meaning for telecommunications infrastructures and the reliance on this old-dated dichotomy is currently a source of violations of privacy for security. Moreover, studying two desirable goals that complement and contradict at the same time reveals power conflicts in the policy process and assists in understanding what is driving the security-privacy balance in the United States. This uncovers the values according to which society develops in the age of digital technologies and determines the accepted use of government power.

The paper asks how do the legislative and regulatory agendas in the U.S. trade security and privacy in cyberspace? More specifically, it asks how these dynamics vary over time and across three main issue-domains? The relationships between security and privacy are examined empirically, over the course of four decades, with regards to three main policy arenas - law enforcement, national security, and cyber-security - to find how safeguarding privacy is pressured by or complements with the security efforts of the state. It seems that in the past twenty years, security efforts are gradually taking over privacy in the U.S. federal arena. We also find that different policy arenas shape different relationships between security and privacy.

The current literature on security and privacy in cyberspace is not only addressing one of these policy goals. It also tends to focus on either contradictory or complementary dynamics and study a limited period and conflict. For example, those who solely

focus on security study the cyber-security arena (Harknett and Stever 2011; Etzioni 2011; Thaw 2013; Clark 2014; Warner 2012 and 2015; Cavelty 2010; Quigley 2012), whereas scholars that study only privacy do so with regards to tensions not only with security, but also with commercial and efficiency goals (Bennet 1992; Raab and Bennet 2003; Flaherty 1989; Newman and Bach 2004). Both groups of scholars increase our knowledge on how security and privacy policies developed, but do not consider their dynamics as important elements of the whole. Others, who study contradictory dynamics between security and privacy, tend to do so either in the law enforcement arena (Regan 1995; BeVier 1999; Soghian 2012; Nylund 2000, Dempsey 1997, Gidari 2006) or in both law enforcement and national security arenas (Logan 2009; Kleining et al 2011; Regan 2004; Diffie and Landau 2007; Birnhack and Elkin-Koren 2003). These studies enrich our understanding of how security mostly dominates privacy in U.S. federal policies over a narrow time frame. A few scholars study the complementary relations between security and privacy in the cyber-security arena (Hiller and Russel 2013, Regan 2009, Schwartz and Janger 2007) and discuss the barriers to advance such federal policies for the private sector. Finally, several scholars study both security and privacy in arenas where they complement and contradict at the same time (Mendez and Mendez 2009, Diebert and Rohozinski 2010). They do so, however, in a rather narrow empirical approach without a comprehensive analysis on the ways security and privacy in cyberspace are shaped over time and across arenas.

By contrast, this paper explores Federal laws, Executive Orders, Presidential Directives, Federal Final rules, and Federal Agencies' guidelines (N=70) between the years of 1968 and 2017 and classifies each to three distinct categories: (1) policies in which security and privacy complement each other; (2) policies that prioritize security over privacy; and (3) policies that create a compromise between security and privacy. This classification reveals three distinct policy periods and arenas that assign different levels of importance to security and privacy. We first identify the shifts in the importance of security and privacy over time. Whereas federal laws and regulations aimed to construct a compromise between security and privacy in the 1970s and 1980s, in the past twenty years, we witness a significant preference of security over privacy. This is evident through a legal framework that expands the ability of the government to collect information and by policies that create technological

mechanisms to make digital infrastructures 'surveillance-friendly.' Moreover, in policies for which security and privacy complement each other, the past twenty years show a protection over public networks and gaps in the extent in which security and privacy are mandated at the private-sector. Finally, in the past three years, following Snowden's disclosures on U.S. mass-surveillance practices, we witness policies that aim to increase oversight over government surveillance and slightly curtail some of the ability to collect information in ways that re-construct a compromise between security and privacy. Beyond variance over time periods, we also show how security and privacy are mediated differently across policy arenas: (1) at the law enforcement arena, the legislative process reflects a compromise between security and privacy. Policy debates take place publicly, with all stakeholders having an opportunity to voice their concerns. The pro-privacy interests of businesses and civil society converge and counter law enforcement security desires. This policy arena became central to the tension between security and privacy after a Supreme Court decision in 1967 that provided constitutional protection for privacy. Ever since, and upon technological developments, law enforces and policymakers usually debate on the extent of privacy violations for security purposes. (2) National security policies, however, work under concentrated and secret decision-making mechanisms. The executive aggressively pushes for security measures at the expense of privacy with very little scrutiny by Congress or civil society. Private businesses are secretly cooperating with government's desires to collect information for national security purposes. This policy arena became significant to the tension between security and privacy since the 1960s, when government surveillance powers were used for political reasons in the name of 'national security.' Congress was able to limit national security surveillance for the first time in 1978 through the Foreign Intelligence Surveillance Act (FISA). Since then, legislatures and regulators mostly support but also limit national security policies that undermine privacy. (3) In the cyber-security arena, which evolved already in the 1960s with the development of digital databases, security and privacy mostly complement each other. This arena is highly fragmented and brings together two conflicting interests - commercial and national security. This prevents from a coherent security and privacy strategy to evolve. The powerful position of private businesses in the policy process facilitates the embracement of self-regulatory rather than mandatory security and privacy standards, whereas the dominance of security agencies undermines privacy for cyber-security.

The analysis is organized in five sections. The first identifies the gaps in the literature. The second presents the methodology and analytical framework through which we test federal policies. The third section presents the shifts and changes in the relationships between security and privacy over time. The fourth identifies different dynamics between security and privacy across the three policy arenas. The last section concludes by assessing the implications of understanding the dual role of the state in cyberspace and addressing the limitations of this research. The paper also includes a methodological and empirical annex on data collection and codification.

1. LITERATURE REVIEW

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

Specifically, with the expansion of cyberspace and the increasing reliance of modern societies on digital technologies, the state adopts a dual role of protecting and utilizing cyberspace at the same time (Deibert and Rohozinski 2010), this role, however, has not been fully explored in the literature. We are still puzzled with regards to how security and privacy relationships are de-facto constructed by policymakers. Deibert and Rohozinski (2010) differentiate between risks 'to the security of cyberspace' and risks from utilizing cyberspace that are generated by states through cyber technologies in order to promote security and political goals. They recognize the contradiction between increasing cyber-security on the one hand, and utilizing cyberspace for surveillance on the other, but do not take us further to understand how this discrepancy is constructed and where does it come from in the policymaking process. Mendez and Mendez (2009) shed more light on the policy process behind these

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

conflicting goals. They jointly consider government laws and regulations that either protect or risk privacy and argue that both policy fields had experienced increased federal concentration of power. Their explanation has two phases. They first emphasize the increasing threat to U.S. commerce posed by strict EU privacy laws in the 1990s and view it as a federal incentive for changing the sectorial 'hands-free' privacy approach in the U.S. towards a more centralized federal approach in the form of a privacy monitoring agency (the FTC). Then, Mendez and Mendez (2009) argue that salient policy issues with 'a dangerous external threat', like the war on terrorism, led to even more centralized solutions by federal actors and paved the way for policies that violate privacy with very little scrutiny by Congress. Their findings raise an immediate puzzle – is this contradictory role of the state advances equally across all federal authorities? Since Mendez and Mendez (2009) base their conclusions on rather narrow empirical foundations,[4] we are still puzzled with regards to how the contradictory role of the state in cyberspace evolves. The authors' empirical analysis does not address the federal arena over time and fails to consider cyber-security policies as a tool for promoting privacy as well.

Other scholars have addressed either privacy or security to study one aspect of the state's role in a limited time period, but did not consider these attempts as part of the whole. Privacy policy scholars explain the lack of privacy protections by either the perception of privacy as an individual value, subordinate to other collective values[5] (Regan 1995), or by the lack of institutional capacities in U.S. to adequately promote privacy (Flaherty 1989). While these studies enrich our understanding on the policy processes that lead to insufficient privacy protections, they are rather outdated and focus on the 1970s and 1980s in the U.S. federal arena.[6] A more recent study by Newman and Bach (2004) analyzes the incentives behind the self-regulation model of digital privacy protections in the United States. They argue that latent threats and the potentially high cost of federal regulation dictate close collaborations between industries to avoid government regulation. While Neman and Bach (2004) shed light

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

[5] Such as national security and business efficiency

[6] What these scholars viewed as insufficient privacy protections is nowadays viewed as the 'golden age' of privacy that was followed by significant government surveillance expansions.

on why this 'hands-free' federal approach over privacy persists, we still lack an understanding of how and why this approach was decided upon in the first place.

Finally, scholars of security in cyberspace shed even less light on the policy process and the contradictory role of the state. Etzioni (2011) explains the reluctance of the private sector to binding cyber-security regulations, while Hiller and Russel (2013) attach the 'regulatory culture' in the U.S. to the self-regulation model of private-sector cyber-security. None of these scholars, however, address the dual role of the state empirically over time and provide explanations on the security and privacy policy processes.

2. METHODOLOGY

This study empirically traces the relationships between security and privacy in cyberspace as constructed by U.S. federal laws and regulations between the years of 1968 - 2017. The data set under study is inclusive and includes not only components of cyber-security and data protection policies, but also covers the promotion of national security and law enforcement goals. The following paragraphs provide (1) the reasoning for choosing the U.S. as a case study; (2) explain the decision to start analyze federal policies from the year of 1968; and (3) explain the type of policy events analyzed by this paper.

The U.S. is a promising case study. First, U.S. political and judicial spheres have a rich history with defining and deciding on privacy issues. Privacy was on the agenda as early as the year of 1890, with the seminal paper of Warren and Brandies on the right to privacy. Ever since, judges ruled over constitutional protections for privacy in conflicting ways and sparkled major privacy debates in society. At the political level, U.S. Presidents throughout the history were abusing government power and violating the privacy of Americans on a regular basis. This was a well-entrenched norm by the Executive, at least from the 1940s – 1970s, facilitated by the first head of the Federal Bureau of Investigations (FBI), J. Edgar Hoover. Thus, the U.S. case allows the tracing of privacy policies over long periods of time and in different contexts. Second, technology has been having a profound impact on the relationships between security and privacy. Since the U.S. enjoys high technological capabilities that allow

it to set the tone of digital advancements over the past several decades,[7] it serves as a promising case-study for balancing security and privacy in light of technology. The expansion of telecommunications networks, the development of commercially-used encryption, and the monopoly power of U.S.-based digital service providers, are all promising contexts for studying security and privacy in cyberspace. Third, the United States, as a major liberal democracy, experiences the tension between security and privacy in a great frequency and volume. The nation aims to safeguard the liberty of its citizens by democratic processes while also ensuring their security through advanced intelligence agencies. The importance of privacy is repeatedly emphasized in U.S. court rulings, laws, and regulations. At the same time, security is promoted through highly capable security agencies that often take advantage of technological infrastructures to fulfill their missions. Over the years, a series of whistleblowers and investigative journalists have provided data on this inherent tension and exposed how the U.S. government is often utilizing technological capacities for security purposes despite privacy consequences. These leaks and reports have traditionally led to public outcries and political re-construction of U.S. security and privacy dynamics.

The starting point for the policy events under study is the year of 1968. Two major developments for the relationship between security and privacy took place a year before and influenced the policy agenda since. In 1967, the Supreme Court had a landmark ruling,[8] that overturned a decision from 1928,[9] and provided constitutional privacy protections for the first time according to the Fourth Amendment. This decision had triggered significant policy actions on the balance between security and privacy, and established the first legal framework for government surveillance. In addition, the RAND research institute had conducted a 1967 study on security and privacy in information systems. This study provoked debates in the Department of Defense regarding new threats to security and privacy that shaped the tone of 1980s U.S. policies on computer security.

From the entire set of federal policymaking, this paper focuses on policies that affect both security and privacy at the same time in either way. We do not consider policies

[7] Some of the main infrastructures that the digital world relies on were developed in the United States: The Internet, digital switches, encryption, the operating systems from the U.S.-based Microsoft, Apple, and Google companies, Internet Search engines, and social networks.

[8] Katz vs. the United States

[9] Olmstead vs. the United States

that promote either security or privacy, and carry no implications on the relationships between the two. Examples for such laws include the 1998 Children's Education Privacy Act that protects the privacy of children but does not directly affect the promotion of security. In contrast, the 1998 Presidential Decision Directive 63 (PPD-63) promotes the security of critical infrastructures but has no implication on the right to privacy. Moreover, federal policies over time do not only contrast privacy with security, but also address privacy against interests of government efficiency[10] or financial gains.[11] We, however, chose to solely focus on security and privacy dynamics and filtered federal policies accordingly. Such filtering yielded federal policies[12] from three main security policy arenas – law enforcement, national security, and cyber-security.

2.1. Tradeoffs across the dataset

Following these filter schemes, we have created an original data set with policy events[13] (N=70) from the years 1968 – 2017 that address the collection of information for security purposes; limitations on government information collection in the name of privacy; and the promotion of data security in information systems that enhance both security and privacy.

Each policy event was classified to one of three policy categories according to the extent that security and privacy complement or contradict each other. The *first* category includes policy events from 1984 – 2016 that promote security and privacy at the same time (N=28). These are mainly cyber-security and privacy policies that aim to enhance the security of information systems as well as the privacy of

[10] For instance, the 1974 Privacy Act and the 1988 Computer Matching and Privacy Protection Act safeguard privacy against federal agencies' goals of providing better service for American citizens.

[11] For instance, the 1970 Fair Credit Reporting Act and the 2016 Federal Communication Commission (FCC) guidelines attempt to prevent commercial organizations from taking advantage of their customers' data for revenue purposes

[12] Choosing to solely focus on the federal level should be explained as well. Whereas national security policies are mostly conducted at the federal level, with intelligence agencies working almost exclusively at the federal arena, law enforcement and data privacy issues are significantly shaped by the states as well. Nevertheless, by focusing on one central policy level we can draw conclusions on the efforts of the federal government in each of these policy domains. The states mostly complement or fill a vacuum created by the federal government, but do so in various degrees, with a lack of coherent and unified approach. By studying a central and important arena like the federal level, we can reflect on how the federal government chooses to construct the relations between security and privacy through its policymaking efforts, and uncover tendencies to leave some of the decisions to the level of the states.

[13] Federal Legislation, Executive Orders, Presidential Orders and Directives, National Security Directives, Federal Register Rules from federal agencies, and Policy Guidelines from federal agencies that provide additional interpretation to federal statutes.

individuals whose personal information is processed by those systems. Examples include the 1990 National Security Council (NSC) Directive #42 that establishes guidelines and responsibilities for securing computer systems of national security and intelligence agencies, or the 2002 Title III of the e-government act, the Federal Information Security Management Act (FISMA), that applies mandatory security and privacy standards over federal information systems. Similar examples from other sectors are the 1996 Health Insurance Portability and Accountability Act (HIPAA) and the 1999 Gramm-Leach-Bliley Act (GLBA) that protect the security and privacy of health and financial records.

The *second* category includes policy events from 1976 – 2017 that promote security at the expense of privacy (N=26). These are policies that open new avenues for government information collection. Two types of policies stand out in this category. First, there are policies that expand the legal authority of the government to collect information with lax privacy safeguards. Examples include the 1981 Executive Order #12333 that authorizes the collection of information overseas for national security purposes without oversight or scrutiny by Congress. Information can be collected on U.S. citizens, without a court order, as long as it is related to a foreign intelligence investigation. Another example is the 2001 "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorist Act" (Patriot Act) that amends various privacy laws and acts to increase government information collection. With its many sections, the Patriot Act allows the collection of any 'tangible information', across all sectors, for security investigations, and blurs the boundaries between information collection for law enforcement (criminal) and national security (foreign intelligence) purposes.[14] The second type of policies in this category creates or alters technological infrastructures to allow government information collection. Most of these kinds of policies are government programs, headed by the NSA, that were mostly secret before exposed to the public by whistleblower Snowden.[15] Examples from Congress and the Administration are

[14] While information for criminal prosecutions should be collected with a warrant and upon a 'probable cause', foreign intelligence information collection enjoys lesser barriers. The erosion of boundaries between the two significantly jeopardizes privacy.

[15] Exposed NSA programs to weaken digital infrastructures include working with private companies like Cisco to make their devices accessible for the government and install backdoors in the company's routers; attempts to subvert encryption standards facilitated by NIST in a way that would be easy for the government to decrypt; paying companies to adopt these lower encryption standards; weakening the Secure Socket Layer (SSL) protocol to make it accessible for the government; stealing encryption keys

mainly from the mid-1990s, when technological advancements troubled security agencies and threatened to curtail their surveillance capabilities. For instance, The 1994 Communications Assistance for Law Enforcement Act (CALEA) aimed to address the development of digital phone switches and required telecomm companies to build 'surveillance-friendly' infrastructures that would allow the government to be a 'salient participant' in phone conversations.

The *third* category of policies includes policy events from 1968 – 2017 that limit government information collection to promote privacy (N=16). There are two types of policies in this category. First are policies that restrict and oversight surveillance by security agencies. Examples include the 1968 Title III of the Omnibus Safe Streets and Crime Control Act[16] that limits wiretapping and creates oversight mechanisms for information collection by law enforcement agencies. The act was updated in 1986 by the Electronic Communicates Privacy Act (ECPA) to authorize wiretapping in new forms of communication – emails, cellular phones, computer transmissions of data, and voice and paging devices – and protect the privacy of affected individuals in these new methods of communications as well. A more recent example is the 2015 U.S. Freedom Act that restricts information collection by national security agencies for the first time in three decades. It limits bulk collection by intelligence agencies, requires transparency reports over national security wiretapping, and appoints an external technical adviser to judges who decide on surveillance requests. A second type of policies in this category protects privacy against security agencies practices on a sector-by-sector basis. The 1978 Financial Privacy Act protects the privacy of financial information and allows the collection of such information only through a subpoena or a formal written request reviewable in court. Additionally, the 1984 Cable Communications Policy Act protects the privacy of cable subscribers through consent and notification before the government can use personal information obtained by these companies. Ultimately, we could not find examples for a *fourth* category of policies that downgrade both security and privacy at the same time.[17] The following

from a cellular chip manufactures to make mobile calls easily intercepted; and installing software back doors in the Skype voice over IP (VoIP) program to intercept calls.

[16] Also known as 'The Wiretap Act'

[17] While some view recent and historical attempts of the federal government to break encryption of commercial products as measures that downgrade privacy as well as cyber-security at the same time, the rationale behind these types of policies is to achieve short-term security goals (Landau 2006). Therefore, these types of policies were classified as promoting security over privacy, in category #2, rather than downgrading both.

table 1 demonstrates the conceptual classification of laws and regulations as discussed:

	Enhancing Privacy	**Weakening Privacy**
Enhancing Security	Security & Privacy complements each other: *28 Cases* Cyber-security practices that strengthen the security of personal information systems and advance the right to privacy of associated data subjects.	Security overrides Privacy: *26 Cases* National Security / Law Enforcement / Cyber-security policies that increase the collection of personal information, weaken digital infrastructures for information collection purposes, or undermine privacy for cyber-security purposes.
Weakening Security	Privacy concerns potentially limit security efforts *16 Cases* Privacy practices that limit government information collection for security purposes and promote privacy at the expense of potential security risks that may arise from the lack of collected information.	Security & Privacy are downgraded No cases Hypothetically, these would be economic or other development interests that promote the deployment of insecure services or infrastructures in cyberspace.

Table 1: The conceptual mapping of policy events according to the relationships between security and privacy

3. SECURITY VIS-À-VIS PRIVACY OVER TIME

By considering federal laws and regulations over the course of fifty years, we learn that the relationships between security and privacy are a function of time and context. Certain time periods reflect different concerns of policymakers and lead to different trade-offs between security and privacy. We trace two types of conceptual relationships. For contradictory dynamics between security and privacy, we recognize

three distinct time periods with different policy trends. The analysis of complementary relationships, however, reveals a single trend of an overarching gap in the promotion of security and privacy across most of the private-sector.

3.1. Contradictory dynamics in security and privacy over time

The analysis of contradictory dynamics between security and privacy reveals the importance of studying these goals over time. In the first twenty years under study (1968 – 1989), policymakers mostly aimed to construct a compromise between security and privacy. In the 1990s and 2000s, however, security is advanced at the expense of privacy in two main ways: In the 1990s, policymakers advance security over privacy by altering new technological developments in order to make them 'surveillance friendly.' In the 2000s, most of the promotion of security over privacy takes place through the expansion of the government's legal authority to collect personal information. Recently, in the past four years, a third trend of mild limitations on information collection practices is emerging. Figure 1 below reflects these three trends in time.

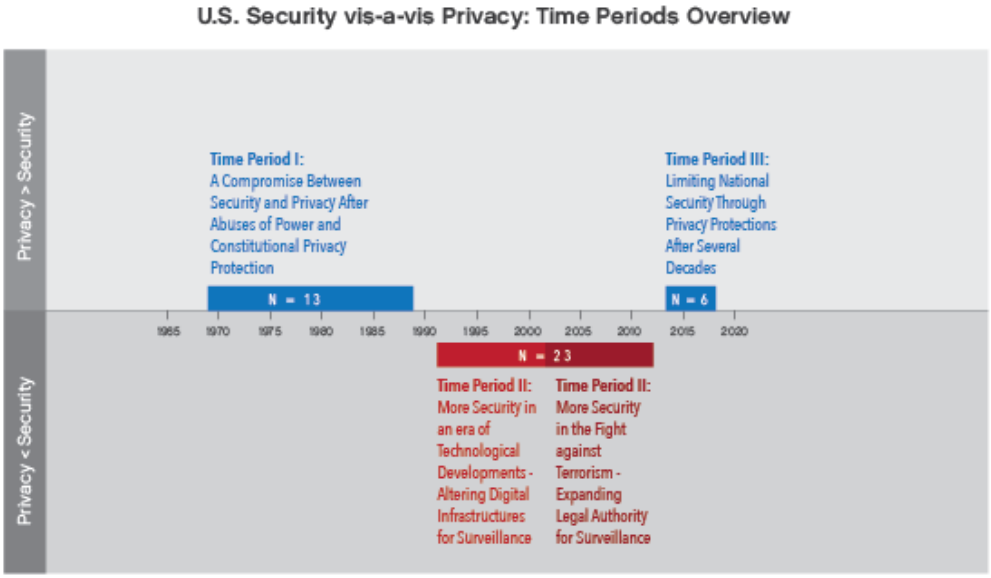

Figure 1: Security vs. Privacy policy trends in the Federal Arena over time

3.1.1. Time Period I [1968 – 1989, N = 13]

In the first time period, between 1968 and 1989, we identify 13 policy events which on balance reflect a compromise between security and privacy. The most significant ones are three federal legislations[18] and two executive orders[19] that significantly limit privacy violations by security agencies and increase Congressional scrutiny over security decisions. For example, the Foreign Intelligence Surveillance Act (FISA) of 1978 establishes procedures that approve and supervise information gathering by the intelligence community for national security purposes. The law creates a new judicial authority to decide upon surveillance requests within U.S. borders and requires routine transparency reports to Congress regarding the amount of authorized surveillance requests. Still, the law does not address information collection outside U.S. borders nor does it ask for a 'probable cause' or individual notification upon surveillance. The goal of the law was to prevent abuses of government power while preserving the ability to protect the nation against security threats (Church Committee 1976). Another compromise between security and privacy was enacted in 1986. The Electronic Communications Privacy Act (ECPA) amends the 1968 Wiretap Act and updates information collection procedures by law enforcement agencies. Policymakers agreed on the need to extend privacy protections to new forms of communication in order to prevent wiretapping of digital communication without a consent or court approval. At the same time, the law also advances security as new methods of communication can now be legally obtained. The act also expands the list of felonies for which a wiretap order may be issued and allows wiretapping of unspecified targets in certain cases. By contrast to this trend, we can also witness a dominance of security in a few cases. In 1981, President Raegan issued a significant privacy-intrusive order. Based on Executive Order 12333, security agencies can collect information outside U.S. borders without a court order or warrant required. Additional example for the dominance of security over privacy and attempts to conduct a compromise is the late 1980s debate over the authority to protect federal information systems. In 1984, Raegan's National Security Directive #145 authorized the National Security Agency (NSA) to become responsible for the security of federal networks. This authority was further extended through a memo from National

[18] The three significant legislative acts are the 1968 Wiretap Act (Title III) that limit law enforcement information collection, the 1978 Foreign Intelligence Surveillance Act (FISA) that limit national security information collection, and the 1986 Electronic Communications Privacy Act (ECPA) that updates the 1968 Wiretap Act to include new methods of communication.

[19] The orders were issued by Presidents Ford (1976) and Carter (1978) following surveillance scandals that revealed an abuse of government power in jeopardizing privacy for political reasons.

Security Adviser, John Poindexter, to expand NSA authority over 'all computer and communications security for the federal government and private industry.'[20] In response, Congress, industry, and civil society expressed concerns that a secret intelligence agency would enjoy the authority of oversight over U.S. federal and private information systems. Law makers passed the 1987 Computer Security Act to assign the civil agency of National Institute of Standards and Technology (NIST) responsibility over the security of federal networks. In 1989, however, NIST and the NSA signed a Memorandum of Understanding that places the NSA in all critical decision making processes over computer security issues in federal networks.

During the first time period (1968 – 1989) a regulatory framework through which security agencies can collect information was firstly established. This status-quo maintained until 1993. Between 1988 and 1993 the tension between security and privacy was less on the agenda. With the emergence of digital databases, policymakers were focused on regulating the ability of government agencies to build personal profiles of citizens for efficiency purposes.[21] The conflict between security and privacy was back on the agenda in the beginning of the 1990s, when law enforcement agencies became worried about the emerging ability of individuals to encrypt information and the development of digital telephone switches. Both technological developments had posed serious constrains on the surveillance capabilities of the government.

3.1.2. Time Period II [1993 – 2012, N = 23]

Debates over surveillance and technology embarked the second major time period between the years of 1993 to 2012. During this period, the number of policy events increases to 23 and we can see a clear dominance of security over privacy. In the 1990s we witness security policies that aim to alter technological infrastructures for surveillance purposes. In the 2000s, security policies mainly extend the legal authority of the government to collect information with lax privacy protections.

[20] National Telecommunications and Information Systems Security Policy (NTISSP) Memo No. 2: "Policy for the Protection of Sensitive, but Unclassified information in Federal Government Telecommunications and Automated Systems"

[21] By that time, federal government agencies had 910 major databases containing personal data (Diffie and Landau 2007). In 1988, Congress passed the Computer Matching and Privacy Protection Act in order to safeguard privacy in the light of matching practices between different government data bases and building profiles of individual citizens.

The 1990s started with the debate over the commercial usage of public-key encryption. In 1993, the U.S. government decided to fight the widespread use of privacy-enhancing encryption through export controls and the spreading of its own encryption standard in U.S.-based products. The government plan was to install a 'clipper chip' in every telephone product[22] in order to allow for a built-in ability to decrypt information. Despite strong opposition from the industry and civil society, NIST ordered that the government's encryption protocol would become a federal standard. AT&T started to develop appropriate models, but by 1995 it was clear that the Clipper Chip is not popular. Following public controversy over the program, Congress ordered an independent study on encryption. The National Research Council conducted the study and reached the conclusion that widespread use of strong cryptography is in line with the security and privacy interests of the country. Seven years after the announcement of the Clipper Chip program, the export regulations were changed and barriers to cryptography exportation were removed. In 2000, the U.S. government acknowledged defeat in its efforts to directly control the spread of cryptography for security purposes. Another government battleground for security over privacy was the commercial usage of digital telephone switches. After a series of attempts by the head of the FBI, Freeh, to allow the FBI the authority to design new commercial telephone switches, Congress passed the 1994 Communications Assistance for Law Enforcement Act (CALEA). The legislation ordered all new telecom equipment providers to produce 'surveillance-friendly' infrastructures through which the government would be a salient participant in personal calls to gather information. This was an unprecedented attempt of the government to disrupt systems' design for surveillance purposes. Despite FBI's desires, the law gave the industry the mandate to create the standards and required a transparent implementation process. The law was further extended in 2006 by the Federal Communications Commission (FCC) to include Voice over IP (VoIP) calls as well. At the same time, government's attempts in the 1990s to extend legal authority over information collection were blocked by Congress. In 1995, following the bombing of the Murrah Federal Office Building in Oklahoma City, the head of the FBI, Freeh, proposed new legislation that

[22] The NSA tried to make NIST dictate this vulnerable encryption standard on all telecommunications instead of only 'telephone communications' and failed after NIST opposition.

would permit law enforcement agents to obtain roving wiretap permission[23] without having to get individual court order for every tap. The White House further suggested expanding the list of crimes that can require wiretapping according to the Wiretap Act to any federal felony. They also wanted the legal ability to use illegally obtained information in courts, obtain long-distance telephone billing without a court order, and provide full funding for CALEA. Congress turned down all suggestions, but accepted funding for CALEA. Another example of a failed attempt to extend legal authority for surveillance took place after the TWA flight explosion in 1996. President Clinton offered that terrorist actions would be included among the list of crimes under the law enforcement Wiretap Act. Clinton also recommended more liberal provisions for roving wiretaps, 48-hour emergency warrantless wiretapping, and the profiling of airline passengers through electronic records. All these proposals did not pass Congress. The policy climate in the 1990s was not ready (yet) to expand the legal authority of the government over personal information of citizens, beyond 'adjustments' to the changing nature of communication technologies

In the 2000s, and especially following the 9/11 terrorist attacks, the U.S. government moved to changing the legal surveillance status-quo of the 1980s in favor of security over privacy. Within a few weeks from the attacks, and without a significant public scrutiny, Congress passed the Patriot Act for a 'systematic sector-by-sector reduction of privacy' (Regan 2004). The act passed in a tensed and highly fearful atmosphere from security threats which led citizens to accept greater constrains on their liberties. Practically, the act served as a 'shopping list' for the Department of Justice and allowed the collection of any 'tangible data objects' that might be loosely connected to a specific surveillance target. Expansions of security powers in the act also include extending the list of crimes that can trigger a wiretap order, authorizing law enforcement to share information with national security agents, mandating emergency disclosure of private communication by Internet Service Providers (ISPs), loosening the barriers the for pen-register and trap and trace installments, allowing FISA wiretaps to be roving in case the target changes phones,[24] extending authorized

[23] Roving wiretap takes place when a surveillance target changes communication devices and agents want to maintain their authority and capability to tap the target's communications despite the changing types of devices.

[24] The amount of FISA wiretaps' requests is generally increasing over time with a slight decline in the past seven years. From averaging 500 orders per year from 1979 – 1995, to averaging 868 order requests from 1996 – 2001, averaging 1,918 order requests from 2002 – 2008, to averaging 1,575 order requests from 2009 – 2016. The vast majority (more than 90%) of requests orders are approved by FISA courts.

surveillance on non-U.S. citizens to ninety days, adding more types of information that could be obtained through subpoenas, amending the Wiretap Act to apply on cable operators of Internet and telephone, eliminating civil liability for carriers complying with FISA or an emergency order, and allowing warrantless surveillance on computer trespassers. The expansion of authority to conduct government surveillance took place away from Congress oversight as well. In 2001, The Bush Administration believed that FISA does not cover all legitimate cases for surveillance. The President was unsatisfied with the current privacy barriers on the intelligence community and decided to secretly launch the President's Surveillance Programs (PSP). These were unlawful surveillance programs, operated by the NSA, without the scrutiny of Congress, that allowed warrantless surveillance between targets abroad and when they communicate to the United States. The President re-authorized these programs secretly, on a yearly basis, based on his own judgement. The existence of these programs was leaked to the New York Times in 2005. This caused a major public outcry,[25] and in light of these revelations, Congress decided to revisit FISA[26] in 2007 through the Protect America Act (PAA). This was an attempt to amend FISA in a way that would legally authorize the unlawful surveillance programs. The act excludes from the protection of FISA any warrantless surveillance of international communications if the foreign target is outside U.S. borders, even if it was an American citizen. Practically, the act removed the FISA warrant requirement from any national security surveillance which was taking place over a target overseas. The act was sharply criticized since it gave the government too much authority to target international communications of American citizens. In 2008, Congress revised FISA again through the FISA Amendments Act (FAA) and changes in Section 702 of the original act. The FAA sets different rules for international communications based on whether the target of surveillance was a 'United States Person'[27] or a 'Non-U.S.

[25] After the program was leaked to the New York Times, a judge in 2006 ruled that the program is a violation of FISA and the constitution.

[26] Throughout the second time period (1993 – 2012), the number of FISA wiretaps requests by the government has significantly increased. From 1979 to 1995 the average of wiretap requests was 500. From 1996 – 2001 the average was already 868. The peak was between 2002 – 2008 when the average reached 1,918 surveillance requests. From 2009 – 2012 the average was lowered to 1,639. Almost all surveillance requests (99%) were approved by FISA courts. The number of emergency warrants[26] also increased – in 2002, 170 of them were used. This was three times more than the total number in the previous 23 years of FISA.

[27] This category includes American citizens and non-citizens who are legal permanent residents.

Person.' According to FAA, if the target is a U.S. person who is outside the United States, the surveillance has to satisfy the traditional requirements of FISA. Thus, a FISA court order based on a probable cause that the target is an agent of a foreign power has to be applied. On the other hand, if the target is a non-U.S. person who is reasonably believed to be outside U.S. borders, section 702 of the FAA provides that the government need no probable cause or a warrant to conduct surveillance, even if the wiretapping takes place within U.S. borders. Section 702 also applies minimizations procedures on the collected information. Minimization procedures should apply to ensure that the privacy of U.S. persons is not violated. The Attorney General and Director of National Intelligence (DNI) should review these procedures and make sure they satisfy all requirements. Over time, FISA Court judges were exposed to the NSA's difficulty to apply minimizations procedures under section 702, especially for the 'upstream' program that collects internet communications through the Internet's backbone. They concluded that the act basically allows mass collection of global communications data in ways that minimizations procedures cannot fully apply. Incidental collection on U.S. citizens became a norm in the surveillance practices of intelligence agencies. On top of providing vast authorities to collect global communications, FAA also immunes telecommunications companies from civil liabilities when they co-operate with the surveillance efforts of the government.

An outlier in this time period was the successful industry opposition in 2002 against the attempts of the government to move the civic Computer Security Division (CSD) of NIST to the newly established Department of Homeland Security. Instead of placing the division under political settings that are more aligned with law enforcement rather than commerce concerns, the successful opposition allows computer security standards to continue and develop in somewhat distance from government power..

3.1.2. Time Period III [2013 – 2017, N = 6]

After twenty years of dominance of security over privacy, the third time period, between the years of 2013 – 2017, with its six policy events, reveals an emerging trend of privacy limitations on security practices. The period started with the revelations by whistleblower Edward Snowden on U.S. government surveillance practices. The disclosures led to a significant public outcry and facilitated the

formation of unlikely coalitions in Congress aiming to promote privacy. While a clear policy trend in the past four years does not stand out, we do witness an emerging set of privacy protections at the expense of security for the first time in several decades. In 2014, the President ordered the Presidential Policy Directive #28 that requires intelligence agencies to publicly state their exact uses of information collected in bulk. In addition, the order applies privacy protections on data collected on foreigners. Still, the limitations to bulk collection are mainly on information usages for non-security purposes, and the extent of privacy protections on foreigners is not clear. The order also creates new positions for privacy officials across the U.S. government in order to supervise information collection and calls for minimization procedures on gathered data. Yet again, these minimizations are subject to the 1981 Executive Order #12333 that provides vague limitations for what can be collected by security agencies. This pro-privacy trend continued in 2015, when Congress passed the U.S. Freedom Act, limiting privacy violations by security agencies through legislation for the first time since 1986. The law replaces the privacy-intrusive section 215 of the Patriot Act that allowed the collection of any 'tangible thing' and ends the mass collection of phone records (meta-data) by intelligence agencies. It also limits the routine use of emergency tools for surveillance by the FBI. It requires security agencies to be specific as possible when issuing emergency orders for surveillance. The act also orders the appointment of an external public-interest advocate, with technical background, to the secret Foreign Intelligence Surveillance Courts. The act orders these courts to publicly disclose authorized but controversial surveillance decisions. While the Freedom Act advances privacy at the expense of security, it does so for only certain information collection procedures, and it is far from a comprehensive reform on U.S. government surveillance practices. Recently, in 2017, additional regulation was published by the Director of Intelligence's (DNI) to restrict Central Intelligence Agency (CIA) information collection of publicly available information. Such a restriction is the first time since 1981 that the CIA is officially limited to collect information. In contrast to this pro-privacy trend, the Director of National Intelligence (DNI) also published 2017 guidelines for NSA's information sharing. These guidelines advance security at the expense of privacy as they allow law enforcement agencies to use information collected by the NSA with lax privacy protections. These data is gathered by the NSA according to executive order 12333, without a warrant or a court order. With these guidelines, the DNI further erodes the

border between law enforcement and national security activities and allow information that was collected with lax barriers to be used domestically against Americans.

Figure 2 below summarizes the main policy events discussed above that construct the dynamics between security and privacy over the three time periods. The length of the lines has no comparative meaning, but only allows each policy event to be presented in a readable manner.

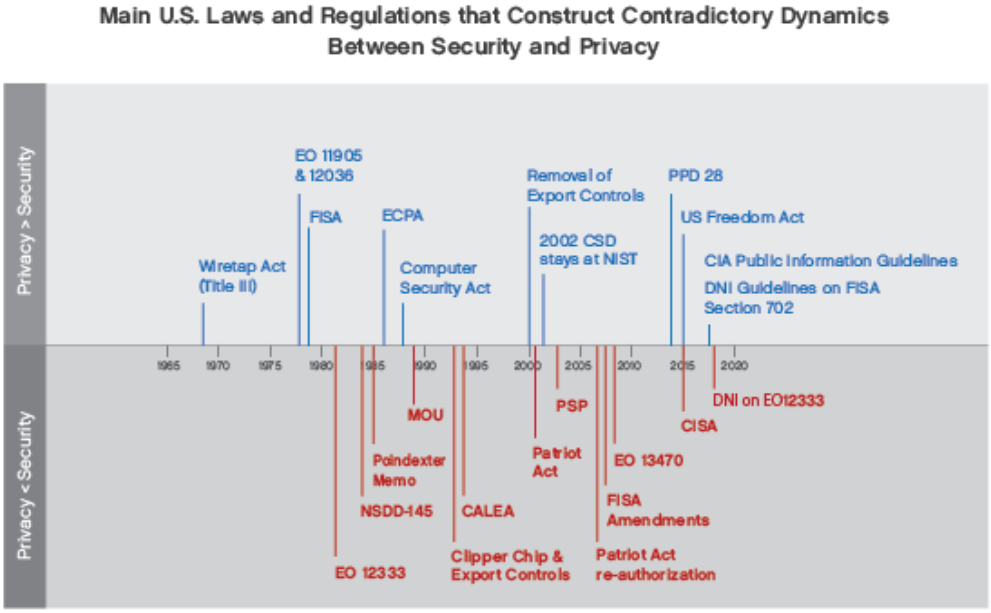

Figure 2: Main policy events at the U.S. federal arena that reflect a tradeoff between security and privacy

3.2. Complementary dynamics of security and privacy over time

When inspecting complementary dynamics we can witness significant policy efforts to increase security and privacy in federal networks, but gaps in doing so for other sectors, especially in those that might curtail the ability of the government and private-sector companies to collect personal information.

Initially, the cyber-security problem was framed as a 'computer security problem' and occupied U.S. policymakers already in the 1960s.[28] Over the decades since, the landscape of evolving threats as well as the conflict between national security and commercial interests both shaped federal policymaking that promote security and privacy at the same time (Warner 2015). We witness how policy efforts to ensure security and privacy are fragmented - in the private-sector, beyond health and financial services, mandatory government regulation is barely present. In addition, 'non-critical' sectors are only addressed through declarative policy-making and their protection is mainly based on self-regulation models. Figure 3 below demonstrates the lack of federal government efforts to pose mandatory requirements to increase security and privacy in the business and communications sectors. Almost half of the regulatory efforts are channelled to federal government networks.

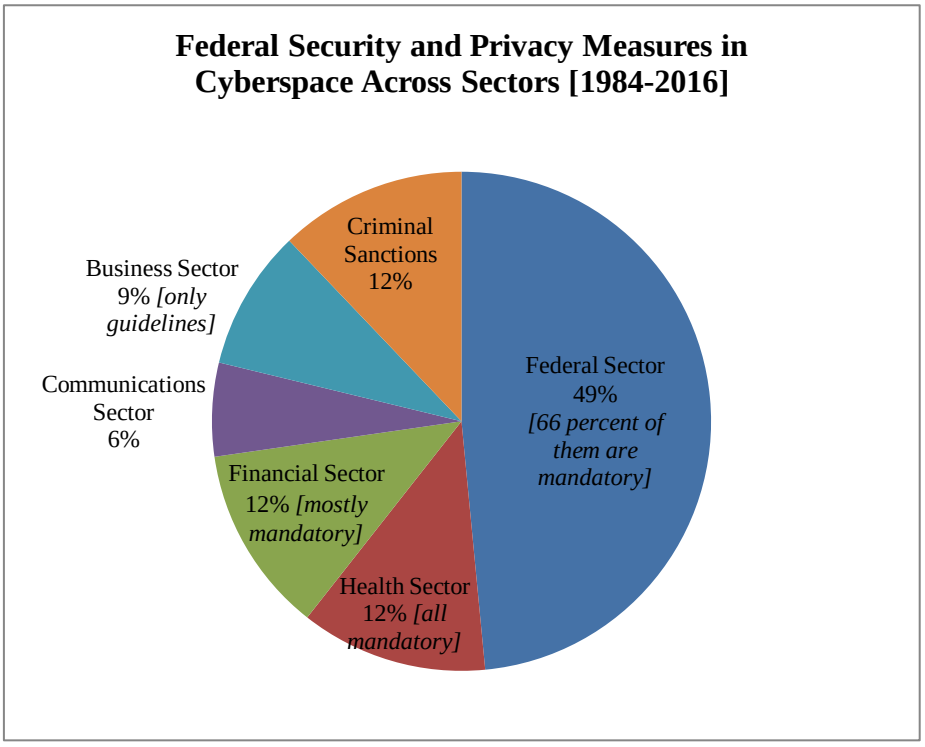

Figure 3: Mandatory and Voluntary Security and Privacy Measures Across Sectors [1984-2016]

[28] The 1965 Brooks Act addressed the way the federal government purchase information systems and assign the civilian agency NIST responsibilities for ensuring efficiency, security, and privacy of federal computer systems (Warner 2015).

This trend is not surprising when considering the government's agenda from the very early days of digital databases (1970s) and the development of the Internet (1990s). Policy decisions back then left the private-sector unregulated and determined a policy course of lax protections on the private-sector that is still in place. The 1974 Privacy Act was enacted by Congress after long debates over the importance of protecting private information from federal authorities. During the policy debates, the private industry argued that there was little concrete evidence of abuses in the information practices by private businesses. They claimed that they were already overburdened by government regulation and the proposed regulation was unnecessary and costly (Regan 1995, p.78). Their strategy was to urge companies to enact voluntary protections for personal information in order to lessen the pressure for government regulation. The private sector also opposed establishing a federal agency to oversee information collection and use. A more rigorous Senate bill that included the creation of a privacy protection commission and suggested tighter restrictions on personal information was rejected in favour of a weaker House bill (Regan 1995).

This trend has continued in the mid-1990s, when the federal government responded to the growth of the Internet by regulating the information security and privacy of specific private networks. In 1997, The Clinton Administration published The 'Framework for Global Electronic Commerce' (Clinton and Gore 1997) which described online businesses as essential to the growing online economy. The Administration did not want to limit businesses' expansion by posting costly and mandatory regulations over their operations. The framework called for applying self-regulation models over privacy protections, leaving privacy decisions to the judgement of commercial companies. This practically mandated the private sector to self-set the standards of privacy protections. It allowed the business practice of the commodification of personal information to thrive, and led to extensive private sector surveillance for economic purposes we witness today.[29] In the year of 2000, this policy trend of exempting the private-sector from regulations continued. In the first-ever U.S. cyber-security strategy, the Administration acknowledged the importance of protecting critical infrastructures, but still, did not want to push the private sector to costly regulations. The strategy states that "*while the President and Congress can*

[29] by information monopolies like Google and Facebook

order federal networks to be secured, they cannot and should not dictate solutions for the private sector systems."[30]

Despite this 'hands-off' approach, Congress did aim to ensure security and privacy over selective sectors. It ended up passing legislation solely on the health and financial sectors. Health records were recognized as critical and the 1996 Health Insurance Portability and Accountability Act (HIPAA) was the first time that information security standards were codified into law. After long debates and expressed concerns of private companies over the cost and complexity of the regulation, the act became a binding federal rule in 2003. Policy-makers have also posed requirements on the financial sector through the 1999 Gramm-Leach-Bliley Act (GLBA). An additional indirect boost to security and privacy in the financial sector was the 2002 Sarbanes-Oxley Act (SOX). The Act was introduced following the collapse of Enron and WorldCom in order to restore public trust in US corporations. The legislation changed the way publicly traded companies manage their audit, financial reporting, and internal controls. While information security is not specifically mentioned in the Act, reviews of companies' controls include information security standards that according to the Act have to follow strict restrictions.

In 2010, after a decade of federal laws and regulations that mainly dealt with the protection of federal networks and critical infrastructures, the regulatory agenda was shifted back to regulating the private sector. But instead of changing the 40-year trend towards mandatory and strict requirements, the Department of Commerce posed no mandatory security and privacy requirements on private companies. Instead, the Department published a strategy document[31] to address the privacy and security problems of 'non-critical' sectors. Specifically, the strategy recommends the adoption of the Federal Information Processing Standard (FIPS) – a privacy standard that was enacted in 1974 by the Privacy Act. The Department of Commerce also suggests that after a decade of failed attempts and opposition from the private-sector, the government should pass federal breach notification rules.[32] The strategy further calls

[30] B. Clinton, "Defending America's Cyberspace: National Plan for Information Systems Protection", Jan. 2000

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

[32] These are rules that require companies to report and face financial consequences in case of a data breach. Currently, the U.S. has 47 versions of breach notification laws across its states and was unable to pass a unified federal legislation despite many

for the establishment of a privacy oversight office under the Department of Commerce. A similar policy suggestion on the oversight of the privacy of federal networks through a dedicated office was made in the 1970s, but has been unable to get on the agenda since. Despite these efforts, the cyber security and privacy of businesses remained almost completely a product of self-interest and judgement, bounded only to what is considered 'fair trade practices' that could be enforced by the Federal Trade Commission (FTC).

Since 2013, however, we have seen a few significant steps at the agencies level to ensure private sector security and privacy. The Federal Communications Commission (FCC) is increasing its role as a privacy and security regulator in cyberspace. The agency published a strategy document[33] with voluntary recommendations to communication providers on how to mitigate cyber security risks and comply with the National Institute for Standards and Technology (NIST) network security framework. Additionally, the 3rd U.S. Circuit Court of Appeals in Philadelphia had recently taken a significant stand on the authority of the Federal Trade Commission (FTC) to enforce cyber security protections in the private sector (FTC vs. Wyndham Worldwide Corporation 2015). Previously, the FTC had relied on the reasonableness of companies' security practices and enforced regulation based on unfair business practices.[34] Following this ruling, the FTC has a new mandate and institutional power to enforce cyber security and privacy protections. This trend of agencies getting more involved continued in 2016, with the FCC moving from recommendations to actions. It published a new rule that requires Internet Service Providers (ISPs) to protect their consumers against information collection practices and require full transparency in personal information processing. However, with the recent change in the U.S. Administration and the appointment of a new FCC Chair by President Trump, these mandatory privacy guidelines have already been partially reversed.[35]

---

attempts in the last 15 years. There is controversy over issues like – federal preemption, desired policy goals, scope of notification, and effectiveness of policy.

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

[34] These enforcement powers were authorized by section 5 of the 1914 FTC Act

[35] The new FCC chairman, Ajit Pai, blocked FCC requirements from ISPs to apply common sense security practices to protect personal information.

Figure 4 below presents security and privacy protections across sectors over time. For each year, the cumulative amount of mandatory laws and regulations regarding the federal, health, financial, and other private-sectors is presented. We can notice how the protection of federal rather than private sectors has been dominating the agenda. Moreover, private-sector measures mostly protect the health and financial sectors (80%) and the vast amount of mandatory efforts (92%) address only these three sectors.

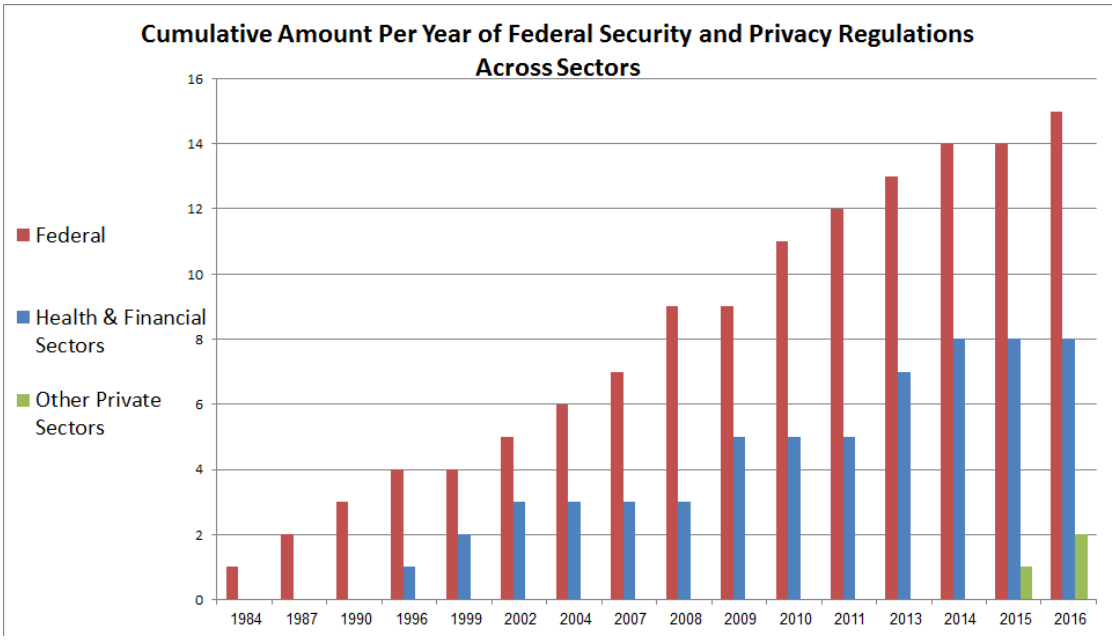

Figure 4: Cumulative Presentation of all Complementary Measures to Advance Security and Privacy across Sectors

4. SECURITY VIS-À-VIS PRIVACY ACROSS ISSUES

The relationships between security and privacy considerably vary across the issue domains of law enforcement, national security, and cyber-security. Each policy arena embodies a peculiar decision making mechanism that produces different levels of importance to security and privacy: (1) Law Enforcement policies are mostly driven by changes in technology, allow an open multi-stakeholder process, and aim to construct a compromise between security and privacy; (2) The National Security policy arena reflects secret and concentrated decision-making processes that advance security at the expense of privacy; and (3) the Cyber-security arena embodies a

conflict between commercial and national security interests that prevent the promotion of security and privacy across cyberspace sectors.

Figure 5 below summarizes the security and privacy relationships as they are dictated across the three policy arenas.

Figure 5: Security and Privacy Dynamics across Policy Arenas

4.1. Law Enforcement [N = 13]

The purpose of law enforcement is to domestically prevent, interdict, and investigate crimes to prosecute criminals. Over time, this policy arena experienced two major changes. First, the increasing use of technology has changed the role of law enforcement agents. Police work was once related to community expertise and field work and is now inherently connected to technology and wiretapping capabilities (Diffie and Landau 2007, chapter 5). The policy efforts of senior FBI officials in Congress usually follow technological developments that question the surveillance capabilities of law enforcement agents. Outcomes from these policy debates shape the

amount of privacy provided by newly emerging technologies.[36] Second, the distinction between domestic law enforcement practices and foreign national security practices has been blurred by various Administrations and legislative acts over the years. Since the oversight over national security surveillance is much more lax, this erosion means the establishment of new privacy-intrusive surveillance paths for law enforcement agencies.[37] This erosion took place mainly after 9/11 and has blended law enforcement and national security policies ever since.

Overall, we find that policies are shaped through a multi-stakeholders process. A typical policy processes follows a certain advancement in technology with the purpose of adapting law enforcement capabilities to new methods of communication. Policies are publicly debated through Congress with all stakeholders involved.[38] This political pattern provides a voice for all relevant policy actors - civil society, private businesses, and government agencies - to agree on policies that mostly construct a compromise between security and privacy. Within this policy arena, the interests of civil society and private businesses usually converge. They both attempt to promote privacy and limit information collection by the government. At the same time, we witness failed attempts by law enforcement agents to increase their legal authority over collecting information in ways that do not involve a technological change.

A good example is the 1986 Electronic Communications Privacy Act (ECPA). This is a legislation that updates the 1968 Title III Wiretap Act in order to apply wiretapping on newly emerged digital communications. The Department of Justice (DOJ), the telecom industry, Members of Congress, and civil society were able to agree on a bill that constructs a compromise between law enforcement needs to legally wiretap new communications and the goal of protecting privacy of digital and wireless phones. The bill was passed after two years of discussions and with a consensus from all stakeholders on its importance. Initially, the DOJ was reluctant to support changes in

[36] Two examples from previous sections in this paper: the debates over encryption and the commercial use of digital communications switches.

[37] In 1976, the Church Committee stressed the importance of distinguishing between national security and criminal investigations. The Committee revealed repeated practices of domestic political surveillance in the name of national security, and laid the foundations of the FISA act, to separately authorize surveillance for national security rather than law enforcement. FISA, however, allowed intelligence officers to inform criminal investigators in cases where they identify that a federal crime had been or is about to take place. In 1995, Attorney General Reno set the guidelines for maintaining a 'wall' between law enforcement and national security procedures, but after the 9/11 terrorist attacks, new guidelines were in place and intelligence and law enforcement agencies were eager to share information in order to uncover potential plots.

[38] The FBI Law Enforcement Agency, the industry that produces technological products that will be affected, Civil Society that usually aim to protect privacy amid technological changes, and Members of Congress that try to decide on the public interest

the 'well-understood' Wiretap Act of 1968. Nonetheless, in the hearings in front of the Judiciary committee, the DOJ was ready to negotiate and discussed the conditions with Industry and Congress (Regan Chapter…). Following the Bell System breakup of 1982,[39] businesses were eager to ensure the privacy of their consumers in a new market structure of several regional carriers. They aligned with the American Civil Liberties Union (ACLU) and advocated for privacy restrictions on law enforcement wiretapping (Regan Chapter…).

Another example is the 1994 Communication Assistance for Law Enforcement Act (CALEA). Unlike the 1986 ECPA, CALEA was surrounded with much more controversy as it required a technological change of telecomm operators to design their infrastructures in a way that would allow the government to be a salient participant in every phone call. Initial attempts by the FBI to pass such bill in 1992 had failed, but eventually Congress was able to pass the bill as a compromise between the interests of the FBI, civil liberties organizations, and business groups. Congress wanted to avoid a potential gap in surveillance capabilities, but did not want technology to be fully developed according to surveillance needs (Regan Chapter…). Telecomm carriers were less eager to support the bill, but were compensated with $500 million for potential costs and were mandated by Congress to take the decisions over the new standards in their infrastructures. Eventually, these standards were less privacy-intrusive than what the FBI had wanted. Civil liberties groups had also accepted the bill after recognizing the difficulty of law enforcement agencies to collect information in a new technological environment (Regan Chapter …). They were claiming that law enforcement has a legitimate need and had to work hard to keep up with all the technological changes of that time. Still, Congress decided on a transparent implementation process to ensure public scrutiny. Beyond these examples of adapting surveillance to new technologies, law enforcement agencies also attempted to extend their legal authority over private information following security crises in 1995 and 1996. These attempts, which were discussed in detail in the previous section,[40] were not approved by Congress.

[39] This was an anti-trust decision that effectively took the Bell System monopoly and split it into entirely separated companies. AT&T would continue to provide long-distance service, while a new Regional Bell Operating Companies would provide local service no longer directly supplied by AT&T subsidiary company Western Electric.

[40] This was discussed in section 3.2. about Time Period II (1993-2012)- we have described policy attempts to increase the legal basis for law enforcement agencies following the 1995 terrorist act in Oklahoma, and the suspicion over terrorism after the 1996 TWA flight explosion

4.1. National Security [N = 28]

The notion of 'national security' is relatively new in American politics and can be traced to the early post World War II period. The main purpose of 'National Security' is to protect the country against foreign attacks. Therefore, the main mission of a national security agency is to collect foreign intelligence (Diffie and Landau 2007, chapter 4). Historically, this policy arena has been vulnerable to abuses of power. Courts and Congress have traditionally given the President a broad leeway to obtain foreign intelligence. National security wiretapping faces lax constrains on information collection. The FISA Act for instance, is much less stringent than the law enforcement Wiretap Act.[41] The more lax requirements seemed appropriate since foreign intelligence warrants are primarily for information collection rather than criminal prosecution (Diffie and Landau). These soft requirements are an attractive source for power abuse, and were abused repeatedly by U.S. Presidents such as Kennedy, Johnson, and Nixon (Diffie and Landau 2007, p. 195). In 1972, the Supreme Court even ordered to end warrantless domestic wiretapping for 'national security' purposes. The court argued that *'Fourth Amendment freedoms cannot by properly guaranteed if domestic security surveillance is solely conducted with the discretion of the Executive branch'* (US vs. US district court). It is only after major privacy crises and public scandals that a shift towards more privacy and less security is taking place in this arena. Usually, however, these pro-privacy shifts are limited, and the next security crisis reserves and even strengthens the policy pattern of security over privacy.

This policy arena reveals a concentrated decision-making process dominated by President and the Executive. Congress provides very little scrutiny and oversight over national security decisions. Most policy actions and debates are secret – they take place behind closed doors or through the classified FISA courts. Developments in technology have significantly boosted the capabilities of national security agencies to violate privacy. They allowed security agencies to practice mass instead of targeted surveillance and increased secrecy even further. National security agents have been constantly using misleading language about the actual meaning of surveillance requests. In addition, mass surveillance authorizations usually enter the agenda

[41] In FISA it is stated simply that there should be a probable cause only to believe that the individual is an agent of foreign power. Also, notice to surveillance targets in FISA is given after the fact and surveillance can go for months without a notice.

temporarily but soon become permanent. Private businesses are significant actors in the government's surveillance efforts as wll. They are either secretly cooperating with the government or hacked by the government in order to open more avenues for information collection of private communications. Overall, the Executive dominates the policy agenda and aggressively, often secretly, pushes for national security practices at the expense of privacy.

An example for this decision-making mechanism is the 1981 Executive Order 12333. It was issued by President Regan, without going through Congress, to allow government information collection outside U.S. borders. The order was an exceptional to the political climate at that time. The 1976 Church Committee exposed scandals and illegitimate use of government power in collecting information about citizens in the name of national security.[42] Henceforth, intelligence agencies were limited in their wiretapping practices within U.S. borders through the 1978 FISA act. President Reagan passed EO 12333 in response to the undermined capabilities of the intelligence agencies. Unlike other wiretapping orders, EO 12333 allows the collection of the content of communications and applies vague self-regulatory mechanisms for privacy violations within the intelligence community. Another example for the aggressive promotion of security in this domain is the 2001 – 2007 President's Surveillance Programs (PSP). Post 9/11, the president was eager to remove legal barriers for information collection and had secretly authorized massive surveillance programs that expanded NSA's authority to conduct surveillance within U.S. borders without a court order. The Executive did not seek authorization from Congress to launch and operate these illegal programs. In fact, President Bush and his Attorney General justified this concentrated decision-making mechanism based on a 2001 legislation that passed one week after 9/11 and granted the president the authority to use all necessary force against those who were linked to the 9/11 terrorist attacks. The close relations between businesses and government over national security issues are demonstrated through government programs exposed by whistleblower Edward Snowden. In these revelations we can learn about secret cooperation between companies like Google and Yahoo and the NSA that allows government's access to the companies' infrastructures. Moreover, Snowden uncovered programs that work

[42] The 1976 Church Committee studied U.S. domestic surveillance practices and exposed an on-going practice of surveillance in the name of national security against socialist movements, political leaders, judges, and activists.

secretly, without the awareness of private manufactures, on making private infrastructures accessible for the government. This includes secretly installing back doors on Cisco routers or stealing cellular chips from a private company in order to make these networks accessible. Limitations of national security in the name of privacy are a few and arise only after major public outcries in the face of exposed government surveillance scandals. The 1978 FISA act was a product of the Church Committee work that exposed surveillance scandals through U.S. history. Similarly, Edward Snowden's revelations in 2013 uncovered enormous capabilities of power abuse by the National Security Agency and led to the passage of the 2015 U.S. Freedom Act, limiting national security for the first time after several decades.

4.3. Cyber-security [N = 35]

Cyber-security[43] is the third central policy arena that shapes the security and privacy dynamics. In contrast to the previous arenas, cyber-security policies mostly complement with the right to privacy since they increase the security of personal information. This policy arena brings together interests and actors that do not naturally 'sit together.' The main stakeholders are (1) Law enforcement agencies who aim to tackle cyber-crime; (2) The national security establishment – DHS, DoD, CIA, and NSA - that protects critical infrastructures and national security systems in cyberspace; and (3) Private companies, that are the majority of cyberspace actors, and work to maintain influence on computer security standards and promote minimal mandatory regulations. The arena is rife with agencies and reflects an on-going conflict between commercial and national security interests. The dominance of national-security interests is reflected by the authority granted to intelligence agencies over the cyber-security of federal and private sectors. Commercial interests usually oppose the influence of intelligence agencies, but prevent the policy agenda from assuring mandatory privacy and security protections on private sectors. The interplay of interests creates a policy arena in which security and privacy are loosely promoted.

[43] The word 'cyber' has acquired the meaning of 'through the use of a computer', and the term 'cyberspace' brings together all the communication networks, databases, and sources of information into a diverse sphere of electronic interchange. This sphere is not only virtual, but grounded in the physical reality of servers, computers, satellites, and telecom infrastructures (Dunn Cavelty 2010). The term cyber-security then, refers to making this digital environment safe through the confidentiality, integrity, and availability of the information.

It seems that the policymakers are reluctant to advance laws and regulations that might curtail government surveillance capabilities or hamper commercial interests.

Policies are developed according to changing landscape of threats and demonstrate the dominance of national security interests. Back in the 1960s, federal officials warned about the privacy and national security risks that arise from digitally stored information.[44] In 1965, Congress enacted the Brooks Act that gave NIST, under the Department of Commerce, the responsibility to set the standards and guidelines to ensure the security, privacy, and efficiency of federal systems. The tension with national security was evident already there, as the Act made an exception for certain CIA and DoD activities as long as they involve operational activities. By that, the Act made a significant differentiation between operational sensitive systems, supervised by the intelligence community, and administrative systems that should be guided under the authority of NIST and the Department of Commerce (Warner 2015). A 1976 report from the Senate Committee on Government Operations revealed how NIST is posing voluntary instead of mandatory requirements and warned that the civil agency has limited influence on computer security standards. The emergence of TCP/IP networking protocols paved the way for new threats to develop. In 1984 The Raegan Administration decided to completely perceive the threat to information systems as a national security threat. The 1984 National Security Directive (NSD) #145 added a third category to the Brook Act's differentiation of information systems and urged for the protection of 'unclassified but sensitive' data by the NSA. Members of Congress viewed this expansion as 'an increasing military influence on society.' They saw it as a threat to all sectors of economy and argued that values and goals like freedom of speech, economic trade, scientific innovation, and intellectual inquiry would be undermined from this new NSA authority (testimony quote). The American Civil Liberties Union warned that 'unleashing the NSA to patrol computers is dangerous since the NSA is operating outside normal accountability channels. Its existence was not acknowledged until 1962.'[45] In 1987, Congress responded and passed the Computer Security Act, that re-authorizes the civilian agency NIST, rather than the NSA, to be responsible for the security of federal networks. Congress did acknowledge though, that certain systems require NSA guidelines. In March 1989,

[44] In April 1967, Willis H. Ware wrote a RAND study about security and privacy in computer systems
[45] Jerry Berman, ACLU, testimony before Senate committee on Governmental Operations, 1976

however, NIST and the NSA had signed a Memorandum of Understanding (MOU) that is inconsistent with the Computer Security Act and creates a framework through which the NSA regains authority over unclassified government systems. The NSA upgraded its status from providing assistance as NIST saw fit to de-facto setting the rules for computer security. The memo injects secrecy to the policy process and requires that *'all matters regarding technical systems security must be reviewed, prior public discourse, to ensure that they are consistent with national security.'* The same pattern of national security influence happened in 2010. Following the enactment of the 2002 Federal Information Security Management Act (FISMA)[46] to increase enforcement powers over information security and require all agencies to comply with NIST standards, the NSA aimed to re-assure its influence. Through a 2010 Memorandum of Understanding between NIST and the NSA, the intelligence agency was able to regain its authority and be part of NIST computer security standards development. Just like in 1989, the NSA was able to be an essential part for any cyber-security decision taken by NIST. The threat landscape kept expanding as offensive capabilities were acknowledged, and the use of the Internet has increased. Congress recognized the revolution and passed the Clinger-Cohen Act of 1996. The Act had expanded the category of 'national security systems' to include all systems related to intelligence, cryptography, and military command and control. Following the 9/11 terrorist attacks, the dominance of security agencies in cyber-security had even further increased. The Homeland Security Department was established, and several orders that were secret at that time (NSPD #38 from 2004, The 2008 Comprehensive National Cybersecurity Initiative, and NSPD #54 from 2008, PPD #20 from 2012), authorized the use of offensive privacy-intrusive capabilities to increase cyber-security.

Despite the dominance of security agencies in this policy arena, commercial interests gained a few successes in the cyber-security arena, mainly in their attempts to influence computer security standards and avoid mandatory regulations. In section 3.2. we discussed three central policy events in which the private-sector was able to remain exempt from mandatory regulations: (1) The 1974 Privacy Act that was the first time Congress regulates information privacy in digital systems; (2) The 1997 Framework for Global Electronics Commerce which was the first White House

[46] Title III of the e-government act of 2002

strategy document with regards to the Internet economy; and (3) The 2000 first-ever national strategy for cyber-security. These policy documents had determined the tone for the lack of mandatory security and privacy protections in the private sector and worked in favor of commercial interests. Further, as discussed in section 3.1.2, commercial interests gained success in 2002 when the Computer Security Department of NIST did not become party of the newly established Homeland Security department. This allowed computer security standards to be developed with the influence of the private-sector. The 2000 removal of export regulations over encryption was also a victory for commercial companies. After years of policy debates with the government, commercial organizations were able to overcome government interests for control over exports of encrypted products. The dominance of commercial interests is also reflected in the repeated failures of Congress to pass a federal breach notification act. Currently, private-sector companies are operating according to 47 different versions of state breach notification laws. There is no unified requirement from companies to report on data breaches, and despite Congressional attempts to pass such an act since 2003, issues such as federal preemption, the scope of the notification, and the requirements from companies prevent the passage of a federal act that would increase security and privacy at the same time. In addition, a recent example for the dominance of commercial interests is the enactment of the 2015 Cyber Information Sharing Act (CISA). After a decade of stressing the importance of information sharing between the public and private sectors for cyber-security, Congress was able to pass a voluntary information sharing act after introducing liability waivers for companies that choose to share cyber threat information with the government. This has created an incentive for companies to share information with the government, without a court order, in a non-transparent approach, that might violate the privacy of the customers.

5 – CONCLUSION

We find that U.S. Federal decision-making over security and privacy in cyberspace is carried forward via a patchwork of laws and regulations in patterns that change over time and across three main issue domains. *First*, over time, there are two types of contextual relationships to follow: (1) Policies that construct contradictory dynamics

between security and privacy reflect three trends in time. In the 1970s and 1980s (N=13), following exposed government surveillance scandals and changes in technology, Congress was able to pass policies that mostly construct a compromise between security and privacy. Since the mid-1990s, with advancements in technology and the emerging threat of terrorism, the relationship has started to shift towards more security at the expense of privacy (N=23). The U.S. had either altered technological infrastructures for security purposes or expanded government authority to collect and process personal information through non-transparent practices. Recently, in the past four years and following the disclosures of surveillance scandals by Snowden, policies (N=6) mostly suggest mild limitations on national security for privacy purposes; (2) Policies that construct complementary dynamics between security and privacy reflect a single trend over time of mostly focusing on the federal, health, and financial sectors (75% of all policies). Most of the private-sector, however, is left to self-regulate, with no mandatory privacy or cyber-security requirements at the federal level. *Second*, the relationships between security and privacy also vary across the different political arenas of law enforcement, national security, and cyber-security. Each arena has its own peculiar decision-making mechanism that differently orchestrates security and privacy dynamics. Whereas law enforcement issues allow mostly open debates and multiple stakeholders to influence the policy process in a way that partially limit security for privacy, national security issues reflect a concentration of power and high levels of secrecy through which the government aggressively push for security at the expense of privacy. The cyber-security arena suggests a much less coherent trend. Policymaking is dominated by private businesses and security agencies that battle over influence and responsibility. The lack of interest by the government to regulate most of the private sector along with the dominance of security agencies in cyber-security decision-making processes creates an arena in which private-sector privacy and cyber-security are loosely promoted.

After five decades of public policies that shape security and privacy in the U.S federal arena, this paper reveals the policy trends and the political settings that design security and privacy decisions. The findings shed light on the importance of context in the promotion of security vis-à-vis privacy in the United States. The three trends in time are determined by the context of the time period and the need of a government response to privacy scandals, technological changes, and new security threats. The

findings also increase our understanding on the political settings by which security and privacy are discussed in the U.S. policy process. Relationships between security and privacy are determined not through one, but by three main policy arenas, with distinct actors and policy processes set the tone. The framing of a security and privacy issue as a law enforcement / national security / cyber-security issue dictates the actors and the decision making processes according to which security and privacy would be advanced. We show how instead of a strategic thinking by policymakers on the amount of power given to security agencies at the expense of citizens' privacy, the decision-making is mostly context-dependent. Despite the importance of security and privacy dynamics to the liberal nature of U.S. society, we find three policy arenas, mostly disconnected from one another, that advance security and privacy in varying degrees of transparency and sometimes without all stakeholders involved.

This paper allows for a nuanced understanding of the characteristics that shape security and privacy policies in the U.S. federal arena. At the same time, it also provides a comprehensive understanding of trends over time. We seek to understand how the U.S. trades security and privacy, and find that the answer is directly attached to the context of events as well as the political settings of the decision making process. With this mind-set of security and privacy context and politics, the next logical step would be to uncover the interests and actions of each political actor within a policy arena over time and reveal how these networks operate over a few policy issues.