Digital Transformation and Public Services

Societal Impacts in Sweden and Beyond

Edited by
Anthony Larsson and Robin Teigland

Routledge
Taylor & Francis Group
LONDON AND NEW YORK

First published 2020
by Routledge
2 Park Square, Milton Park, Abingdon, Oxon OX14 4RN

and by Routledge
52 Vanderbilt Avenue, New York, NY 10017

Routledge is an imprint of the Taylor & Francis Group, an informa business

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library

Library of Congress Cataloging-in-Publication Data
Names: Larsson, Anthony, editor. | Teigland, Robin, 1964– editor.
Title: Digital transformation and public services : societal impacts in Sweden and beyond / edited by Anthony Larsson and Robin Teigland.
Description: Abingdon, Oxon ; New York, NY : Routledge, 2020. | Includes bibliographical references and index.
Identifiers: LCCN 2019026170 | ISBN 9780367333430 (hardback) | ISBN 9780429319297 (ebook)
Subjects: LCSH: Public welfare—Sweden. | Human services—Technological innovations—Sweden. | Educational innovations—Sweden. | Medical care—Technological innovations—Sweden. | Public administration—Technological innovations—Sweden.
Classification: LCC HV338 .D55 2019 | DDC 361.609485—dc23
LC record available at https://lccn.loc.gov/2019026170

ISBN: 978-0-367-33343-0 (hbk)
ISBN: 978-0-429-31929-7 (ebk)

Typeset in Times New Roman
by Apex CoVantage, LLC

11 Citizen protection

A capabilities and intentions framework

Mark A. Conley and Emily Nakkawita

1 Introduction

Citizens evaluating domestic security might ponder two aspects of their trust in the government. First, does my government have the *capability* to protect me? Second, do I trust my government's *intention* to protect me? These assessments of a state's capacity and motivations are fundamental to citizen perceptions of internal security, with consequences for private responses. Due to wide-ranging, accelerating technological advancement, digital innovation has enabled effective and extensive private efforts with the potential to disrupt traditional governmental roles. Herein, we study how digitalization has affected historical citizen protection functions using a capabilities and intentions framework. This framework does not assume any baseline trust levels, and it is important to emphasize that we do not assume that citizens automatically trust their governments. We measure citizen trust with public opinion polls, and present this evidence alongside a time series analysis of other sources of public trust.

First, we broadly define citizen protections and summarize their historical origins in the United States and their recent evolution. We hypothesize that private government contractors – all with a major digital component that bolsters citizen security – signal increasing concern with threats, vigilance, and protection in the age of digitalization. However, during the same time period, public institutions charged with citizen protection have also pursued and exhibited these same concerns and intentions. After highlighting extensive public-private collaboration across a wide range of protective functions, we identify important considerations that this hybrid model raises in the coming years. This chapter addresses serious structural and moral issues inherent to large government efforts, but we avoid diverting into lengthy treatments on civic topics that merit entire library sections. We therefore balance tension between terseness and tedium in order to emphasize our argument that citizen protection roles have evolved recursively between public and private institutions in this age of digitalization.

1.1 Defining citizen protection

We define citizen protection as the work of institutions aimed at minimizing public harm and ensuring enumerated fundamental rights, including: inalienable

rights such as "life, liberty and security of person" (UN General Assembly, 1948); human rights to private property and self-defense (Barnett, 2004); and legal rights including a fair trial (The Constitution of the United States, Amendment VI). Due to its size and global influence, we focus this analysis on US public security institutions and the accompanying industrial complex; however, the interpretation and conclusions transcend national boundaries and government structures. These data describe how digitalization affects citizen protections and welfare both within and beyond *any* country's public security apparati.

Within the broad realm of citizen protection are three key distinctions that clarify the structure and function of organizations and their general missions.[1] We explore each dimension below.

1.1.1 International vs. intranational protection

Security requires parallel efforts – international and intranational protection – each with different sets of responsibilities and legal constraints. *Inter*national security encompasses protection from hostile foreign actors. In the United States, this duty belongs primarily to well-known public defense and intelligence organizations: the Department of Defense, the Central Intelligence Agency, and the National Security Agency. *Intra*national security efforts safeguard citizens from internal actors (i.e., other individuals within the state). Intranational security has primarily been led by public entities, including the police and courts, though in many parts of the United States, there remains a strong custom of self-protection via firearm ownership that is rooted in US history and values, including "culture of honor" norms and the primacy of rights to liberty (Cohen et al., 1996; Kocsis, 2015).

Guarding against both inter- and intranational threats is an evolving challenge in the digital age. In a digital world war, national boundaries are practically irrelevant to an enemy that plans attacks and recruits fighters worldwide (Ullah, 2017). Instead of focusing on the characteristics of these resilient and amorphous enemies, this chapter focuses on public and private efforts to guard against them.

1.1.2 Public vs. private protection

Traditionally, citizen protection efforts have fallen under the purview of local, state, and federal government entities. However, beyond the historic use of hired soldiers in armed conflicts (Avant, 2004), beginning in the early 20th century, governments began to collaborate with private entities in their efforts to promote citizen security for reasons ranging from financial efficiency to technological superiority (Markusen, 2003). Today, governments stand at a critical juncture where new technology is evolving at a rapid pace and financial incentives have changed, such that the consumer market for innovation has surpassed the public sector. As a result, governments are no longer the primary drivers of the innovation agenda (FitzGerald and Parziale, 2017). In this changing landscape, citizen protection efforts are distributed across a public–private continuum, and the lines between public and private efforts are blurring. This trend, rooted in the

development of digital technology, has augmented private entities' capabilities to play a larger – perhaps, even leading – role in citizen protection. Some defense scholars have suggested that private capabilities will continue to grow such that they eventually supersede the power and relevance of public structures (Leander, 2005; Minow, 2005; Singer, 2005, 2008). We explore those claims with data: markers for protective capabilities and intentions across both public and private institutions. We proceed to interpret those trends and speculate about the future of this public-private collaboration.

1.1.3 Direct vs. indirect protection

We focus on *direct* protection: citizen protections from physical threats that directly imperil rights to life and immediate "security of person" (UN General Assembly, 1948). This definition excludes many *indirect* protections, and in some cases, makes distinctions on certain security tactics depending on their ultimate aim. For example, this chapter's scope includes online surveillance by technology organizations who attempt to prevent imminent terrorist attacks, but excludes organizations who aim to protect citizens from hate speech on the Internet. Distinctions like these narrowed the list of public and private organizations we studied (see Section 2: "Methods").

1.2 Overview of citizen protection structures in the United States

The US government is a model hierarchical bureaucracy, consisting of delineated departments with complementary missions. Among 15 cabinet departments within the executive branch (agriculture, commerce, defense, education, energy, health and human services, homeland security, housing and urban development, interior, justice, labor, state, transportation, treasury, and veterans affairs), five departments pursue citizen protection as a primary mission: the Departments of Defense (DOD), Homeland Security (DHS), State (DOS), Justice (DOJ), and Energy (DOE).[2] In addition to these cabinet departments, we review the protective functions of intelligence agencies, the US judiciary branch (i.e., public courts), and local law enforcement. Appendix A briefly sketches out the histories, functions, and counterparts to these direct citizen protection structures.

1.3 Evolution of citizen protection in the United States

Although public entities have delivered protection to citizens since the country's founding, more recently, non-governmental actors have augmented the government's capabilities. Since the 1950s, public structures (see Appendix A) have been transformed by privatization, primarily resulting from expectations of cost efficiencies and greater technological prowess (which, in recent decades, has included digital technology). Despite the increased ability of private entities to engage in citizen protection, we propose that the acceptance of such an

arrangement depends on citizens' beliefs about public and private *capabilities* and *intentions*.

1.3.1 Evolution of international protection

In this section, we highlight growing privatization within various forms of international protection, including the nation's armed forces and intelligence efforts. In the United States, this privatization has generally taken the form of public-private partnerships. Although private companies play increasingly important protective roles, they typically work in close collaboration with public entities.

Military and diplomatic protection: international defense endeavors comprise a major portion of the US annual budget, chiefly via the DOD. Until recent decades, the most significant technological advances within citizen protection in the United States were driven by the public entities reviewed in Appendix A, whether directly (i.e., technologies developed within government agencies) or indirectly (i.e., through government-sponsored grants) (FitzGerald and Parziale, 2017). However, today private contractors play important and growing roles in international citizen protection, as evidenced by a US defense contractor workforce that had expanded to 3.7 million by 2015 (Light, 2017; Prem, 2018). The extent of this privatization is somewhat unique to citizen protection: Security-related agencies and departments, including the Departments of Defense and Energy, rely more heavily on outsourcing than other public entities (Markusen, 2003). In fact, a review of 1996 data revealed that, by this date, five contract and grant jobs existed for every DOD role, with a ratio of only 1.5-to-1 in areas of government not dedicated to citizen protection (Light, 1999). Similarly, the share of defense roles accounted for by private contractors grew to 50 percent in 2000 from 36 percent in 1972, whereas military and Pentagon (i.e., the US DOD Headquarters) civilian employees' share decreased from 64 percent to 50 percent during the same period (Markusen, 2003). There is much more privatization within the citizen protection sector.

Explanations for this shift to privatization are often rooted in claims about the greater efficiency and expertise of private entities; their operations are seen as more agile and less costly than similar efforts would be if managed publicly (Rosenberg, 2016; Markusen, 2003). Since the 1970s, the scope of work outsourced to contractors has grown, and these entities have responded to increasing calls for less "bloated" government by expanding their offerings to provide a wider range of services, from troop training to base maintenance (Abrahamsen and Williams, 2009; Markusen, 2003). This is a recursive process by which governments have a need, private organizations respond to that need by expanding their offerings, and government structures come to rely on those broadened skillsets. Over time, this partnership expanded from garrison services to combat operations.

However, cost efficiency is not the only driver of security privatization; digitalization and technological aspirations also play an important role in this process. As an example, consider the advancement of military capabilities: In the first half of the 20th century, thanks to the emergence of new technology (air warfare), the

US government looked to the private sector for the development of advanced aircraft (Markusen, 2003). Following private success in developing ballistic missiles in the 1950s, the Air Force's strategic reliance on private contractors prevailed over the Army's preference for public research and development (Kelsey, 1982). In the decades that followed, the majority of weapons development has been led by private entities contracted by government forces (Markusen, 2003). This trend is also reflected in the US nuclear program: Although a wide range of public entities both oversee the country's nuclear arsenal (e.g., the DOE) and work to prevent the spread of such technology (e.g., the Bureau of International Security and Nonproliferation) (Holgate, 2018), private contractors play a leading role in the development and production of these weapons. This public-private partnership enhances the government's effectiveness in maintaining a strong nuclear program, as these private entities' capabilities are superior to the public's (Cole and Vermeltfoort, 2018).

Beyond weapons technology, privatization within international citizen protection has also been driven by research and innovation more broadly. In their review of DOD commercial activities programs, Tighe et al. (1996) found that military research, development, testing, and evaluation (RDT&E) increasingly relies on the work of private entities; for example, the Navy outsourced only 30 percent of RDT&E activities in 1970, and by 1996, this share had grown to 50 percent. Public security reliance on private technology is even more evident when examining the financial growth of companies with government contracts, such as Computer Sciences Corporation, whose defense sales exceeded USD 1 billion by 1997 (Berteau, 1998); for a more modern perspective, Leidos's defense contracts exceeded USD 6.8 billion in 2016 (Washington Technology, 2017). Though some citizens have raised concerns about this privatization of international security, the outcry has not been loud enough to prompt any change (Leander, 2005).

Evidenced by little resistance to public-private partnerships, citizens appear to consider defense contractors trustworthy enough. Americans indicate positive feelings toward technology firms that are likely responsible for digitalization: 71 percent indicate that tech companies have a "positive effect on the way things are going in the country" (Doherty et al., 2015). Beyond the greater capabilities of these private organizations, this strong privatization trend may also reflect citizens' mistrust in the motivations of public entities. Public opinion studies have tracked American sentiments toward defense with polls depicting tenuous confidence in public protection. From 2002 to 2012, public opinion on defense spending showed a reliable trend of more people thinking that the United States spends too much and fewer people thinking that the United States spends too little (Corman et al., 2015). Other polls confirm waning trust in the US government; in 2015 only 19 percent of Americans reported trusting the government always or most of the time, as compared to a peak of 77 percent in 1964 (Doherty et al., 2015). These public-private hybrids thrive in times of waxing and waning government trust alike. Taken together, these two poll investigations indicate that trust in US government institutions has been generally lower than trust in its private defense industry and indicates taxpayer openness to joint public-private

protection efforts. Citizens generally do not deconstruct, it appears in these polls, which exact aspects of public-private hybrids are trustworthy; if either component appears trustworthy, that quality bestows citizen trust upon the whole unit.

Digital surveillance: this reliance on public-private partnerships extends into cyberspace. US intelligence agencies have worked closely with private organizations to cultivate citizen protection via digital surveillance of foreign actors. For example, through its PRISM program, the NSA partners with the FBI and CIA (with oversight from the DOJ and the Judiciary) to collect digital data on foreign intelligence targets from private Internet service providers (Director of National Intelligence, 2013). This public-private collaboration is no surprise: Given that these companies own the technology platforms and data that individuals around the globe use to browse, learn, and communicate (Blumenthal, 2018), public entities will be most successful in identifying potential threats through public-private partnerships, as the private entities' capabilities are vastly superior.

Despite the strong protection of individual rights for US citizens, these international protection efforts (whether public or private) do not extend those individual privacy rights to foreign actors. Warrantless surveillance against noncitizens is approved through the Foreign Intelligence Surveillance Act (FISA) section 702 (Pulver and Medina, 2018), and while some groups have voiced concerns over these tactics (Weber, 2015), more than half of Americans find it acceptable for the US government to conduct digital surveillance of foreign actors (Rainie and Madden, 2015). Similarly, as of 2016, the Pew Research Center found that US citizens were more concerned with protection from terrorism (49 percent) vs. civil liberties (33 percent) (Doherty, Kiley and Johnson, 2016). These trends suggest that US citizens trust the capabilities and intentions of these hybrid public-private entities regarding international surveillance.

1.3.2 Evolution of intranational protection

In the United States, despite the existence of strong public institutions with citizen security responsibilities, the realm of intranational security has historically included a considerable private component thanks to the country's revolutionary foundation and strong protections for individual firearm ownership. Be that as it may, similar to the international space, intranational protection has evolved to place even stronger emphasis on private security thanks to the emergence of digital tools. These technologies have bolstered the capabilities of private entities and have better positioned those entities to play a larger role in citizen protection. In addition, powerful, readily available, and relatively inexpensive digital technology has increased citizens' personal protection capabilities relative to traditional law enforcement.

Private commercial security: the commercial use of private security forces has grown in recent years, as evidenced by the presence of uniformed guards in seemingly innocuous establishments from supermarkets to shopping malls. Today the United States is the world's largest private security market, employing 1.5 to 2 million individuals; nearly three private contractors exist for every single

member of the public police force (Abrahamsen and Williams, 2009). Interestingly, in this age of relative peace, these private security companies often work in alignment with public entities, forming a loosely organized group of actors Abrahamsen and Williams term "global security assemblages" (2009). The relative lack of public protest against this trend suggests citizen trust in the capabilities and intentions of these private guards. US students view private security officers' professionalism and goals positively (Nalla and Heraux, 2003). These positive citizen perceptions of private security appear even stronger among students in countries in "emerging" and "flawed" democracies; perhaps in such systems where a lack of confidence in public institutions is common, the intentions of private contractors are viewed as more trustworthy by comparison (Nalla, Maxwell and Mamayek, 2017).

Private home security: beyond this growth in the commercial security market, digital technology has also increased citizens' own protection capabilities. This protection takes several forms, including the rise of a private home security market. Following an increase in crime after World War I, the notion of home security systems, installed and managed by private companies, grew in popularity (Electronic Security Association, 2018). Despite the industry's modest beginnings in which human "door shakers" would confirm that customers' doors were locked each evening, by the 1940s, the American District Telegraph company had installed the first automated burglar system connected via telephone to a central monitoring center (ADT, 2018). The availability of improved camera technology in the 1970s sparked the widespread installation of what are now considered modern home security systems, complete with video surveillance (Electronic Security Association, 2018). Today, an ever-growing number of mobile- and WiFi-based home security options are available to consumers, from the Ring video doorbell and security camera, to the wireless SimpliSafe home security system, to former NSA contractor (also former CIA staff) employee Edward Snowden's Haven app, which converts any Android smartphone into a mobile surveillance tool (Greenberg, 2017). Additionally, despite falling crime rates, the home security market is growing (NextMarket Insights, 2014), suggesting that consumers trust both the capabilities and intentions of these purveyors of private security.

Private individual protection: advocates purport that widespread private gun ownership serves a citizen protection function (Kleck and McElrath, 1991; Lott Jr. and Landes, 1999). Also, see Hemenway (1997) and McDowall (2005) for rigorous rebuttals. Those claims follow from the US Constitution's suggestion that gun ownership is a necessary structure for security: "A well regulated militia, being necessary to the security of a free state, the right of the people to keep and bear arms, shall not be infringed" (The Constitution of the United States, Amendment II). Centuries after its writing, that security structure was reinforced by a US Supreme Court decision that interpreted the Second Amendment to guarantee gun ownership at the level of the individual (*District of Columbia v. Heller*, 2008). It is remarkable that this form of citizen protection is the only structure that delegates security tasks to the individual citizen. The explicit rights in the Second Amendment in effect hire out part of the government's otherwise robust citizen protection

role to private citizens. Unlike most government contracts, however, the labor is unpaid; in fact, the security providers purchase and maintain their own equipment. It appears that gun owners accept the government's mandate; gun owners cite defense as their primary reason for gun ownership, not recreation or hunting (Dimock, Doherty and Christian, 2013). Beliefs about the benefits of gun ownership parallel this trend: 79 percent of gun owners find that owning a gun makes them feel safer, and only 7 percent report that it makes them feel uncomfortable (Dimock, Doherty and Christian, 2013).

This unusual protection structure has been resistant to digital transformation. Many technological advances in guns are traditional improvements to ballistics, harmonics, and optics. Some proposed new technologies are digital transformations; biometric trigger lock devices are fingerprint identification surfaces that would allow only a specific person, ostensibly the adult owner of the gun, to access the trigger. This digital technology affects firearms only until these locks are disabled; after that, the firearms function as usual. There are a variety of analog locks and safes that perform the same function; biometric trigger locks are not an innovation that have transformed citizen protection functions as much as they are an innovation aimed to prevent accidents (Kloepfer et al., 2018). Also, see Mossberg, Kluwe and Kinion (2001) for a similar digital innovation.

Like other methods of protection we have reviewed, steady support for *private* self-protection appears to be driven by a lack of trust in public entities' capacity and motivation to carry out their protective duties. For example, in rural areas where law enforcement response times are greater (indicating a deficiency in the public capability to protect), citizens support Second Amendment rights more strongly (Parker et al., 2017). This perspective appears related to a construct called legal cynicism, in which people view law enforcement as incapable of executing its protective duties: "unresponsive, and ill equipped to ensure public safety" (Sierra-Arévalo and Crowther-Dowey, 2016). Legal cynicism in this domain is also summarized blithely, "When seconds count, police are minutes away." Among gun owners, negative perceptions of police correlate positively with seeking private gun ownership as a defense alternative (Sierra-Arévalo and Crowther-Dowey, 2016). Independent of opinions toward police, perceptions of the state of the world can drive gun ownership. Gun owners are sensitive to diffuse threats that the world is inherently dangerous (Stroebe, Leander and Kruglanski, 2017; Ziegenhagen and Brosnan, 1990; Parker et al., 2017).

Case study: school shooting prevention efforts: consider the first paragon of a school shooting in America – the Columbine massacre – and compare that with the most recent notorious school shooting (at the time of this writing) in Parkland, Florida. The perpetrators of both crimes wrote prolifically about their intent. The Columbine shooters scrawled ink into private notebooks; the Parkland shooter uploaded his dark musings to YouTube for anyone on the Internet to access. Digitalization has transferred even male teenage written angst that precedes deadly violence from private to public view. Private citizens read the Parkland shooter's comment, "Im [sic] going to be a professional school shooter" on YouTube, and

reported him to authorities, including local sheriffs and the FBI (Goldman and Mazzei, 2018). Those private citizens certainly acted with intent for citizen protection, but whether public authorities were capable of delivering that protection is debatable. These macabre examples portray how digital tools may augment the both private and public capabilities for citizen protection. Private citizens noticed the threat; public security forces were incapable of executing to deter the threat. Despite this catastrophe, it is reasonable to hope that the sequence of events in this case will inform future public citizen protection procedures. If so, both private and public capabilities for citizen protection will be enhanced by digital tools.

1.4 Behind the evolution

Broad acceptance of changes to citizen protection structures, roles, and responsibilities should depend on widespread perceptions of the capabilities and intentions of both the public entities typically tasked with this protection and the private organizations that may support or supplant them. If citizens find their governments' capabilities to be deficient or motives to be questionable, and they also believe that private companies can not only fill those roles but also act with benevolent intentions, citizens will allow public-private defense partnerships to thrive with taxpayer support. To this end, private companies use digital tools to tout their capabilities and reinforce their protective intentions.

For these reasons, understanding the role of digitalization in citizen protection requires the present capabilities and intentions framework. In the "Methods" section below, we describe our linguistic measurement tool that captures the degree to which organizations signal their ability to protect and their benevolent motivation. In keeping with our framework, we constructed a robust sample of private and public citizen-protection entities and tested for differences in their communication of protective capabilities and intentions over time.

2 Methods

2.1 Overview

This chapter's arguments rest upon the proposed capabilities and intentions framework for understanding the roles of different actors in the citizen protection landscape. For this reason, we operationalized the signaling of protective capabilities and intentions using a modern linguistic analysis. Organizations, both public and private, communicate their ability to protect citizens effectively, as well as their positive motivations, in the way they outwardly describe themselves. In the digital age, organizations disseminate these self-descriptions on their websites – particularly on their "About Us" web pages. We aimed to measure the amount of protective language on those pages among public vs. private organizations. This linguistic analysis quantifies the extent to which private and public entities each signal their concerns for citizen protection.

2.2 Data and sample

The government departments and agencies discussed in Appendix A comprise our sample of public organizations. Every government entity with a primary mission for citizen protection is included in the sample. We compare those defense-oriented government organizations with the top government contractors – private companies with citizen-protection capabilities. Although the top 100 government contractors are publicly available in ranked order (Washington Technology, 2017), we constrained this sample to organizations with a 2017 government contract over USD 500M. This constraint limited the size of the private sample to 40 organizations to compare to 12 public entities. Each of these private organizations performs its roles using digital tools, strives for digital advances, and capitalizes on digital transformations.

2.3 Measures

The Linguistic Inquiry and Word Count (LIWC) is a text analysis program that measures valuable psychological content in digitalized written samples (Pennebaker et al., 2015b; a). For example, LIWC can measure markers for analytic thinking and emotions (Ritter, Preston and Hernandez, 2014), motivations and risk (Gamache et al., 2015), and even fear and aggression (Soroka, Young and Balmas, 2015). For the purposes of the present analysis, we constructed a dictionary that is sensitive to written markers that signal concern for citizen protection. We adapted the motivational LIWC dictionary (Gamache et al., 2015) to also measure common military and defense terminology (US Department of Defense, 2018).

2.3.1 Independent variable

To measure increasing communication of citizen protection, we used time as our predictor variable to show the evolution of concerns for threat manifested in company descriptions. We mined the Internet for a historical record of organizations' self-descriptions over time using the Internet Archive's Wayback Machine (available at https://archive.org). This website allowed us to capture the language each organization used to describe itself every year dating back to its inaugural website (beginning in the year 1996, when the Internet Archive was founded). For standardization, we attempted to capture all text-based content contained in the first available snapshot of each organization's "About Us" page for each calendar year. For the many cases where the website for any given year was unavailable, we proceeded forward in time to the closest available update. The dates for each observation, and the sample text we analyzed, are available on the Open Science Framework at https://osf.io/xj843, and within a public Github repository here: https://github.com/mac2393/CitizenProtection.

2.3.2 Dependent variables

The Citizen Protection LIWC dictionary yields a continuous measure that is a ratio of key citizen protection words to the total word count in the sample text. As a result, we analyzed 1077 scores from the text of 52 entities (40 private organizations and 12 public entities), from the present back to 1996, where available. Given that the "About Us" page of an organizational website is intended to convey the entity's strategic positioning and capabilities to the public (both potential government clients and private citizens alike), each of those scores serves as a proxy for the organization's intention to signal its capacity and motivation for engaging in protective efforts at that moment in history. This continuous outcome measure allows for the detection of change over time.

2.3.3 Control variables

Our analyses controlled for protection-focused investment, measured using publicly available annual contract sizes for every private defense contractor and annual budgets for every public entity (both from the most recent available calendar year). The three statistical models presented below include budget size as a covariate. All reports hold at the same significance level with and without this covariate included in the regression model.

3 Results

Three notable trends emerged. First, concerns for citizen protection have been reliably increasing, creeping upward, among private defense firms ($t = 8.35$, $p < .001$). Further, this same trend is detectable among US government security entities ($t = 5.37$, $p < .001$). Importantly, and perhaps surprisingly, testing for differences between those slopes reveals that the government's concerns are growing significantly more rapidly, approximately twice the rate of its private contractors ($t = 4.09$, $p < .001$). Figure 11.1 reflects increasing private and public concerns for citizen protection, and also shows their significantly different slopes side by side.

4 Discussion

4.1 Findings

These results indicate increased signaling of protective capabilities and intentions by both public and private entities from 1996 to 2018. Based on this pattern of data, it appears that the organizations within our sample are increasingly concerned with conveying their interest in citizen protection to individual citizens (across both organization types) and, potentially, clients within public entities

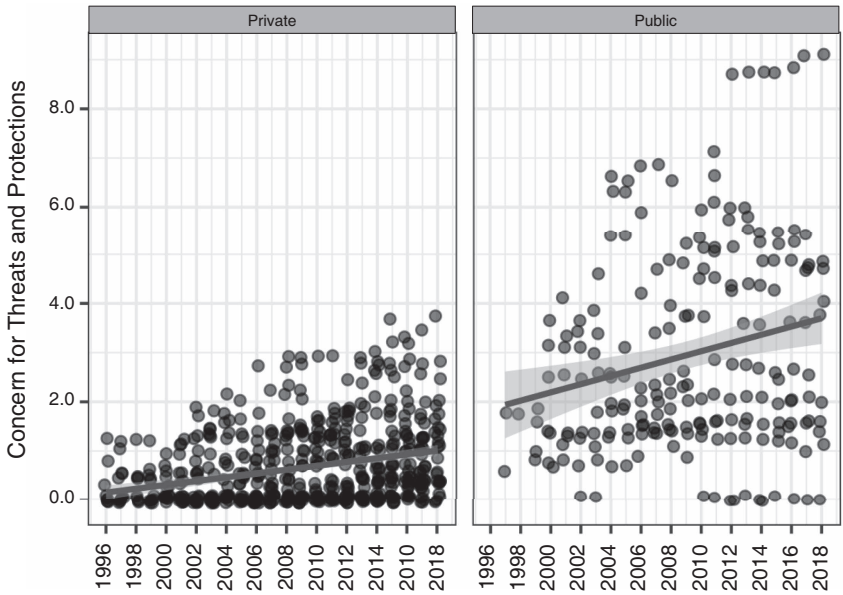

Figure 11.1 Private and public "About Us" statements. Although both continue to signal growing concerns for citizen protection, public institutions outpace private organizations.

responsible for awarding government contracts (in the case of private organizations' websites). Combined with the general evolution of citizen protection in the direction of public-private collaboration, these data suggest that this hybrid approach to citizen protection can be expected to persist.

4.2 Key considerations

Despite some doubts about the capabilities and motivations of the government, 94 percent of Americans still report believing that the government should play a major role in a particular type of citizen protection: "keeping country safe from terrorism" (Doherty et al., 2015). Public views of private institutions have also improved: when comparing 2015 to 2010, the percentage of Americans believing small businesses had a positive effect on the country grew by 11 percentage points, and large corporations by 8 percentage points (Doherty et al., 2015). These numbers suggest an environment ripe for more frequent and extensive public-private partnerships. With this in mind, we identify several challenges this hybrid approach will pose to protective entities in the coming years.

4.2.1 Key consideration #1: navigating borderline cases

Despite apparent public support for privatization and digitalization within certain domains, the distinctions between intranational and international citizen protection have blurred and thus create a wide range of potential "gray areas." For example, consider the protection of citizens from terrorists *within* the state: What is the appropriate balance between maintaining citizen security and yet still adhering to domestic privacy norms? Further, given that these efforts will certainly involve digital surveillance, what might be considered a responsible level of data encryption, whereby law-abiding citizens' rights to privacy are upheld yet the activities of potentially dangerous actors can be monitored? Similarly, consider the protection *from* the state *within* the state (an issue that underlies the right to bear arms within the US Constitution): To what extent should Second Amendment rights allow citizens to prepare a defense against their own government, digitally or physically, should it turn tyrannical? This line of inquiry also raises questions about private oversight of the state: To what extent should private citizens be privy to military plans, operations, and spending information (an especially timely question given the prevalence of digitally facilitated leaks)?

We propose that when the distinctions between inter- and intranational protection are unclear, as illustrated in the examples above, privatization efforts should be accompanied by extensive oversight safeguards, audits, and reviews revisited often. This recommendation becomes even more important when tactics typically assigned to international security (which may fail to uphold individual privacy rights, for example) would be used for the purposes of domestic protection. The importance of this distinction is illustrated by recent events, in which the New York police department shared plans in 2012 to use terahertz ("T-Ray") imaging technology that facilitates long-distance gun detection, enabling public police officers to detect if an individual is carrying a gun under their clothing (Parascandola, 2017). This technology was originally developed by the Department of Defense for international security purposes: specifically, to detect suicide bombers carrying explosives. Though this technology might help police officers identify potential offenders at vulnerable events, it also conflicts with strong privacy protections in the United States ensuring that no citizen or their property can be searched without reasonable cause and a warrant (The Constitution of the United States, Amendment VI). Not surprisingly, the New York Civil Liberties Union pushed back on the adoption of this technology, and the police department subsequently decided to abandon its use (Parascandola, 2017). This example acts as a useful case study for future protective initiatives that cross the inter- vs. intranational divide; proactive engagement with respected civil libertarian groups prior to the adoption of new technology may enable protective entities to identify digital solutions that simultaneously pursue citizen security and uphold fundamental civil rights.

4.2.2 Key consideration #2: maintaining necessary oversight of private entities

As citizen protection structures grow ever more complex through a wide range of public-private partnerships, it naturally becomes more challenging for any "central" public entity to maintain oversight of the associated network of organizations. One important type of oversight relates to the coordination of work among entities that share responsibility for a specific protective function. Given that each involved organization maintains its own internal hierarchy, which indirectly connects with similar hierarchies within partner organizations, the ultimate chain of command across various entities is necessarily more convoluted (and contains additional points of potential failure) than if a single entity were responsible for the same work (Markusen, 2003). If not carefully managed, a complicated cross-organizational structure may also create a lack of transparency within which corruption can thrive. Further, various working groups within this cross-organizational team may suddenly vanish, for all intents and purposes, if the scope of work changes or entities' management cannot align on or adhere to a contract, creating a great deal of operational risk for the "central" entity. Managing these risks and maintaining contingency plans requires substantial oversight, a burden that must be balanced against the apparent benefits of such public-private partnerships.

A second and important type of oversight relates to the assumed cost savings of privatization. Research into the financial realities of public-private partnerships suggests that the cost efficiencies that often drive privatization are ultimately specious; the long-term contracts underlying these partnerships are written in order to impede competition from other firms and flexibility within the scope of work (Avant, 2004). Further, given the limited number of large prime contractors in each realm today, some speculate that these organizations function as an oligopoly and likely engage in some price collusion (Markusen, 2003). This challenge seems only likely to grow given the steep degree of technological expertise required to compete as a contractor within modern weapons development and digital surveillance. Due to these challenges, public entities should maintain vigilant oversight, conducting frequent audits to ensure that partner organizations are delivering the benefits promised.

4.2.3 Key consideration #3: ensuring equitable protection for all citizens

A third challenge for privatization (particularly as it pertains to intranational protection) relates to the unequal distribution of resources inherent in private markets. In its report on Citizen Security and Human Rights, the Inter-American Commission on Human Rights (2009) warns that the privatization of protective functions jeopardizes a nation's ability to guarantee fundamental rights. The report argues that privatization reduces citizen protection to a product that can be retained only by those with the resources to purchase it. Beyond these demand-side challenges to equitable citizen protection, private intranational security solutions are also likely to proliferate within larger and wealthier markets where greater profit margins

can be expected. Thanks to these supply-side differences, rural and low-income areas may experience a dearth of private interest and, as a result, the citizens of these regions may find themselves with diminished access to protection vs. their more affluent, urban-dwelling counterparts (Isima, 2009). For these reasons, it is critical that public organizations maintain a focus on ensuring democratic access to citizen security. In many cases, this emphasis on equal protection will constrain the extent to which these intranational functions can be privatized.

4.2.4 Key consideration #4: aligning public and private objectives

Finally, public entities may find that, at some point, their objectives are no longer aligned with those of their private counterparts. Markusen (2003, p. 490) shares a well-considered list of challenges in her paper arguing against the privatization of international protection:

> What happens when a firm's home government's interest and its employers' interest diverge? How will the potential to sell army and air force modernization advice worldwide affect the proliferation of conventional weapons and techniques? Might not these private arrangements alter the career strategies of members of the armed services? These questions begin to convey the extraordinary challenges facing a world in which the best Western military training and experience is offered for sale on the private market.

In the past 15 years, those predicted challenges have come to fruition. As governments today embark on extensive partnerships with private organizations, they should and can now measure the long-term implications of their collaborations. Specifically, the DOD should track publicly available information on defense contractors: what percentage of their revenue comes from which nations; what percentage of the work in these companies is devoted to the United States compared to all other nations. To address Markusen's third question above, the DOD can capture in exit surveys the proportion of military retirees who have been hired by a defense contractor and conduct more research on whether that opportunity compelled them to leave active duty. Since noncompete agreements are valid between government contractors, would such agreements be tenable between the government and defense contractors? The government might care about the answer to that question only to the extent that it deems the loss of experienced military officers into private employment deleterious to the government's capabilities. This concern would be intensified in a public-private model where the intentions of the private organizations are less trustworthy.

5 Conclusion

The growing public-private hybrid model where private organizations master digital innovations and apply them toward public citizen protection missions shows

no sign of fading and no sign of tilting heavily toward either side. The relationship is symbiotic and recursive, and is supported by public opinion; citizens trust government capabilities and intentions. The borderline cases where governments face dilemmas in order to deliver protection, the challenges of oversight, the concerns for equity, and the tenuous alliance all make these public-private partnerships one of the most important issues in the defense industry.

The sturdiness and longevity of public-private hybrids foment interest in the potential dangers they pose. Consider this contrived scenario that depicts a public-private partnership gone awry where the public entity loses some capability to protect its citizens, while the private component's intentions are unknown. Imagine a government funding a private organization to build a particularly destructive weapon or capability. Perhaps that contractor and its employees could wrest control of material capabilities from any government oversight, access, or failsafe procedures onsite. The government has lost control of the weapon, the capability, and the private aspect of the hybrid might be able to wield that new threat against the government or against the citizenry. Alternatively, the private organization might offer to protect the citizenry against the government with these hijacked capabilities.

Many practical realities undermine the plausibility and dampen the severity of these or similar scenarios. First, a government with military competence enabled by digitalization is likely to deter any rogue takeovers. Next, the decentralization of public-private partnerships would benefit the government in this scenario, where that rogue private organization would represent just one of many capabilities, with the other security relationships intact. Most important, digital communication tools would enable that government to maintain citizen trust. The implausibility of the above scenario underscores and offers some explanation for the endurance of public-private hybrids. Simply put, the size and scope of the existing security apparati in developed countries acts as a check to the dangers new hybrid ventures pose.

As digitalization increases government capabilities, whether in isolation or via partnerships, dangerous scenarios become less, not more, of a legitimate potential danger. Public institutions are incrementally bolstered by the results of these hybrids, and those reinforcements discourage disruptions to the recursive capabilities and intentions framework. Despite these serious concerns, digital innovators secure large government contracts and expand their defense capabilities, but the government is still leading the public-private hybrid model for citizen protection.

Acknowledgments

Members of the motivation science lab and affiliated scholars helped us to create the Citizen Protection LIWC dictionary using their knowledge of regulatory focus theory. We especially thank Maya Rossignac-Milon and Katherine Zee.

Appendix A

International citizen protection structures

This appendix provides a cursory description of key US government citizen protection entities. These brief illustrations of mission sets, histories, and interoperability notes may serve to familiarize readers from outside the United States, and may spark recognition of the roles and responsibilities of parallel ministries and departments within other governments.

The US Department of Defense

The DOD is the largest and longest-standing US government agency, with a primary mission to "provide the military forces needed to deter war and ensure our nation's security" (US Department of Defense, 2019, para.1). The DOD lists on its website that it was founded in conjunction with the American Revolution (US Department of Defense, 2019). The site describes that although the Army, Navy, and Marine Corps were created before the country's official founding, in 1789 the War Department was established. However, the website notes that all branches of military remained under separate direction and, despite several reorganizations, were not unified under a single department until the creation of the National Military Establishment in 1947, and formalized as the Department of Defense (along with the newly formed Air Force) under the National Security Act in 1949. Today, the DOD's website notes that it is responsible for the training and deployment of all branches of the US military. Many nations around the world have a Ministry of Defense that is similar in structure and mission set to the US DOD.

The US Department of State

The DOS leads US diplomatic efforts. The department's website notes that its mission is to "lead America's foreign policy through diplomacy, advocacy, and assistance" (US Department of State, 2019a, para.2). The site describes that the DOS underwent a similar pattern of expansion and reorganization to the DOD since its founding, also in 1789. Primary drivers of the department's expansion were the two world wars in the first half of the 20th century and the ending of the Cold War in the second half; the accompanying changes in the world prompted the United States to enhance its abilities to diplomatically respond to issues ranging from the

new global economy to terrorism (US Department of State, 2019b). Importantly, the DOS also contains dedicated groups with specific citizen protection roles. For example, the Bureau of International Security and Nonproliferation prevents global threats relating to Weapons of Mass Destruction (US Department of State, 2018a). The Bureau of Consular Affairs warns citizens about country-specific threats through its travel alerts and warnings, found on the Bureau's Travel Advisories webpage as well as on its network of embassy and consulate websites (US Department of State, 2018b). Many nations around the world have a Ministry of Foreign Affairs that is similar in structure and mission set to the US DOS.

The US Department of Energy

The DOE website describes that the department aims "to ensure America's security and prosperity by addressing its energy, environmental and nuclear challenges through transformative science and technology solutions" (US Department of Energy, 2019c, para.1). The department's role within citizen protection encompasses the maintenance and security of the country's nuclear arsenal, efforts to protect against threats to critical energy infrastructure, and oversight of emergency energy supplies such as the Strategic Petroleum Reserve (US Department of Energy, 2019d). Since launching the Manhattan Project in 1939, the DOE has played a leading role in both the development of nuclear technologies in the United States and their regulation around the globe (US Department of Energy, 2015). Similar to the DOS, the DOE maintains several organizations with a focus on citizen security. For example, the Office of Nuclear Energy is dedicated to the use of nuclear power as an energy resource, and its focus on citizen protection resides in both promoting the country's energy security and minimizing the risks associated with the proliferation of nuclear technology (US Department of Energy, 2019b). Conversely, the National Nuclear Security Administration (NNSA) was founded in 2000 to oversee military applications of nuclear energy, including oversight of the country's stockpile of nuclear weapons (US Department of Energy, 2019a). The analogous department in some other countries is the Ministry of Energy.

The US Department of Homeland Security

The DHS website describes that the department was established in 2002 following the September 11, 2001, attacks on the World Trade Center in New York, combining 22 distinct federal agencies and departments into a single department with the objective of coordinating the country's homeland security efforts (US Department of Homeland Security, 2016). The site lists DHS goals as "preventing terrorism and enhancing security; managing our borders; administering immigration laws; securing cyberspace; and ensuring disaster resilience" (US Department of Homeland Security, 2016, para.2). The Ministry of the Interior in many countries performs roles similar to the US DHS.

The US Central Intelligence Agency

The CIA describes on its website (2013) that the agency was founded in 1947 under the National Security Act with the purpose of collecting and evaluating intelligence (often with a special focus on human intelligence) to ensure national security. In support of this mission, the CIA indicates on its website that it invests in the development of technology for intelligence purposes. The site also describes that the agency has established dedicated teams with specific citizen protective roles: "nonproliferation, counterterrorism, counterintelligence, international organized crime and narcotics trafficking, environment, and arms control intelligence" (US Central Intelligence Agency, 2013, para.10). Almost every nation around the world has a similar primary intelligence service.

The US National Security Administration and Central Security Service

Established in 1952 following World War II, during which time the country's code-breaking abilities proved critical, the NSA works with its CSS colleagues within the armed forces on the United States' cryptology efforts (US National Security Administration, 2016). Collectively, these organizations serve two primary missions: signals intelligence, the collection of digital intelligence required for national security purposes, and information assurance, the protection of vital United States digital systems from violence and theft (US National Security Administration, 2016). Very few countries perform citizen protection with a robust signals intelligence comparable to the scale and scope of the NSA.

Intranational citizen protection structures

The US Department of Justice (DOJ)

The DOJ's website describes its mission as "[t]o enforce the law and defend the interests of the United States according to the law; to ensure public safety against threats foreign and domestic; to provide federal leadership in preventing and controlling crime; to seek just punishment for those guilty of unlawful behavior; and to ensure fair and impartial administration of justice for all Americans" (US Department of Justice, 2019, para.1). The site further describes that although the Office of the Attorney General was created as a single position in 1789 as part of the Judiciary Act, the DOJ was not officially established until 1870. This new department was intended to oversee both criminal and civil cases with federal interests at stake. Since then, the DOJ has evolved structurally to become "the world's largest law office and the chief enforcer of federal laws" (US Department of Justice, 2019, para.6). Ministries of Justice in other countries perform similar protection roles.

The US judiciary

The judiciary consists of the federal court system, including the Supreme Court, and is primarily responsible for interpreting the meaning of laws in regard to individual cases and determining if laws violate the Constitution (US Government, 2019). Meanwhile, the judiciary was founded with the establishment of the Supreme Court "under Article III of the Constitution to administer justice fairly and impartially, within the jurisdiction established by the Constitution and Congress" (US Judicial Branch, 2019a, para.1). Beyond the Supreme Court, with the Judiciary Act of 1789, the broader federal court system was established with a structure that has broadly remained intact today (The Library of Congress, 2017). Though they share a similar name, the judicial branch is distinct from the DOJ, and these two structures work closely together; for example: "The Department of Justice, which is responsible for prosecuting federal crimes and for representing the government in civil cases, is the most frequent litigator in the federal court system" (Eastern District of Washington, 2018, sec.1.4).

The US Federal Bureau of Investigation

The FBI was established in 1908 as the first federal organization dedicated to addressing national law enforcement (US Federal Bureau of Investigation, 2019a). Since the founding of the FBI Laboratory in 1932, the Bureau has led the use of the latest scientific and technological advances in promoting national security, which originated in practices including fingerprint and handwriting analysis (US Federal Bureau of Investigation, 2019c). Today, the FBI strives to protect American citizens from threats within the country, including terrorism, cyberattacks, civil rights violations, large crime organizations, and "significant" violent crime (US Federal Bureau of Investigation, 2019b). The Ministry of the Interior in many countries performs roles similar to the FBI.

US state courts

In the United States, state courts hear both civil and criminal cases, including tort cases, contract cases, and family cases (US Judicial Branch, 2019b). They are also responsible for interpreting state laws and constitutions (US Judicial Branch, 2019b). As it concerns citizen protection, these courts work with law enforcement officers within the criminal justice system in the trial and judgment of individuals who commit crimes.

Police power

Police in the United States are responsible for local law enforcement, based on states' authority to enforce lawful regulation of citizen behavior (Barnett, 2004). Importantly, the police force is distinct from the military because military forces are not trained to manage citizen security, which has unfortunately led to human

rights violations in certain circumstances (Inter-American Commission on Human Rights, 2009).

Though an important and public-facing component of citizen protection on the local level, police power is not specifically delegated within the United States Constitution and was applied inconsistently within writings from the period of the country's founding (Barnett, 2004). In his seminal treatise on states' legislative power, Michigan Supreme Court Justice Cooley (1871, p. 572) described the police as an entity that seeks:

> not only to preserve the public order and to prevent offences against the State, but also to establish for the intercourse of citizen with citizen those rules of good manners and good neighborhood which are calculated to prevent a conflict of rights, and to insure to each the uninterrupted enjoyment of his own, so far as is reasonably consistent with a like enjoyment of rights by others.

Other scholars have conceived of police power more broadly, which has important implications when weighing individuals' rights (e.g., to privacy) vs. promotion of the "common good" – even if this means prevention of crimes that may or may not take place (Barnett, 2004).

Appendix B

Citizen Protection LIWC dictionary

Table 11.1 Citizen Protection LIWC dictionary. This word list facilitated quantitative measurement of protective language signaled by public and private organizations

Prevention motivational dictionary		*Additional words: citizen protection*	
Accuracy	Loss	Attrition	Mitigate
Afraid	Obligation	Avert	Monitor
Careful	Ought	Constrain	Patrol
Anxious	Pain	Counter	Preserve
Avoid	Prevent	Curb	Recover
Conservative	Protect	Deny	Regulate
Defend	Responsible	Deport	Rescue
Duty	Risk	Duress	Restrict
Escape	Safety	Evacuate	Retain
Escaping	Security	Guard	Safeguard
Evade	Threat	Hostage	Save
Fail	Vigilance	Inhibit	Shield
Fear		Keep	Stave
		Limit	Ward
		Maintain	

Table 11.2 Military, armaments, and defense. More Americans think the US spends "too much" on military, armaments, and defense, while fewer Americans think the US spends "too little"

	2002	*2004*	*2006*	*2008*	*2010*	*2012*
Too little	32	35	25	24	27	25
About right	46	39	33	33	38	43
Too much	22	26	41	43	35	32
N	1324	1367	1442	965	986	965

Source: Adapted from Corman et al., 2015, p. 169.

Table 11.3 National defense. More Americans think the US spends "too much" on defense, while fewer Americans think the US spends "too little"

	2002	*2004*	*2006*	*2008*	*2010*	*2012*
Too little	36	33	28	27	25	26
About right	44	39	34	37	41	43
Too much	20	28	38	37	35	31
N	1348	1371	1445	980	981	934

Source: Adapted from Corman et al., 2015, p. 169.

Table 11.4 Polling indicates low trust and confidence in government

Democrat and Republican beliefs about government		
	Democrats	*Republicans*
How much of the time do you think you can trust the government in Washington to do what is right? (*Only some of the time or never*)	72%	89%
Government is doing too many things better left to businesses and individuals.	29%	71%
Government is almost always wasteful and inefficient.	40%	75%

Source: Adapted from Doherty et al., 2015, pp. 9, 39, 112.

Notes

1 Beyond these three key distinctions, other scholars have called attention to the difference between preventive vs. reactive protection and positive vs. negative protection. We believe the first is self-explanatory; for more detail on the second, see the Report on Citizen Security and Human Rights (Inter-American Commission on Human Rights, 2009).
2 Although the Department of Energy may not be readily categorized as a protection-focused organization, security and protection feature prominently in the DOE mission statement.

References

Abrahamsen, R. and Williams, M.C., 2009. Security beyond the state: global security assemblages in international politics. *International Political Sociology*, 3(1), pp. 1–17.

ADT, 2018. *Our history*. [online] ADT. Available at: <www.adt.com/about-adt/history> [Accessed 4 Sep. 2019].

Avant, D., 2004. The privatization of security and change in the control of force. *International Studies Perspectives*, 5(2), pp. 153–7.

Barnett, R.E., 2004. The proper scope of the police power. *Notre Dame Law Review*, 79(2), pp. 429–95.

Berteau, D., 1998. Defense conversion in information technology service industries. In: G.I. Susman and S. O'Keefe, eds. *The defense industry in the post-Cold War era: corporate strategies and public policy perspectives, technology, innovation, entrepreneurship, and competitive strategy series*. Oxford, UK: Pergamon.

Blumenthal, P., 2018. *Facebook and Google's surveillance capitalism model is in trouble*. Huffington Post. [online] Available at: <https://www.huffingtonpost.com/entry/facebookgoogle-privacy-antitrust_us_5a625023e4b0dc592a088f6c> [Accessed 4 Sep. 2019].

Cohen, D., Nisbett, R.E., Bowdle, B.F. and Schwarz, N., 1996. Insult, aggression, and the southern culture of honor: an 'experimental ethnography.' *Journal of Personality and Social Psychology*, 70(5), pp. 945–59.

Cole, C. and Vermeltfoort, R., 2018. The private military industry. In: *U.S. government contractors and human trafficking, springerbriefs in criminology*. Cham, Switzerland: Springer International Publishing, pp. 9–16.

The *Constitution of the United States, Amendment II*.

The *Constitution of the United States, Amendment VI*.

Cooley, T., 1871. *A treatise on the constitutional limitations which rest upon the legislative power of the states of the American union*. 2nd ed. Boston, MA: Little, Brown & Co.

Corman, J., Harris, K., Levin, D., Schulte, J. and Shanks, B., 2015. Support for defense and military spending. *Public Opinion Quarterly*, 79(1), pp. 166–80.

Dimock, M., Doherty, C. and Christian, L., 2013. *Why own a gun? Protection is now top reason*. Washington, DC: Pew Research Center.

Director of National Intelligence, 2013. *Facts on the collection of intelligence pursuant to section 702 of the Foreign Intelligence Surveillance Act*. [online] Available at: <www.dni.gov/index.php/newsroom/press-releases/press-releases-2013/item/871-facts-on-the-collection-of-intelligence-pursuant-to-section-702-of-the-foreign-intelligence-surveillance-act> [Accessed 4 Sep. 2019].

District of Columbia v. Heller [2008] 554 US 570.

Doherty, C., Kiley, J. and Johnson, B., 2016. *15 years after 9/11, a sharp partisan divide on ability of terrorists to strike US*. Washington, DC: Pew Research Center.

Doherty, C., Kiley, J., Tyson, A. and Jameson, B., 2015. *Beyond distrust: how Americans view their government*. Washington, DC: Pew Research Center.

Eastern District of Washington, 2018. *Educational resources*. [online] US Courts. Available at: <www.waed.uscourts.gov/educational-resources> [Accessed 4 Sep. 2019].

Electronic Security Association, 2018. *The history of home security*. [online] Alarm.org. Available at: <https://alarm.org/the-history-of-home-security> [Accessed 4 Sep. 2019].

FitzGerald, B. and Parziale, J., 2017. As technology goes democratic, nations lose military control. *Bulletin of the Atomic Scientists*, 73(2), pp. 102–7.

Gamache, D.L., McNamara, G., Mannor, M.J. and Johnson, R.E., 2015. Motivated to acquire? The impact of CEO regulatory focus on firm acquisitions. *Academy of Management Journal*, 58(4), pp. 1261–82.

Goldman, A. and Mazzei, P., 2018. YouTube comment seen as early warning in shooting left little for F.B.I. to investigate. *New York Times*, 15 Feb.

Greenberg, A., 2017. Snowden-backed app 'Haven' turns your phone into a home security system. *Wired*. [online] Available at: <www.wired.com/story/snowden-haven-app-turns-phone-into-home-security-system> [Accessed 4 Sep. 2019].

Hemenway, D., 1997. Survey research and self-defense gun use: an explanation of extreme overestimates. *Journal of Criminal Law and Criminology*, 87(4), pp. 1430–45.

Holgate, L.S.H., 2018. *The enduring challenge of nuclear security coordination*. [online] Arms Control Association. Available at: <www.armscontrol.org/act/2018-01/features/enduring-challenge-nuclear-security-coordination> [Accessed 4 Sep. 2019].

Inter-American Commission on Human Rights, 2009. *Report on citizen security and human rights*. Washington, DC: Organization of American States.

Isima, J., 2009. The global marketplace and the privatisation of security. *IDS Bulletin*, 40(2), pp. 113–20.

Kelsey, B.S., 1982. *The dragon's teeth? The creation of United States air power for world war II*. Washington, DC: Smithsonian Institution Press.

Kleck, G. and McElrath, K., 1991. The effects of weaponry on human violence. *Social Forces*, 69(3), pp. 669–92.

Kloepfer, K.T., Stapley, B.D., Haymond, B.R. and Seiter, P.D., 2018. *System and method for authenticating an identity for a biometrically-enabled gun*. U.S. Pat. 9,857,133.

Kocsis, M., 2015. Gun ownership and gun culture in the United States of America. *Essays in Philosophy*, 16(2), pp. 154–79.

Leander, A., 2005. The power to construct international security: on the significance of private military companies. *Millennium: Journal of International Studies*, 33(3), pp. 803–25.

The Library of Congress, 2017. *Judiciary act of 1789: primary documents of American history*. [online] Web Guides by the Library of Congress Digital Reference Section. Available at: <www.loc.gov/rr/program/bib/ourdocs/judiciary.html> [Accessed 4 Sep. 2019].

Light, P.C., 1999. *The true size of government*. Washington, DC: Brookings Institution Press.

Light, P.C., 2017. *The true size of government*. [online] The Volcker Alliance. Available at: <https://www.volckeralliance.org/publications/true-size-government> [Accessed 4 Sep. 2019].

Lott Jr., J.R. and Landes, W.M., 1999. *Multiple victim public shootings, bombings, and right-to-carry concealed handgun laws: contrasting private and public law enforcement*. University of Chicago Law School, John M. Olin Law & Economics Working Paper, No. 73. Chicago, IL: University of Chicago.

Markusen, A.R., 2003. The case against privatizing national security. *Governance*, 16(4), pp. 471–501.

McDowall, D., 2005. Review: John R. Lott, Jr.'s defensive gun brandishing estimates. *The Public Opinion Quarterly*, 69(2), pp. 246–63.

Minow, M., 2005. Outsourcing power: how privatizing military efforts challenges accountability, professionalism, and democracy. *Boston College Law Review*, 46(5), p. 989.

Mossberg, J.E., Kluwe, G.E. and Kinion, K.F., 2001. *Magnetic tag firearm safety enhancement system*. U.S. Pat. 6,219,952.

Nalla, M.K. and Heraux, C.G., 2003. Assessing goals and functions of private police. *Journal of Criminal Justice*, 31(3), pp. 237–47.

Nalla, M.K., Maxwell, S.R. and Mamayek, C.M., 2017. Legitimacy of private police in developed, emerging, and transitional economies. *European Journal of Crime, Criminal Law and Criminal Justice*, 25(1), pp. 76–100.

NextMarket Insights, 2014. *The smart home security market: market analysis, vendor profiles & forecast*. [online] Available at: <http://web.archive.org/web/20181118183554/www.shield-security.com/hs-fs/hub/208616/file-1882657287-pdf/Smart_Home_Security_Report_.pdf> [Accessed 4 Sep. 2019].

Parascandola, R., 2017. NYPD's 'T-Ray' gun sensors sit idle, but that's OK with cops. *New York Daily News*, 21 Feb.

Parker, K., Horowitz, J., Igielnik, R., Oliphant, B. and Brown, A., 2017. *America's complex relationship with guns*. Washington, DC: Pew Research Center.

Pennebaker, J.W., Booth, R.J., Boyd, R.L. and Francis, M.E., 2015a. *Linguistic inquiry and word count: LIWC 2015 [computer program]*. [online] Available at: <https://s3-us-west-2.amazonaws.com/downloads.liwc.net/LIWC2015_OperatorManual.pdf> [Accessed 4 Sep. 2019].

Pennebaker, J.W., Boyd, R.L., Jordan, K. and Blackburn, K., 2015b. *The development and psychometric properties of LIWC2015*. Austin, TX: University of Texas.

Prem, B., 2018. Who am I? The blurring of the private military and security company (PMSC) category. In: O. Bures and H. Carrapico, eds., *Security privatization: how non-security-related private businesses shape security governance*. Cham, Switzerland: Springer International Publishing, pp. 51–76.

Pulver, A. and Medina, R.M., 2018. A review of security and privacy concerns in digital intelligence collection. *Intelligence and National Security*, 33(2), pp. 241–56.

Rainie, L. and Madden, M., 2015. *Americans' privacy strategies post-Snowden*. [online] Pew Research Center: Internet, Science & Tech. Available at: <www.pewinternet.org/2015/03/16/americans-privacy-strategies-post-snowden> [Accessed 4 Sep. 2019].

Ritter, R.S., Preston, J.L. and Hernandez, I., 2014. Happy tweets: Christians are happier, more socially connected, and less analytical than atheists on Twitter. *Social Psychological and Personality Science*, 5(2), pp. 243–9.

Rosenberg, M., 2016. *At Booz Allen, a vast U.S. spy operation, run for private profit*. [online] The New York Times. Available at: <https://www.nytimes.com/2016/10/07/us/booz-allen-hamilton-nsa.html> [Accessed 4 Sep. 2019].

Sierra-Arévalo, M. and Crowther-Dowey, C., 2016. Legal cynicism and protective gun ownership among active offenders in Chicago. *Cogent Social Sciences*, 2(1), 1227293, pp. 1–21.

Singer, P.W., 2005. Outsourcing war. *Foreign Affairs*, 84(2), pp. 119–32.

Singer, P.W., 2008. *Corporate warriors: the rise of the privatized military industry*. 2nd ed. *Cornell studies in security affairs*. Ithaca, NY: Cornell University Press.

Soroka, S., Young, L. and Balmas, M., 2015. Bad news or mad news? Sentiment scoring of negativity, fear, and anger in news content. *The Annals of the American Academy of Political and Social Science*, 659(1), pp. 108–21.

Stroebe, W., Leander, N.P. and Kruglanski, A.W., 2017. The impact of the Orlando mass shooting on fear of victimization and gun-purchasing intentions: not what one might expect. *PLOS ONE*, 12(8), e0182408, pp. 1–15.

Tighe, C.E., Kleinman, S.D., Jondrow, J.M. and Trunkey, R.D., 1996. *Outsourcing and competition: lessons learned from DOD commercial activities programs*. Occasional Paper, October. Alexandria, VA: Center for Naval Analyses.

Ullah, H., 2017. *Digital world war: Islamists, extremists, and the fight for cyber supremacy*. New Haven, CT: Yale University Press.

UN General Assembly, 1948. *The universal declaration of human rights*. Paris, France: United Nations.

US Central Intelligence Agency, 2013. *About CIA*. [online] US Central Intelligence Agency. Available at: <https://cia.gov/about-cia> [Accessed 4 Sep. 2019].

US Department of Defense, 2018. *DOD dictionary of military and associated terms*. [online] Available at: <www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf?ver=2018-09-28-100314-687> [Accessed 4 Sep. 2019].

US Department of Defense, 2019. *Our story*. [online] US Department of Defense. Available at: <www.defense.gov/Our-Story> [Accessed 4 Sep. 2019].

US Department of Energy, 2015. *History of the energy department's role in nuclear security*. [online] US Department of Energy. Available at: <www.energy.gov/articles/history-energy-departments-role-nuclear-security> [Accessed 4 Sep. 2019].

US Department of Energy, 2019a. *About NNSA*. [online] US Department of Energy. Available at: <www.energy.gov/node/2764052/timeline> [Accessed 4 Sep. 2019].

US Department of Energy, 2019b. *About us (ONE)*. [online] US Department of Energy. Available at: <www.energy.gov/ne/about-us> [Accessed 4 Sep. 2019].

US Department of Energy, 2019c. *Mission*. [online] US Department of Energy. Available at: <www.energy.gov/mission> [Accessed 4 Sep. 2019].

US Department of Energy, 2019d. *National security & safety*. [online] US Department of Energy. Available at: <www.energy.gov/national-security-safety> [Accessed 4 Sep. 2019].

US Department of Homeland Security, 2016. *Mission*. [online] US Department of Homeland Security. Available at: <www.dhs.gov/mission> [Accessed 4 Sep. 2019].

US Department of Justice, 2019. *About DOJ*. [online] US Department of Justice. Available at: <www.justice.gov/about> [Accessed 4 Sep. 2019].

US Department of State, 2018a. *Bureau of international security and nonproliferation (ISN)*. [online] US Department of State. Available at: <www.state.gov/t/isn> [Accessed 4 Sep. 2019].

US Department of State, 2018b. *Travel advisories*. [online] US Department of State. Available at: <https://travel.state.gov/content/travel/en/traveladvisories/traveladvisories.html> [Accessed 4 Sep. 2019].

US Department of State, 2019a. *About the U.S. Department of State*. [online] US Department of State. Available at: <www.state.gov/aboutstate> [Accessed 4 Sep. 2019].

US Department of State, 2019b. *Department history*. [online] Office of the Historian. Available at: <https://history.state.gov/departmenthistory> [Accessed 4 Sep. 2019].

US Federal Bureau of Investigation, 2019a. *A brief history*. [online] Federal Bureau of Investigation. Available at: <www.fbi.gov/history/brief-history> [Accessed 4 Sep. 2019].

US Federal Bureau of Investigation, 2019b. *Mission & priorities*. [online] Federal Bureau of Investigation. Available at: <www.fbi.gov/about/mission> [Accessed 4 Sep. 2019].

US Federal Bureau of Investigation, 2019c. *The FBI and the American gangster, 1924–1938*. [online] Federal Bureau of Investigation. Available at: <www.fbi.gov/history/brief-history/the-fbi-and-the-american-gangster> [Accessed 4 Sep. 2019].

US Government, 2019. *Branches of government*. [online] USA.Gov. Available at: <www.usa.gov/branches-of-government> [Accessed 4 Sep. 2019].

US Judicial Branch, 2019a. *About federal courts*. [online] United States Courts. Available at: <www.uscourts.gov/about-federal-courts> [Accessed 4 Sep. 2019].

US Judicial Branch, 2019b. *Comparing federal & state courts*. [online] United States Courts. Available at: <www.uscourts.gov/about-federal-courts/court-role-and-structure/comparing-federal-state-courts> [Accessed 4 Sep. 2019].

US National Security Administration, 2016. *Frequently asked questions about NSA*. [online] US National Security Administration and Central Security Service. Available at: <www.nsa.gov/about/faqs/about-nsa-faqs.shtml#about11> [Accessed 4 Sep. 2019].

Washington Technology, 2017. *2017 top 100*. [online] Washington Technology. Available at: <https://washingtontechnology.com/toplists/top-100-lists/2017.aspx> [Accessed 4 Sep. 2019].

Weber, R.H., 2015. The digital future – a challenge for privacy? *Computer Law & Security Review*, 31(2), pp. 234–42.

Ziegenhagen, E.A. and Brosnan, D., 1990. Citizen recourse to self protection: structural, attitudinal and experiential factors. *Criminal Justice Policy Review*, 4(2), pp. 91–104.