Georgia Law Review

Volume 49 | Number 3 Article 2

2015

Outsourcing, Data Insourcing, and the Irrelevant Constitution

Kimberly N. Brown
University of Baltimore School of Law

GEORGIA LAW REVIEW

VOLUME 49 SPRING 2015 NUMBER 3

ARTICLES

OUTSOURCING, DATA INSOURCING, AND THE IRRELEVANT CONSTITUTION

Kimberly N. Brown[*]

TABLE OF CONTENTS

* Associate Professor of Law, University of Baltimore School of Law. B.A., Cornell; J.D., University of Michigan. Thanks to Michele Gilman, Dionne Koller, Matthew Lindsay, C.J. Peters, Elizabeth Samuels, and Colin Starger for tremendously helpful comments on earlier drafts, and to Ben Bor, Laura Gagne, and Andrew Geraghty for excellent research assistance.

I. INTRODUCTION

When Edward Snowden became a household name in the summer of 2013, a majority of Americans still viewed dragnet-style surveillance by the National Security Agency (NSA) as an acceptable means of combatting terrorism.[1] President George W. Bush publicly acknowledged in 2005 that the NSA had been conducting surveillance of ordinary Americans through the unprecedented collection of individual phone records and emails after the terrorist attacks on September 11, 2001 (9/11).[2] By January of 2014, however, public opinion had shifted.[3] For the first time in history, Americans are grappling with the gravity of our emerging surveillance state.

The American public has legitimate cause for alarm. Once the stuff of "paranoid fantasy,"[4] the era of ubiquitous government surveillance has arrived in large part due to the expansion of

---

[1] PEW RESEARCH CTR., MAJORITY VIEWS NSA AS ACCEPTABLE ANTI-TERROR TACTIC: PUBLIC SAYS INVESTIGATE TERRORISM, EVEN IF IT INTRUDES ON PRIVACY (2013), *available at* http://www.people-press.org/files/legacy-pdf/06-10-13%20WP%20 Surveillance%20Release.pdf.

[2] Devlin Barrett, *U.S. Declassifies Some Details of Bush-Era Surveillance; Obama Administration Still Opposes Disclosure of Specifics*, WALL ST. J., Dec. 22, 2013, http://online.wsj.com/news/articles/SB10001424052702303773704579272121175326400; James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 15, 2005, http://www.nytimes.com/2005/12/16/politics/16program.html. The program was reportedly discontinued in 2007. Dan Eggen, *Court Will Oversee Wiretap Program*, WASH. POST, Jan. 18, 2007, at A01, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2007/01/17/AR2007011701256.html; Letter from Alberto R. Gonzales, U.S. Attorney Gen., to Patrick Leahy, Chairman of the Comm. on the Judiciary, and Arlen Specter, Ranking Minority Member of the Comm. of the Judiciary (Jan 17, 2007), *available at* http://hosted.ap.org/dynamic/files/specials/interactives/wdc/documents/fisa/Gonzales070117.pdf?SITE=AP&SECTION=HOME.www.people-press.org/files/legacy-pdf/06-10-13%20WP%20Surveillance%20Release.pdf.

[3] *See* Susan Page, *Poll: Most Americans Now Oppose the NSA Program*, USA TODAY (Jan. 20, 2014, 3:10 PM), http://www.usatoday.com/story/news/politics/2014/01/20/poll-nsa-surveillance/4638551/ (finding that most Americans polled now indicate their disapproval of the sweeping NSA surveillance).

[4] *See* James Risen & Laura Poitras, *N.S.A. Examines Social Networks of U.S. Citizens*, N.Y. TIMES, Sept. 29, 2013, at 22, *available at* http://www.nytimes.com/2013/09/29/us/nsa-examines-social-networks-of-us-citizens.html?src=twrhp&_r=0 (describing the extremity of the government intrusion); Dan Frookin, *Top Journalists and Lawyers: NSA Surveillance Threatens Press Freedom and Right to Council*, THE INTERCEPT (July 28, 2014, 9:34 AM), http://firstlook.org/theintercept/2014/07/28/nsa-surveillance-threatens-press-freedom-right-counsel-survey-finds/ (describing the actual intrusion as "previously considered the stuff of paranoid fantasy").

advanced technology and bulk data in *private* hands.[5] Gone are the days in which cutting-edge clandestine surveillance was conducted through direct—yet relatively exceptional—methods like court-ordered wiretaps. The government now carries out much of its surveillance by applying mathematical algorithms to huge sets of data that customers willingly turn over to third-party sources such as Verizon and Google.[6] Privately-sourced phone, e-mail, and IP address information is then paired with so-called "enrichment data" from Facebook, credit card companies, airline manifests, voter registration rolls, GPS devices, aerial and closed-circuit camera photos,[7] facial recognition systems,[8] embedded microchips,[9] and web-tracking technologies to create intimate personal dossiers of unsuspecting individuals who have broken no laws.

---

[5] *See Obama's Speech on N.S.A. Surveillance*, N.Y. TIMES, Jan. 17, 2014, http://www.nytimes.com/2014/01/18/us/politics/obamas-speech-on-nsa-phone-surveillance.html (acknowledging that technological advances, including those that facilitate bulk data gathering by private corporations, invite abuse of Americans' civil liberties if left unrestrained).

[6] *See* Barton Gellman, Aaron Blake & Greg Miller, *Edward Snowden Comes Forward as Source of NSA Leaks*, WASH. POST, June 9, 2013, http://www.washingtonpost.com/politics/intelligence-learders-push-back-on-leakers-media/2013/06/09/ffff80160-d122-1e2-a73e-826d299ff459_story.html (discussing the shocking revelation of surveillance programs that collect data from third-party sources such as Verizon); Timothy B. Lee, *Here's Everything We Know About PRISM to Date*, WASH. POST, June 12, 2013, http://www.washingtonpost.com/blogs/wonkblog/wp/2013/06/12/heres-everything-we-know-about-prism-to-date/ (discussing how the NSA's PRISM program allows the NSA to collect data directly from the servers of Internet companies).

[7] *See* Craig Timberg, *New Surveillance Technology Can Track Everyone in an Area for Several Hours at a Time*, WASH. POST, Feb. 5, 2014, http://www.washingtonpost.com/business/technology/new-surveillance-technology-can-track-everyone-in-an-area-for-several-hours-at-a-time/2014/02/05/82f1556e-876f-11e3-a5bd-844629433ba3_story.html (discussing state use of aerial camera surveillance).

[8] *See* Kimberly N. Brown, *Anonymity, Faceprints, and the Constitution*, 21 GEO. MASON L. REV. 409, 432–36 (2014) (describing facial recognition technology and its use); James Risen & Laura Poitras, *N.S.A. Collecting Millions of Faces from Web Images*, N.Y. TIMES, June 1, 2014, at A1, *available at* http://www.nytimes.com/2014/06/01/us/nsa-collecting-millions-of-faces-from-web-images.html (describing the NSA's expanding use of facial recognition technology for surveillance); Naomi Wolf, *The New Totalitarianism of Surveillance Technology*, THE GUARDIAN, Aug. 15, 2012, http://www.theguardian.com/commentisfree/2012/aug/15/new-totalitarianism-surveillance-technology (discussing the use of facial recognition technology in New York City); Natasha Singer, *Never Forgetting a Face*, N.Y. TIMES, May 18, 2014, at BU1, *available at* http://www.nytimes.com/2014/05/18/technology/never-forgetting-aface.html (describing a scientific pioneer's misgivings with the trajectory of facial recognition technology).

[9] *See generally* KATHERINE ALBRECHT & LIZ MCINTYRE, SPYCHIPS (Plume 2006) (discussing the impact of microchip technology on privacy).

Such data *insourcing*[10] for purposes of surveillance is of a piece with the government's widespread practice of *outsourcing* sovereign responsibilities to third parties through service contracts and other devices that effectively transfer public power to private hands. In both circumstances, existing law is not up to the task of ensuring that government officials remain accountable to the populace for sponsored activities. Statutory surveillance law and Fourth Amendment doctrine were crafted in the pre-digital age, when unconsented monitoring by the government was the greatest threat to privacy.[11] Yet today, private industry parses and stores personal information on a scale that is exponentially greater than that which the government can aspire to on its own.[12] The government capitalizes on such troves of private sector

---

[10] Insourcing is typically used to describe "the use of government personnel to perform functions that contractors have performed on behalf of federal agencies." KATE M. MANUEL & JACK MASKELL, CONG. RESEARCH SERV., R41810, INSOURCING FUNCTIONS PERFORMED BY FEDERAL CONTRACTORS: LEGAL ISSUES (2013), *available at* http://fas.org/sgp/crs/misc/R41810.pdf. It has been promoted by recent Congresses as well as the Obama Administration in response to concerns over outsourcing. *Id.* As used in this Article, "insourcing" refers to the government's use of private sector data and lack of constitutional limitations that govern it. It does not include information that private persons are required to provide the government by law or regulation. *See infra* notes 76–79 and accompanying text (summarizing routine data collection through tax returns and other incidents of citizenship). This Article does not discuss The Privacy Act of 1974, 5 U.S.C. § 552a (amended 2014), which is the primary legal authority addressing the government's use and sharing of records but does not bind private parties or restrict the government's ability to collect information from third parties. It provides that agencies shall "collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs." *Id.* § 552a(e)(2). The Privacy Act contains an exception for law enforcement activity. *Id.* § 552a(b)(7).

[11] *See* Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1940 (2013) (observing that existing surveillance laws "focus[ ] on unconsented surveillance rather than on surveillance as part of [a] transaction"); Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV. 547, 620 (1999) ("[T]he historical sources show that the Framers worded the search and seizure provisions as they did to counter the possibility that legislators might authorize use of general warrants for customs searches of houses . . . ."). In referring to privacy, this Article focuses less on information nondisclosure and more on liberty or, as Anita Allen describes it, "freedom from governmental or other outside interference with decisionmaking and conduct, especially respecting appropriately private affairs." Anita L. Allen, *Taking Liberties: Privacy, Private Choice, and Social Contract Theory*, 56 U. CIN. L. REV. 461, 464–66 (1987). For a discussion of the dangers of ubiquitous surveillance, see Brown, *supra* note 8, at 434–36.

[12] *See* Jon D. Michaels, *All the President's Spies: Private-Public Intelligence Partnerships in the War on Terror*, 96 CALIF. L. REV. 901, 902 (2008) (discussing how the private sector has a "comparative advantage over the government in acquiring vast amounts of potentially useful data").

information for its own surveillance.[13] It also hires private parties for military combat operations, nuclear weapons management, municipal policing, prison administration, policy planning and rulemaking, public benefits determinations, international relations work, and its own personnel management.[14]

Because the Constitution only applies to state action,[15] the government's use of *private* sources to conduct its work evades constitutional barriers that would otherwise operate to ensure accountability to the people.[16] Outsourcing and data insourcing occupy what amounts to a pocket of constitutional immunity as an accident of doctrinal shortsightedness.[17] Numerous scholars have outlined legislative proposals for addressing private sector involvement in government practices.[18] This Article seeks to

---

[13] Paul Ohm, *The Fourth Amendment in a World Without Privacy*, 81 MISS. L.J. 1309, 1311, 1321–22 (2012) (discussing the government's increasing reliance on private surveillance); Michaels, *supra* note 12, at 909 ("[I]f the government can convince private businesses to share their data collections, it can make an end-run around the more stringent restrictions limiting its ability to access information directly.").

[14] Dan Guttman, *Governance by Contract: Constitutional Visions; Time for Reflection and Choice*, 33 PUB. CONT. L.J. 321, 323 (2004); *see* Michaels, *supra* note 12, at 902 (discussing the extent to which the government relies on the private sector).

[15] *See* United States v. Jacobsen, 466 U.S. 109, 113–14 (1984) ("This court has . . . construed [Fourth Amendment] protection as proscribing only governmental action.").

[16] *See* Christopher Slobogin, *Government Data Mining and the Fourth Amendment*, 75 U. CHI. L. REV. 317, 321 (2008) (observing that "Fourth Amendment jurisprudence appears to leave data mining completely unregulated" and proposing a framework for interpreting the doctrine to require limitations on government data mining); *cf.* Marc Jonathan Blitz, *Video Surveillance and the Constitution of Public Space: Fitting the Fourth Amendment to a World That Tracks Image and Identity*, 82 TEX. L. REV. 1349, 1364–65 (2004) (arguing that, instead of protecting individual expectations of privacy, courts should identify and protect public spaces that allow privacy interests to exist).

[17] *Cf.* Alfred C. Aman, Jr., *Globalization, Democracy, and the Need for a New Administrative Law*, 10 IND. J. GLOBAL LEGAL STUD. 125, 130 (2003) (discussing how privatization of outsourcing creates a "democracy deficit" by reducing transparency under current policies).

[18] *See, e.g.*, *id.* at 151–54 (advocating for amendment of the Administrative Procedure Act to ensure proper accountability of government contractors and private actors performing government functions); Anthony LaPlaca, *Settling the Inherently Governmental Functions Debate Once and for All: The Need for Comprehensive Legislation of Private Security Contractors in Afghanistan*, 41 PUB. CONT. L.J. 745, 764 (2012) ("Congress should explicitly preclude the Government from outsourcing certain functions by adopting binding legislation that gives teeth to restrictions on private security contracting."); David Thaw, *The Efficacy of Cybersecurity Regulation*, 30 GA. ST. U. L. REV. 287, 370–71 (2014) (indicating that cybersecurity regulatory reform should include a combination of "Management-Based Regulatory Delegation" and "directive regulation"); *see also* Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 311–15

establish that, in spite of the many shortfalls in prevailing doctrine, recognition of constitutional limits on the government's use of insourcing and outsourcing to perform sovereign functions is—or should be—inexorable. Such limits can be derived from the Constitution's structure, which assumes that the government remains ultimately accountable to the people for the exercise of its functions. With an eye towards creative litigation, this Article recasts state action, private delegation, and Fourth Amendment doctrine in ways that enable judicial review of whether the government has structured its outsourcing and data insourcing relationships in ways that preserve constitutional accountability.

Part I describes the problem. Although governments have long relied on private parties to perform their core functions,[19] the practice in the United States today is so widespread that "[t]he fact that some of what government does can be done better and cheaper by the private sector has gained such momentum that the public sector is sometimes seen as redundant or irrelevant."[20] The government conducts much of its surveillance using massive amounts of the private sector's data.[21] Because private corporations operate extra constitutionally,[22] the net effect of the

---

(2011) (making cautionary recommendations for legislatures developing privacy law reforms); *cf.* Stan Soloway & Alan Chvotkin, *Federal Contracting in Context: What Drives It, How to Improve It*, *in* GOVERNMENT BY CONTRACT: OUTSOURCING AND AMERICAN DEMOCRACY 192, 235–38 (Jody Freeman & Martha Minow eds., 2009) (arguing for a greater focus on government employees and contract workers, as opposed to increased legislation, to improve government outsourcing).

[19] Guttman, *supra* note 14, at 323; Daniel Guttman, *Public Purpose and Private Service: The Twentieth Century Culture of Contracting Out and the Evolving Law of Diffused Sovereignty*, 52 ADMIN. L. REV. 859, 863–64 (2000) (describing the evolution of privatized government over the course of the twentieth century).

[20] Paul R. Verkuil, *Public Law Limitations on Privatization of Government Functions*, 84 N.C. L. REV. 397, 397 (2006). The primary rationale supporting privatization—that private markets are more efficient and apolitical than government—is itself subject to sharp debate. *See, e.g.*, Matthew Titolo, *Privatization and the Market Frame*, 60 BUFF. L. REV. 493, 494 (2012) (providing a critical examination "of those assumptions and suggest[ing] that we abandon our baseline view of privatization as efficient, neutral, and apolitical to adopt a default view of privatization as fraught with normative implications"); Sidney A. Shapiro, *Outsourcing Government Regulation*, 53 DUKE L.J. 389, 432 (2003) ("When the government depends on private actors for regulatory functions, it has the cost of contracting with those actors and monitoring their performance. These costs can exceed any cost savings created by relying on private actors to perform regulatory functions.").

[21] *See* Ohm, *supra* note 13, at 1322 (discussing the "increasing reliance on technological advances and private surveillance" by the government).

[22] *See supra* note 15.

government's *insourcing* of privately sourced data and its *outsourcing* of power to the private sector is a dilution of the relevancy of the Constitution when it comes to ensuring accountability to the public for the exercise of sovereign functions.

Part III describes the current legislative frameworks that apply to federal outsourcing and data insourcing for government surveillance, and explains how both fail to meaningfully limit the government's ability to outsource public functions or adequately control its access to private data for surveillance.[23]

Part IV reviews the constitutional doctrine bearing on privatization, which developed without a coherent framework for testing alterations to the tripartite structure of government. As a consequence, ad hoc case law under the state action doctrine, the private delegation doctrine, and the Fourth Amendment has failed to account for the myriad ways in which the private sector infiltrates modern government, relying instead on the false assumption that the public and private spheres can be treated as distinct for purposes of constitutional law.[24]

Part V argues that the merging of the public and private sectors should instead be analyzed against a presumption of adherence to constitutional structure that assumes—and thus requires as a matter of first principles—that government is accountable to the people.[25] Recognizing that the law must evolve within existing doctrine to the extent possible, this Article goes on to make a case

---

[23] *See infra* notes 152–58 and accompanying text (summarizing the deficiencies of the current regulatory scheme).

[24] *See infra* notes 296–98, 335–38, 356–75 and accompanying text. For a discussion of the First Amendment in the context of metadata surveillance, see Brown, *supra* note 8, at 449–55.

[25] *See* Akhil Reed Amar, *Of Sovereignty and Federalism*, 96 YALE L.J. 1425, 1431–36 (1987) (contrasting the eighteenth-century British belief that sovereignty was unlimited and "resided in the [King]" with the American concept that "government entities were sovereign only in a limited and derivative sense, exercising authority only within boundaries set by the sovereign People"). *But cf.* Massachusetts v. Envtl. Prot. Agency, 549 U.S. 497, 519 (2007) (suggesting that the Constitution is a compromise between the national government and the states, which ceded "sovereign prerogatives" to the former); Clayton P. Gillette & Paul B. Stephan III, *Constitutional Limitations on Privatization*, 46 AM. J. COMP. L. 481, 482 (1998) (observing that some commentators view the Constitution "as a blueprint for decision making processes, rather than as a guarantee of substantive outcome" and emphasizing that "no clear consensus exists within the United States over what functions are either properly or exclusively the government's" (citing Ronald A. Cass, *Privatization: Politics, Law and Theory*, 71 MARQ. L. REV. 449 (1988))).

for recalibrating state action, private delegation, and Fourth Amendment doctrine as potential tools for rendering the government constitutionally accountable to the public when it outsources sovereign functions to the private sector or insources third-party data for use in its own surveillance activities.[26]

II. OUTSOURCING, DATA INSOURCING, AND THE PRIVATE SECTOR

Although privatization takes many forms,[27] perhaps the most familiar is the traditional service contract, whereby a private third-party agrees to perform some function that the government would otherwise perform for itself, such as routine building maintenance.[28] Traditional service contracting becomes problematic when it implicates core government functions or individual civil liberties,[29]

---

[26] This Article does not advocate for stronger constitutional boundaries on outsourcing in all circumstances. The issue has sharp political undertones that are beyond the scope of this Article. Whereas liberals might seek to limit outsourcing and insourcing in order to enhance government accountability and preserve civil liberties, for example, conservatives might promote the same methods with the objective of shrinking the size of government. *Cf.* Douglas H. Ginsburg & Steven Menashi, *Nondelegation and the Unitary Executive*, 12 U. PA. J. CONST. L. 251, 272 (2010) ("If the Congress had to vote on the Code of Federal Regulations rule by rule, much if not most of it surely would fail. Yet those rules have the force of law without Congress having voted at all."). *See generally* Ellen Dannin, *Red Tape or Accountability: Privatization, Public-ization, and Public Values*, 15 CORNELL J.L. & PUB. POL'Y 111, 113–17 (2005) (discussing the benefits and challenges of contracting out government work).

[27] *See generally* JANINE R. WEDEL, SHADOW ELITE: HOW THE WORLD'S NEW POWER BROKERS UNDERMINE DEMOCRACY, GOVERNMENT, AND THE FREE MARKET 74–75 (2009) (discussing ways in which "a host of nongovernmental players do the government's work, often overshadowing government bureaucracy, which sometimes looks like Swiss cheese: full of holes").

[28] *See* Jack M. Beermann, *Privatization and Political Accountability*, 28 FORDHAM URB. L.J. 1507, 1522–25, 1529–53 (2001) (discussing numerous ways in which the government "contract[s] out"); Paul Seidenstat, *The Mechanics of Contracting Out*, *in* CONTRACTING OUT GOVERNMENT SERVICES 233–47 (Paul Seidenstat ed., 1999) (same); Jon D. Michaels, *Privatization's Progeny*, 101 GEO. L.J. 1023, 1026–27 (2013) (discussing privatization in the form of the "marketization of bureaucracy" and "government by bounty").

[29] *See* Jody Freeman & Martha Minow, *Introduction: Reframing the Outsourcing Debates*, *in* GOVERNMENT BY CONTRACT: OUTSOURCING AND AMERICAN DEMOCRACY, *supra* note 18, at 2 (noting how critics of government outsourcing worry that its expansion in military, security, and intelligence and policymaking functions further restricts the government's ability to ensure adherence to democratic norms); Verkuil, *supra* note 20, at 402, 420–32 (arguing that some discretionary, policymaking functions of government should not be delegated to the private sector and suggesting that the nondelegation doctrine can be used to determine what may and may not be delegated).

such as military operations on the battlefield,[30] the drafting of regulations,[31] or management of nuclear weapons sites.[32] Other forms of outsourcing include industry deregulation; the use of vouchers;[33] the divestiture of government assets to private parties;[34] and the infusion of market principles into the public sector by curtailing collective bargaining rights of government employees or converting civil service jobs to at-will positions.[35] Outsourcing has received substantial scholarly attention because it challenges the basic structure of government and the presumption that the public and the private spheres are distinct.[36]

Edward Snowden brought to the forefront of public consciousness an inconspicuous manifestation of privatization: the government's reliance on privately held personal data for intelligence and law enforcement surveillance.[37] This practice—which this Article calls "data insourcing"—is a form of outsourcing; the government relies on private parties to perform a function (intelligence-gathering) that it would otherwise provide independently. Because the private sector is not bound by the Constitution, it can collect private information with constitutional impunity.[38] In bootstrapping that data as its own, the government

---

[30] *See* Denis Chamberland, *Contractors on the Battlefield: Outsourcing of Military*, NAT'L DEF. MAG., Mar. 2011, *available at* http://www.nationaldefensemagazine.org/archive/2011/March/Pages/ContractorsontheBattlefieldOutsourcingMilitaryServices.aspx (discussing the challenge of maintaining control over private contractors for military services and the methods in place to deal with this challenge).

[31] *See* Chris Sagers, *The Myth of "Privatization,"* 59 ADMIN. L. REV. 37, 45–46 (2007) (noting that privatization writers have expressed concern about the privatization of "seemingly inherent government functions" like policymaking).

[32] *See* Gene Aloise, U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-10-115, NATIONAL NUCLEAR SECURITY ADMINISTRATION NEEDS TO BETTER MANAGE RISKS ASSOCIATED WITH MODERNIZATION OF ITS PLANTS 7 (Oct. 2009) (noting that outsourcing components of a nuclear weapons plant may increase the risk that the components will be obtained by adversaries).

[33] Beermann, *supra* note 28, at 1519.

[34] *Id.*

[35] Michaels, *supra* note 28, at 1026.

[36] *See* Paul Starr, *The Meaning of Privatization*, 6 YALE L. & POL'Y REV. 6, 7 (1988) ("In desperation some theorists announce that the distinction is outdated or so ideologically loaded that it ought to be discarded, or that it is a distinction without a difference."); Sagers, *supra* note 31, at 56–57 (discussing the "line-drawing problem of the public-private distinction"). For a discussion of the benefits of well-structured collaborations between the public and private spheres, see generally JOHN D. DONAHUE & RICHARD J. ZECKHAUSER, COLLABORATIVE GOVERNANCE: PRIVATE ROLES FOR PUBLIC GOALS IN TURBULENT TIMES (2011).

[37] *See supra* note 6.

[38] *See supra* notes 15–17 and accompanying text.

insources the extra-constitutional norms that governed the collection of that information in the first instance. As a result, the government becomes less accountable to the people for its surveillance practices and the Constitution is rendered largely peripheral. The same effect occurs when a government agent signs a contract transferring sovereign power to a private actor who functions outside the boundaries of the Constitution. Considered together, therefore, insourcing and outsourcing provide a platform for pondering a broader constitutional architecture for privatization.

A. OUTSOURCING TO THE PRIVATE SECTOR

The government has long relied on the private sector to perform tasks ranging from public infrastructure development to policymaking.[39] But today, the government simply could not function without private contractors. This is a consequence of hiring caps on federal employees, a desire for flexibility, the need for short-term "surge capacity," and a lack of in-house expertise.[40] From 2000–2014, the federal government paid over $6 trillion to private contractors.[41] They formulate federal policy, interpret laws, administer foreign aid, manage nuclear weapons sites, interrogate detainees, and control borders.[42] The federal

---

[39] *See* Harold Bruff, *Public Programs, Private Deciders: The Constitutionality of Arbitration in Federal Programs*, 67 TEX. L. REV. 441, 460–61 (1989) (describing longstanding examples of private parties making law such as "[a]ncient doctrines of property and contract [that] allow . . . restrictive covenants on land," government authorized collective bargaining, homeowners' associations, and "the formation of special taxing districts by petition of some residents in a territory, against the wishes of the others").

[40] *See* ACQUISITION ADVISORY PANEL, REPORT OF THE ACQUISITION ADVISORY PANEL TO THE OFFICE OF FEDERAL PROCUREMENT POLICY AND THE UNITED STATES CONGRESS 393 (2007) (listing these factors as prompting federal agencies to increase the use private contracting); *see also* JOHN D. DONAHUE, THE PRIVATIZATION DECISION: PUBLIC ENDS, PRIVATE MEANS 4–5 (1989) (describing the rise of privatization in the 1980s).

[41] *Total Federal Spending*, USASpending.gov, http://www.usaspending.gov/trends?trendreport=default&viewreport=yes&maj_contracting_agency_t=&pop_state_t=&pop_cd_t=&vendor_state_t=&vendor_cd_t=&psc_cat_t=&tab=Graph+View&Go.x=Go (last visited Feb. 14, 2015).

[42] *See* Laura A. Dickinson, *Government for Hire: Privatizing Foreign Affairs and the Problem of Accountability Under International Law*, 47 WM. & MARY L. REV. 135, 138 (2005) (discussing the privatization of foreign affairs); Jody Freeman, *The Private Role in Public Governance*, 75 N.Y.U. L. REV. 543, 551–52 (2000) (discussing the pervasiveness of private actors in "regulation, service provision, policy design, and implementation").

government even hires private contractors to find and supervise other private contractors.[43]

Private industry performs government intelligence functions on an eye-popping scale.[44] Telecommunications companies have granted "the NSA complete access to their powerful switching systems," built "classified communications networks for the NSA and the Pentagon," and provided sophisticated "information technology and analytical services to the NSA."[45] Snowden's former employer, Booz Allen Hamilton,[46] advises the government on operations coordination;[47] border, cargo, and transportation security;[48] as well as intelligence, counterintelligence, and counterterrorism,[49] with "more than 1,000 analysts working . . . in research, analyses, case investigation, and operational activities."[50] Academi—the company formerly known as Blackwater—has received over a billion dollars in government contracts[51] for tasks ranging from tactics and weapons training for military, government, and law enforcement agencies;[52] to high-risk protection of sensitive

---

[43] Dana Priest & William M. Arkin, *National Security Inc.*, WASH. POST, July 20, 2010, at A8 (noting that the Department of Homeland Security uses nineteen private staffing companies to help it find other private contractors).

[44] *See generally* KATERI CARMOLA, PRIVATE SECURITY CONTRACTORS AND NEW WARS: RISK, LAW, AND ETHICS (2010) (describing the structure of private military and security companies, the assumptions that underlie their popularity, and how they might be regulated).

[45] TIM SHORROCK, SPIES FOR HIRE: THE SECRET WORLD OF INTELLIGENCE OUTSOURCING 305–08 (2008); *see also* David A. Sklansky, *The Private Police*, 46 UCLA L. REV. 1165, 1177 (1999) (discussing the private contracting of security).

[46] John Bacon, *Contractor Fires Snowden from $122,000-a-year Job*, USA TODAY, June 11, 2013, http://www.usatoday.com/sotry/news/nation/2013/06/11/booz-allen-snowden-fired/2411231/.

[47] *Government Management*, BOOZ ALLEN HAMILTON, http://www.boozallen.com/consultants/civilian-government/government-management (last visited Feb. 14, 2015).

[48] *Homeland Security*, BOOZ ALLEN HAMILTON, http://www.boozallen.com/consultants/civilian-government/homeland-security-consulting (last visited Feb. 14, 2015).

[49] *Law Enforcement*, BOOZ ALLEN HAMILTON, http://boozallen.com/consultants/civilian-government/law-enforcement-consulting (last visited Feb. 14, 2015).

[50] *Id.* In 2012, "98% of the company's $5.9 billion in revenue came from U.S. government contracts," and "[t]hree-fourths of its 25,000 employees [held] government security clearances." Bacon, *supra* note 46. For a detailed discussion of Booz Allen's deep influence on "every aspect of national security, from the military to the highest reaches of national intelligence," see SHORROCK, *supra* note 45, at 40, 38–71.

[51] Editorial, *Blackwater's Rich Contracts*, N.Y. TIMES, Oct. 3, 2007, http://www.nytimes.com/2007/10/03/opinion/03iht-edblack.1.7733227.html.

[52] *See* James Dao, *Attack Turns Spotlight on Private Security Firms*, REG.-GUARD, Apr. 2, 2004, at A2 (noting that Navy SEALs and police units use Blackwater for training). *See*

installations abroad, including CIA offices.[53] After the 2012 attack on the U.S. diplomatic compound in Benghazi, Libya, the budget for the Department of State (DOS) Bureau of Diplomatic Security ballooned to $2.7 billion for security protection plus $1.3 billion for embassy security, construction, and maintenance.[54] According to a report of the Congressional Research Service, of the 36,000 people employed by the Bureau, 90% are private contractors.[55] In addition, DOS employs 32,000 local guards under personal service agreements or as subcontractors to firms under contract with the federal government,[56] enabling "the Executive [to] direct broad swaths of intelligence policy without having to seek ex ante authorization or submit to meaningful oversight."[57]

Upwards of 480,000 federal contractors[58] and nearly five million federal employees have top-secret security clearances, which private contractors are largely responsible for processing.[59] The company USIS conducted clearances for Edward Snowden[60] and Aaron Alexis, the Navy Yard shooter who obtained a secret-level security clearance for his job with a government contractor in

---

generally Blackwater Worldwide, N.Y. TIMES, http://topics.nytimes.com/top/news/business/companies/blackwater_usa/index.html (last visited Feb. 14, 2015) (providing index of articles about Blackwater).

[53] *See* Mark Mazzetti, *Blackwater Loses a Job for the C.I.A.*, N.Y. TIMES, Dec. 11, 2009, at A8, *available at* http://www.nytimes.com/2009/12/12/us/politics/12blackwater.html?ref=blackwaterusa (discussing a few examples of Blackwater's security contracts with the CIA).

[54] Mark Walker, *Private Security Contractors' Military Role Under Scrutiny*, U-T SAN DIEGO, Aug. 31, 2013, http://www.utsandiego.com/news/2013/Aug/31/private-security-contractors-military-role-under/3/?#article-copy.

[55] *See id.* (noting that nine out of ten are private contractors). This is a function of cost. Outsourcing security at the U.S. Embassy in Baghdad costs less than a tenth of what it would cost the government to staff it directly. *See id.* (comparing $858 million to $78 million).

[56] *Id.*

[57] Michaels, *supra* note 12, at 904; *see also id.* at 924, 926–27, 934 (explaining that informally created intelligence relationships leave Congress unable to provide oversight).

[58] Mark Hosenball, *Exclusive: NSA Contractor Hired Snowden Despite Concerns About Resume Discrepancies*, REUTERS (June 20, 2013, 8:52 PM), http://www.reuters.com/article/2013/06/21/us-usa-security-snowden-idUSBRE95K01J20130621.

[59] *See* Jia Lynn Yang & Matea Gold, *Contractor that Vetted Snowden Says It Also Ran Background Check for Navy Yard Shooter*, WASH. POST, Sept. 19, 2013, http://articles.washingtonpost.com/2013-09-19/business/42214893_1_security-clearance-usis-background (noting that USIS handles 45% of all background checks for the Office of Personnel Management).

[60] Dion Nissenbaum, *Company That Vetted Snowden Defends Work*, WALL ST. J., Aug. 28, 2013, http://online.wsj.com/news/articles/SB10001424127887324324404579041350132655752.

2007.[61] With 7,000 employees, USIS handles 45% of all background checks ordered by the United States Office of Personnel Management.[62] In October of 2013, the Department of Justice (DOJ) joined a whistle-blower lawsuit alleging that USIS violated the False Claims Act by automatically releasing incomplete background checks and billing the U.S. government for work it did not perform.[63]

Perhaps unsurprisingly, outsourcing has been critiqued as "paving the way for private contractors to abuse their discretion, evade oversight, and generate unanticipated cost overruns."[64] Jon Michaels has argued that privatization strains the separation of powers by affording the executive branch "greater unilateral discretion—at the expense of the legislature, the judiciary, the people, and successor administrations."[65] Of course, privatization is here to stay, regardless of its merits. And it is taking on new forms that are more difficult for the public to identify and question, let alone dismantle.

B. INSOURCING THROUGH PRIVATE SECTOR DATA ENHANCEMENT

Before the rise of the Internet and big data, government surveillance was conducted in real time by traditional methods that involved fewer partnerships with the private sector than exist today.[66] With modern data mining, the latter form of intelligence

---

[61] Yang & Gold, *supra* note 59. Alexis was an information technology contractor for The Experts, Inc., a subcontractor to Hewlett-Packard, which was under contract with the Navy and Marine Corps to update and replace technology at numerous military installations. Carol D. Leonnig, Matea Gold & Tom Hamburger, *Military's Background Check System Failed to Block Gunman with a History of Arrests*, WASH. POST, Sept. 17, 2013, http://articles.washingtonpost.com/2013-09-17/politics/42132771_1_security-clearance-military-contractor-installations.

[62] Yang & Gold, *supra* note 59.

[63] Evan Perez, *Justice Department Joins Lawsuit on Company's Background Checks*, CNN (Oct. 30, 2013, 4:43 PM), http://www.cnn.com/2013/10/30/us/contractor-background-checks-lawsuit/.

[64] Jon D. Michaels, *Privatization's Pretensions*, 77 U. CHI. L. REV. 717, 718 (2010) (citing Freeman & Minow, *supra* note 29, *in* GOVERNMENT BY CONTRACT: OUTSOURCING AND AMERICAN DEMOCRACY, *supra* note 18, at 1–6).

[65] *Id.* at 719.

[66] For a discussion of historical clandestine surveillance techniques, from " 'mobile surveillance,' " which is "conducted primarily by foot, automobile, or airplane" to "track[ ] a person or other moving target" to "more exotic systems" developed in the late twentieth-

gathering—third party sourcing—is eclipsing the former. Because constitutional jurisprudence and existing legislative accountability schemes evolved to address traditional methods, they are a poor fit for the privacy challenges posed by modern surveillance through big data mining.[67]

1. Government Surveillance Through the Twentieth Century. In early colonial history, little was done by way of government surveillance.[68] Most communities relied on lay members to keep order.[69] In the seventeenth century, the king or the governor appointed sheriffs for larger populations.[70] Because they charged fees for their work, sheriffs focused on income-generating activities such as tax collection, serving subpoenas, and operating the jail, rather than on law enforcement.[71] Their activities were primarily reactive—they addressed problems in response to complaints rather than preventing or investigating crime.[72]

Government surveillance did not begin in earnest until the nineteenth century, when American cities faced increased crime from population growth, ethnic and racial tensions, and economic failures.[73] In 1861, Abraham Lincoln appointed the first secret service agent, a private detective who went on to institutionalize the practice of profiling criminals using posters and photographs during the Civil War.[74] Although technology was limited at that time, the invention of the telegraph in 1844 and the telephone in

---

century, see ROBERT WALLACE & H. KEITH MELTON, SPYCRAFT: THE SECRET HISTORY OF THE CIA'S SPYTECHS FROM COMMUNISM TO AL-QAEDA 401–02, 416 (2008).

[67] *See* Slobogin, *supra* note 16, at 321 ("Current Fourth Amendment jurisprudence appears to leave data mining completely unregulated . . . .").

[68] *See infra* note 73 and accompanying text (noting that government surveillance began in the nineteenth century).

[69] *See* LAWRENCE FRIEDMAN, CRIME AND PUNISHMENT IN AMERICAN HISTORY 68 (1993) ("The creation of police forces was another landmark . . . in the long, slow retreat of lay justice.").

[70] James Geistman, *Sheriffs*, *in* THE SOCIAL HISTORY OF CRIME AND PUNISHMENT IN AMERICA: AN ENCYCLOPEDIA 1663 (Wilbur R. Miller ed., 2012).

[71] *Id.*; Craig D. Uchida, *History of American Policing*, *in* 1 THE ENCYCLOPEDIA OF POLICE SCIENCE 617 (Jack R. Greene ed., 3d ed. 2007).

[72] Uchida, *supra* note 71.

[73] CHRISTIAN PARENTI, THE SOFT CAGE: SURVEILLANCE IN AMERICA FROM SLAVERY TO THE WAR ON TERROR 35–36 (2003); Uchida, *supra* note 71, at 617–18 (describing the development of the first American police departments in response to civil disorder in nineteenth century cities).

[74] J.K. PETERSEN, HANDBOOK OF SURVEILLANCE TECHNOLOGIES 24 (3d ed. 2012).

1876 made surveillance easier.[75] Investigators used simple telescopes or bribed telephone and telegraph operators to eavesdrop.[76] With the advent of the hand-held camera in 1884, photography became a more accessible surveillance tool.[77] The use of mug shots, body measurements, and police files for identification purposes—a method called "Bertillonage" after its French inventor, Alphonse Bertillon—evolved and spread.[78]

By the early 1900s, the federal government used secret operatives, including private organizations, to conduct investigations.[79] Federal and state law enforcement authorities began compiling fingerprint repositories.[80] The Bureau of Investigations—now the FBI—became an official part of the Department of Justice.[81] The federal government began collecting personal financial information and other data on tax returns.[82] During World War I, surveillance technologies such as code-breakers, magnifying devices, and submarines equipped with airship detection equipment were deployed to protect national interests.[83] After the war, law enforcement began to rely heavily on wiretapping to monitor social unrest.[84]

---

[75] DANIEL J. SOLOVE, MARC ROTENBERG & PAUL M. SCHWARTZ, PRIVACY, INFORMATION, AND TECHNOLOGY 64 (2006).

[76] PETERSEN, *supra* note 74, at 30.

[77] *See* Susan W. Brenner, *The Fourth Amendment in an Era of Ubiquitous Technology*, 75 MISS. L.J. 1, 32–33 (2005) (noting how the hand-held camera made eavesdropping simple and popular); PARENTI, *supra* note 73, at 36–38 (discussing law enforcement's use of photographs in the nineteenth century).

[78] PARENTI, *supra* note 73, at 43–45.

[79] PETERSEN, *supra* note 74, at 30; JENNIFER FRONC, NEW YORK UNDERCOVER: PRIVATE SURVEILLANCE IN THE PROGRESSIVE ERA 146 (2009) ("During the war, as a consequence of and in response to the weakness of federal police mechanisms, private organizations were either deputized by agencies of the government or deputized themselves to fill the gaps in the policing system . . . [by] conduct[ing] undercover investigations of prostitutes, immigrants, 'slackers' who failed to register for the draft, and radicals.").

[80] PARENTI, *supra* note 73, at 51–53; PETERSEN, *supra* note 74, at 30.

[81] PETERSEN, *supra* note 74, at 30.

[82] *See* U.S. CONST. amend. XVI ("The Congress shall have power to lay and collect taxes on incomes, from whatever source derived, without apportionment among the several States, and without regard to any census or enumeration."); *see also* I.R.C. § 601 (1970) (repealed 1976) (giving tax deductions to bank affiliates). Law enforcement access to tax records is limited. *See* I.R.C. § 6103(d)(1) (2012) (allowing disclosure to enforce tax laws); *id.* § 6103(h)(4)(D), (i)(1)(A) (authorizing disclosure by court order).

[83] PETERSEN, *supra* note 74, at 30–31.

[84] SOLOVE, ROTENBERG & SCHWARTZ, *supra* note 75, at 64; *see* Erin Murphy, *The Politics of Privacy in the Criminal Justice System: Information Disclosure, the Fourth Amendment,*

During the 1930s and the 1940s, the government expanded routine collection of data on American citizens.[85] The first social security number was issued through the U.S. Postal Service in 1936,[86] and became linked to property ownership, residence histories, medical records, and other public transactions that the government could use to profile individuals.[87] During World War II, Western Union forwarded all international cables to United States intelligence personnel.[88] The National Security Council and the Central Intelligence Agency (CIA) were created to handle national security and intelligence matters.[89] The FBI's jurisdiction was extended to include background checks of federal employees.[90]

In the 1950s, television, radio, and telephone technology improved substantially.[91] State and local government agents routinely eavesdropped on unsuspecting subjects—often in cooperation with local phone companies.[92] Physicists and astronomers developed knowledge that was later applied to orbiting satellite technology.[93] Under President Truman, national responsibility for communications intelligence shifted to the NSA, and surveillance policies were revised to address the Cold War threat of communist expansion.[94] The CIA, at the direction of President Eisenhower, contracted with Lockheed Corporation,

---

and Statutory Law Enforcement Exemptions, 111 MICH. L. REV. 485, 503 n.72 (2013) (noting that the "law outlawing wiretapping" expired at the end of World War I). For a discussion of wiretap legislation, see *infra* Part III and SOLOVE, ROTENBERG & SCHWARTZ, *supra* note 75, at 83–91.

[85] *See infra* notes 86–90 and accompanying text.

[86] *Social Security Numbers*, SOCIAL SECURITY, http://www.ssa.gov/history/ssn/firstcard.html (last visited Feb. 15, 2015).

[87] *See* PARENTI, *supra* note 73, at 84–87 (explaining the development of the social security system and how linking personal information to social security numbers quietly reduced Americans' privacy); William H. Minor, *Identity Cards and Databases in Health Care: The Need for Federal Privacy Protections*, 28 COLUM. J.L. & SOC. PROBS. 253, 260–66 (1995) (discussing the development of the social security system and the privacy concerns it creates).

[88] Michaels, *supra* note 12, at 914. *See generally* THOMAS F. TROY, DONOVAN AND THE CIA: A HISTORY OF THE ESTABLISHMENT OF THE CENTRAL INTELLIGENCE AGENCY (1981) (detailing the history of the CIA through the post-World War II years).

[89] PETERSEN, *supra* note 74, at 36.

[90] *Id.*

[91] *Id.* at 39.

[92] Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9, 12 (2004) (citing SAMUEL DASH ET AL., THE EAVESDROPPERS (1959)).

[93] PETERSEN, *supra* note 74, at 37.

[94] *Id.* at 38.

General Electric, Eastman Kodak, and other companies to build spy planes and other technologies with unprecedented surveillance capabilities "that could see behind the Iron Curtain to measure the strength of Soviet military forces and detect preparations for a surprise attack."[95]

In the 1960s, civil rights turbulence, increased use of recreational drugs, and fear of nuclear proliferation fueled public demand for enhanced foreign and domestic surveillance.[96] Night vision devices enabled long-range military surveillance,[97] aerial mapping cameras allowed for precision topographical photography,[98] and infrared sensors evolved.[99] The CIA developed the capacity to build 3D models of foreign terrain, buildings, and weapons using surveillance photos and intelligence data.[100] Bar codes were in regular use by 1967.[101]

In the 1970s, the Watergate scandal made illegal investigative surveillance and wiretapping a headline issue.[102] The Director of the NSA admitted to Congress in 1975 that the agency "systematically intercepts international communications, both voice and cable," and acknowledged that domestic conversations were captured incidentally, as well.[103] Documents disclosed in 2013 by Edward Snowden reveal that global communications providers began voluntarily handing over customer data to the

---

[95] PHILIP TAUBMAN, SECRET EMPIRE: EISENHOWER, THE CIA, AND THE HIDDEN STORY OF AMERICA'S SPACE ESPIONAGE, at xi (2003); *see also* SHORROCK, *supra* note 45, at 74 (noting the Eisenhower Administration's contracts as historical examples of outsourcing intelligence).

[96] *See* LOUIS FISHER, THE CONSTITUTION AND 9/11: RECURRING THREATS TO AMERICA'S FREEDOMS 286–87 (2008) (noting the national security response to domestic and foreign threats in the 1960s and early 1970s); PETERSEN, *supra* note 74, at 39 (discussing how the social, political, and international climate of the 1960s influenced public opinion towards national security).

[97] Melvin Gutterman, *A Formulation of the Value and Means Models of the Fourth Amendment in the Age of Technologically Enhanced Surveillance*, 39 SYRACUSE L. REV. 647, 678 & n.162 (1988).

[98] *See* Dow Chem. Co. v. United States, 476 U.S. 227, 242 & n.4 (1986) (describing sophisticated equipment used by the Environmental Protection Agency (EPA) to aerially photograph Dow Chemical's facility).

[99] *See* PETERSEN, *supra* note 74, at 438.

[100] *Id.* at 39.

[101] PARENTI, *supra* note 73, at 99.

[102] PETERSEN, *supra* note 74, at 42–43.

[103] *Id.* at 43 (quotation marks omitted).

government in the 1970s, often for hefty fees.[104] The first commercially viable personal computer was introduced in 1975.[105] Computer hackers emerged with the expertise to overtly break into others' computers, including government systems.[106] Magnetic strip technology became readily available for credit card use, and by 1972 "a fully operational network of interconnected computer databanks" was under development in order to "facilitate almost instant credit and background checks."[107] Marketers discovered that data from white and yellow pages, driver's license records, and voter registration cards could be compiled, bought, and sold.[108]

The Internet evolved in the 1980s as a medium for military communications amongst a finite group of government, academic, and computer professionals.[109] After a suicide bomb attack in 1983 left 241 Marines dead in Beirut, the Reagan Administration coined a new phrase, "war against terrorism."[110] The Internet's rapid circulation of information enabled unprecedented opportunities for collaboration amongst law enforcement entities and increased public scrutiny of government surveillance activities, which expanded through the 1990s.[111]

By the mid-1990s, private organizations such as museums, service stations, department stores, grocery stores, and schools routinely installed motion detectors and visual surveillance systems.[112] Digital camcorders and global positioning systems came on the commercial market.[113] Government began to rely

---

[104] Craig Timberg & Barton Gellman, *NSA Paying U.S. Companies for Access to Communications Networks*, WASH. POST, Aug. 29, 2013, http://www.washingtonpost.com/world/national-security/nsa-paying-us-companies-for-access-to-communications-networks/2013/08/29/5641a4b6-10c2-11e3-bdf6-e4fc677d94a1_story.html.

[105] PETERSEN, *supra* note 74, at 43.

[106] *Id.* at 44.

[107] PARENTI, *supra* note 73, at 96.

[108] *See* JULIE ANGWIN, DRAGNET NATION: A QUEST FOR PRIVACY, SECURITY, AND FREEDOM IN A WORLD OF RELENTLESS SURVEILLANCE 30 (2014) (discussing how the rise of modern computing facilitated the buying and selling of personal data).

[109] PETERSEN, *supra* note 74, at 50, 50–52.

[110] SHANE HARRIS, THE WATCHERS: THE RISE OF AMERICA'S SURVEILLANCE STATE 3, 30, 32 (2010).

[111] *Id.* at 60.

[112] *Id.* at 53.

[113] *Id.* at 56.

increasingly on technological developments from the commercial sector for its own surveillance.[114]

2. Twenty-First Century Surveillance and the Private Sector. The first decade of the twenty-first century saw additional growth in computerized communication, with a shift towards a global economy based on the collection, sharing, and analysis of infinite amounts of information.[115] The transition from analog to digital technology in 2009[116] meant that telephone communications were no longer conducted on dedicated paths between two parties. Multiple communications could instead occur on a single line by breaking them down into pieces—or "packets"—and reassembling them at the destination.[117] These "digital trail[s]"[118] of activity could be stored relatively cheaply.[119] As a consequence, government monitoring became "less about analog surveillance and more a matter of 'data mining.' "[120]

Today, the amount of globally available data is staggering. Phone companies, social networking and dating sites, online retailers, Internet service providers, publicly available satellite systems, financial institutions, and credit agencies collectively possess "trillions if not quadrillions-plus bits of information," much of it voluntarily disclosed by individuals as a condition to using a product or service.[121] A CNN reporter bluntly described the data trail created by logging onto the Internet each day:

---

[114] Richards, *supra* note 11, at 1958 ("One of the most significant changes that the age of surveillance has brought about is the increasing difficulty of separating surveillance by governments from that by commercial entities.").

[115] *See* ERIC SCHMIDT & JARED COHEN, THE NEW DIGITAL AGE: RESHAPING THE FUTURE OF PEOPLE, NATIONS AND BUSINESS 4 (2013) ("In the first decade of the twenty-first century the number of people connected to the Internet worldwide increased from 350 million to more than 2 billion. In the same period, the number of mobile-phone subscribers rose from 750 million to well over 5 billion (it is now over 6 billion).").

[116] *See* Digital Television Transition and Public Safety Act of 2005, Pub. L. No. 109-171, §§ 3001–3009, 120 Stat. 4, 21–27 (2006) (terminating all licenses and requiring the cessation of broadcasting by full-power stations in the analog television services).

[117] PATRICIA MOLONEY FIGLIOLA, RESEARCH SERV. RL30677, DIGITAL SURVEILLANCE: THE COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT 2 (2008).

[118] Will Thomas DeVries, *Protecting Privacy in the Digital Age*, 18 BERKELEY TECH. L.J. 283, 292 (2003).

[119] Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. PA. L. REV. 373, 375–76 (2014).

[120] DeVries, *supra* note 118, at 292.

[121] Frida Ghitis, *Google Knows Too Much About You*, CNN (Feb. 9. 2012, 2:58 PM), http://www.cnn.com/2012/02/09/opinion/ghitis-google-privacy/.

> Google has every e-mail you ever sent or received on Gmail. It has every search you ever made, the contents of every chat you ever had over Google Talk. It holds a record of every telephone conversation you had using Google Voice, it knows every Google Alert you've set up. It has your Google Calendar with all content going back as far as you've used it, including everything you've done every day since then. It knows your contact list with all the information you may have included about yourself and the people you know. It has your Picasa pictures, your news page configuration, indicating what topics you're most interested in. And so on.
>
> If you ever used Google while logged in to your account to search for a person, a symptom, a medical side effect, a political idea; if you ever gossiped using one of Google's services, all of this is on Google's servers. And thanks to the magic of Google's algorithms, it is easy to sift through the information because Google search works like a charm. Google can even track searches on your computer when you're not logged in for up to six months.[122]

The government has tapped into private corporations' gargantuan storehouses of data for years.[123] Under a secret executive order issued by President George W. Bush after 9/11,

---

[122] *Id.*; *see also* DAVID KIRKPATRICK, THE FACEBOOK EFFECT: THE INSIDE STORY OF THE COMPANY THAT IS CONNECTING THE WORLD 323–28 (2010) (comparing Google with Facebook, which it describes as having a "vision of providing a universal identity system for everyone on the Internet"). *See generally* STEVEN LEVY, IN THE PLEX: HOW GOOGLE THINKS, WORKS, AND SHAPES OUR LIVES 315–67 (2011) (discussing Google's influence on American politics and government); SIVA VAIDHYANATHAN, THE GOOGLIZATION OF EVERYTHING (AND WHY WE SHOULD WORRY) 3–4 (2011) (discussing Google's global impact and negative effects on "the pursuit of global civic responsibility and the public good").

[123] *See* DAVID K. SHIPLER, THE RIGHTS OF THE PEOPLE: HOW OUR SEARCH FOR SAFETY INVADES OUR LIBERTIES 247 (2011) ("Most personal electronic information is in private hands, and savvy entrepreneurs manage it for profit by selling the data to retailers of all stripes. The government can buy it, too, and since 9/11 various proposals for using it have generated a blizzard of collection programs."); Ohm, *supra* note 13, at 1324–25 (observing that data mining has muted traditional surveillance methods like court-ordered wiretaps and physically tailing suspects); Richards, *supra* note 11, at 1940–41 (discussing the complex entanglement between government surveillance and private business).

telecommunications companies such as AT&T, Verizon, and BellSouth granted senior NSA officials' oral requests for warrantless access to switches carrying domestic telephone calls, which led to the creation of a massive database of information regarding individual calling habits.[124] Much of the government's data now comes from large-scale commercial data brokers such as Thompson Reuters' CLEAR[125] and LexisNexis' Accurint[126] that collect information from private sources for government purchase.[127] A 2008 report by the United States Government Accountability Office (GAO) stated that the Department of Homeland Security (DHS), DOJ, DOS, and the Social Security Administration "used personal information obtained from [such] resellers for . . . criminal investigations, locating witnesses and fugitives, researching assets held by individuals of interest, and detecting prescription drug fraud" at a cost of approximately $30 million that year.[128] The purchased information included "birth

---

[124] Risen & Lichtblau, *supra* note 2; Leslie Cauley, *NSA Has Massive Database of Americans' Phone Calls*, USA TODAY (May 11, 2006, 10:38 AM), http://usatoday30.usatoday.com/news/washington/2006-05-10-nsa_x.htm.

[125] CLEAR, https://clear.thomsonreuters.com/clear_home/government.htm# (last visited Feb. 15, 2015).

[126] LEXIS NEXIS, http://www.lexisnexis.com/government/solutions/investigative/accurint.aspx (last visited Feb. 15, 2015).

[127] Michaels, *supra* note 12, at 918; *see also* David Gray, Danielle Keats Citron & Liz Clark Rinehart, *Fighting Cybercrime After* United States v. Jones, 103 J. CRIM. L. & CRIMINOLOGY 745, 785 (2013) ("[S]ocial networking sites, merchants, and data brokers record and analyze our digital footprints . . . for immediate commercial gain . . . . Some package the information into 'digital dossiers,' which they sell to government and private clients. Law enforcement and other government officials routinely contract with these data brokers or directly request or subpoena information about our online activities from ISPs, e-mail providers, and search engines." (citing DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 2 (2004))); Bruce Schneier, *Do You Want the Government Buying Your Data from Corporations?*, THE ATLANTIC (Apr. 30, 2013, 1:25 PM), http://www.theatlantic.com/technology/archive/2013/04/do-you-want-the-government-buying-your-data-from-corporations/275431/ ("Sometimes [government agencies] simply purchase [privately-held data], just as any other company might.").

[128] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-08-543T, PRIVACY: GOVERNMENT USE OF DATA FROM INFORMATION RESELLERS COULD INCLUDE BETTER PROTECTIONS (2008), *available at* http://www.gao.gov/assets/120/119298.pdf. The term "resellers" refers to "businesses that vary in many ways but have in common collecting and aggregating personal information from multiple sources and making it available to their customers." *Id.* at 5. The National Counterterrorism Center—which is part of the Office of the Director of National Intelligence, *National Counterterrorism Center*, OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, http://www.dni.gov/index.php/about/organization/national-counte

and death records, property records, motor vehicle and voter registrations, criminal records, and civil case files . . . telephone directories, business directories, classified ads or magazines, Internet sites, and other sources accessible by the general public" but not readily available, as well as "[n]onpublic information derived from proprietary or nonpublic sources, such as credit header data, product warranty registrations, and other application information provided to private businesses directly by consumers."[129] The government also accesses a network of over sixty "fusion centers" developed after the 9/11 attacks, which share intelligence information amongst local, state, and federal law enforcement as well as private contractors.[130]

Until recently, the NSA's surveillance programs collected two types of privately-sourced data, which the agency then mines for patterns and trends.[131] The first is metadata, which "includes highly revealing information about the times, places, devices and participants in electronic communication, but not its contents."[132] The Foreign Intelligence Surveillance Court's[133] Verizon order, made public in June of 2013, covered this kind of data—the so-called "envelope" of a customer phone call, including the date and

---

rterrorism-center-who-we-are (last visited Feb. 15, 2015)—uses such data for surveillance, as well. Gray, Citron & Rinehart, *supra* note 127, at 786.

[129] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-08-543T, *supra* note 134, at 6 (footnote omitted).

[130] *State and Major Urban Area Fusion Centers*, U.S. DEPARTMENT OF HOMELAND SECURITY, http://www.dhs.gov/state-and-major-urban-area-fusion-centers (last visited Feb. 15, 2015). A 2012 report by a congressional subcommittee assailed them as "pools of Ineptitude, waste and civil liberties intrusions," according to one journalist. Robert O'Harrow, Jr., *DHS "Fusion Centers" Portrayed as Pools of Ineptitude and Civil Liberties Intrusions*, WASH. POST, Oct. 2, 2012, http://www.washingtonpost.com/investigations/dhs-fusion-centerportrayed-as-pools-of-ineptitude-and-civil-liberties-intrusions/2012/10/02/10014440-0cbl-11e2-bdla-b868e65d57eb_story.html.

[131] *See* Barton Gellman, *U.S. Surveillance Architecture Includes Collection of Revealing Internet, Phone Metadata*, WASH. POST, June 15, 2013, http://www.washingtonpost.com/investigations/us-surveillance-architecture-includes-collection-of-revealing-internet-phone-metadata/2013/06/15/e9bf004a-d511-11e2-b05f-3ea3f0e7bb5a_story.html (describing two collection programs for metadata and two collection programs for content).

[132] *Id. See generally* PATRICIA MOLONEY FIGIOLA, RESEARCH SERV. RL30677, DIGITAL SURVEILLANCE: THE COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT 1–2 (2008) (explaining that modern technology has blurred the traditional distinction between the interception of communication content and the acquisition of identification information).

[133] The Foreign Intelligence Surveillance Court is established by the Foreign Intelligence Surveillance Act of 1978. 50 U.S.C. §§ 1801–1885 (2012); *see id.* § 1803 (establishing the court).

time of a call, its duration, the telephone numbers involved, and location of the participants.[134]

The second type of NSA data collection involves the content of communications.[135] Also in June of 2013, the press revealed that the government through the PRISM program was "tapping directly into the central servers of nine leading U.S. Internet companies, extracting audio and video chats, photographs, e-mails, documents, and connection logs that enable analysts to track" a person's movements and contacts over time.[136] It was later reported that the NSA has also collected "upstream" Internet data,[137] which is traffic sent from a computer or network—such as uploaded files or multiplayer game data in real time—as distinct from "downstream" data received by a computer or network.[138]

---

[134] Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, THE GUARDIAN (June 6, 2013, 7:04 PM), http://www.theguardian.com/world/interactive/2013/jun/06/verizon-telephone-data-court-order.

[135] *See supra* note 131 and accompanying text.

[136] Barton Gellman & Laura Poitras, *U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, WASH. POST, June 7, 2013, at A1, A12, *available at* http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-braod-secret-program-2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html; Glen Greenwald & Ewen MacAskill, *NSA Prism Program Taps in to User Data of Apple, Google and Others*, THE GUARDIAN (June 6, 2013, 3:23 PM), http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

[137] Laura K. Donohue, *Section 702 and the Collection of International Telephone and Internet Content*, 38 HARV. J.L. & PUB. POL'Y 117, 120 (2014) (citing James Ball, *NSA's Prism Surveillance Program: How It Works and What It Can Do*, THE GUARDIAN (June 8, 2013, 1:56 PM), http://www.theguardian.com/world/2013/jun/08/nsa-prism-server-collection-facebook-google); FISC Ct., Mem. Op. & Order, at 30 (Oct. 3, 2011), *available at* https://www.aclu.org/files/assets/fisc_opinion_10.3.2011.pdf. The Obama Administration publicly confirmed the existence of both programs. *See* Press Release, Shawn Turner, Dir. of Pub. Affairs, Office of the Dir. of Nat'l Intelligence, DNI Declassifies Intelligence Community Documents Regarding Collection Under Section 702 of the Foreign Intelligence Surveillance Act (FISA) (Aug. 21, 2013), *available at* http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/915-dni-declassifies-intelligence-community-documents-regarding-collection-under-section-702-of-the-foreign-intelligence-surveillance-act-fisa ("President Obama requested that the [NSA] declassify and make public as much information as possible about certain sensitive NSA programs . . . .").

[138] DOUGLAS DOWNING, MICHAEL COVINGTON & MELODY MAULDIN COVINGTON, DICTIONARY OF COMPUTER AND INTERNET TERMS 154, 535 (9th ed. 2006). Orin Kerr draws the distinction between prospective surveillance—the "capture [of] future communications that have not yet been sent over the network," such as wiretapping—and retrospective surveillance, where the government looks for past communications that are stored in a network. Orin S. Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 607, 616 (2003). He also characterizes this distinction as direct versus indirect surveillance. *Id.* at 621.

The NSA amassed more than 13.25 million upstream transactions in the first six months of 2011.[139] In exchange for the data, it paid U.S. companies a total of $394 million dollars that fiscal year.[140] According to one telecommunications executive, these "voluntary agreements simplify the government's access to surveillance."[141]

The NSA's computers analyze the information it collects for suspicious patterns and so-called "communities of interest"—people in contact with persons of interest overseas.[142] Although traditional database systems required analysts to build and rebuild statistical models after pouring over search results for hours, modern "machine learning" or "cognitive analytics"[143] methods apply algorithms to find patterns and meaning based on context; the algorithms then fine-tune themselves in an iterative process that proceeds without "any significant human intervention."[144] As a result, the government's intelligence capability is cheaper, faster, more powerful—and more elusive—than ever before.[145] By making correlations amongst infinite bits

---

[139] Donohue, *supra* note 137, at 121.

[140] Timberg & Gellman, *supra* note 104. Several companies that have provided information to the NSA under PRISM reported to the *Washington Post* that they do not accept money for doing so. *Id.*

[141] *Id.*; *see also* Robert Lenzner, *ATT, Verizon, Sprint Are Paid Cash by NSA for Your Private Communications*, FORBES, Sept. 23, 2013, http://www.forbes.com/sites/robertlenzner/2013/09/23/attverizonsprint-are-paid-cash-by-nsa-for-your-private-communications/ ("The [NSA] pays AT&T, Verizon, and Sprint several hundred million dollars a year for access to 81% of all international phone calls into the US, according to [the Snowden disclosures]."). Many of these agreements are authorized by the Communications Assistance for Law Enforcement Act, 47 U.S.C. §§ 1001–1010 (2012). *See generally infra* notes 197, 241–44 and accompanying text.

[142] Steve Chenevey, *PRISM: Barack Obama Says 'Nobody Is Listening to Your Telephone Calls,'* ASSOCIATED PRESS, June 7, 2013, http://www.wjla.com/articles/2013/06/prism-barack-obama-says-nobody-is-listening-to-your-telephone-calls--89818.html.

[143] *See* Rajeev Ronanki & David Steier, *Cognitive Analystics, in* TECH TRENDS 2014: INSPIRING DISRUPTION 19, 21 (2014), *available at* http://d2mtr37y39tpbu.cloudfront.net/wp-content/uploads/2014/02/Tech-Trends-2014_FINAL-ELECTRONIC_single.2.24.pdf (classifying machine learning as one of three kinds of cognitive analytics).

[144] Steven M. Bellovin, Renée M. Hutchins, Tony Jebara & Sebastian Zimmeck, *When Enough Is Enough: Location Tracking, Mosaic Theory, and Machine Learning*, 8 N.Y.U. J.L. & LIBERTY 556, 590–91 (2014) (providing a scientific explanation of machine learning).

[145] *See* Michael Hickins, *U.S. News: How the NSA Could Get So Smart So Fast--Modern Computing Is Helping Companies and Governments Accurately Parse Vast Amounts of Data in a Matter of Minutes*, WALL ST. J., June 12, 2013, at A4, *available at* http://online.wsj.com/news/articles/SB10001424127887324049504578541271020665666 (explaining how the NSA can now efficiently parse quantities of data that were unimaginable five years ago); ZYGMUNT BAUMAN & DAVID LYON, LIQUID SURVEILLANCE: A CONVERSATION 5–6 (2013)

of data that are enriched by new technologies such as biometrics, high-resolution cameras, aerial vehicles, and DNA sampling,[146] the government can now track virtually anyone, anywhere, at any time. An internal presentation dated April 2013 for senior NSA analysts described PRISM as "the most prolific contributor to the President's Daily Brief, which cited PRISM data in 1,477 items [the prior] year."[147]

Scholars have identified a litany of harms that flow from unfettered government watching, including "self-censorship and inhibition,"[148] decreased civility in social relationships,[149] restricted freedom to associate with others,[150] and reduced accountability for those doing the monitoring.[151] When surveillance is automated, "the camera itself is not selective in whom it watches; and it provides a searchable record which trumps human memory in longevity, authority and accuracy."[152] Manual surveillance, by contrast, requires that the watcher identify a subject in advance and maintain some degree of proximity to him. When a machine collects the data, there are fewer opportunities for human interaction that would enable the subject to thwart the surveillance by hiding. Automation prevents

---

(describing the mutability of so-called "liquid surveillance," whereby "[s]urveillance power, as exercised by government departments, police agencies and private corporations . . . now appear[s] . . . in databases that may not even be 'in' the country in question").

146 PETERSEN, *supra* note 74, at 72–75, 743.

147 Gellman & Poitras, *supra* note 136.

148 ANITA L. ALLEN, UNPOPULAR PRIVACY: WHAT MUST WE HIDE? 172 (2011); *see also* SHIPLER, *supra* note 123, at 240–43 (discussing how the sensation of being watched affects behavior). This phenomenon was identified in an 1897 study in which the presence of other riders caused cyclists to pedal faster. Matthew Lynch, *Closing the Orwellian Loophole: The Present Constitutionality of Big Brother and the Potential for a First Amendment Cure*, 5 FIRST AMEND. L. REV. 234, 271 & n.136 (2007) (citing Norman Triplett, *The Dynamogenic Factors in Pacemaking and Competition*, 9 AM. J. PSYCHOL. 507, 533 (1898)).

149 *See* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 536–37 (2006) (describing how exposure may impede a person's ability to participate in society).

150 *See* ANGWIN, *supra* note 108, at 51–64 (asserting that government surveillance restricts freedom to associate through the internalization of censorship).

151 *See* Solove, *supra* note 149, at 508–09, 523 (explaining how data aggregation unsettles people's expectations and how excluding people from participation in their personal data reduces government accountability). *See generally* THE SURVEILLANCE STUDIES READER (Sean P. Hier & Joshua Greenberg eds., 2007) (collecting essays on topics such as how surveillance operates as a modern mechanism of social control and structures individual behavior and everyday life).

152 Kevin Macnish, *Unblinking Eyes: The Ethics of Automating Surveillance*, 14 ETHICS INFO. TECH. 151, 152 (2012).

the watcher from assessing "the realities on the ground," making "the possibility of negotiation, subtlety and discretion" less likely.[153] The subject of the surveillance becomes disempowered.[154]

Studies have also shown that the selection criteria programmed into automated systems is "overwhelmingly determined by age, ethnicity and sex."[155] For example, "people from different cultures, sexes and ages will behave differently in crowds."[156] If distinctive behaviors are built into an automated surveillance system, an innocent individual "could register as deviating from the norm" simply because she has a different cultural approach to personal space and tolerance for crowds than expected.[157] As a consequence, "[s]urveillance fosters suspicion in those who wield it."[158] The programmer's prejudices become "frozen into the code, effectively institutionalizing those values."[159]

Since the Snowden scandal broke, the dangers of ubiquitous government monitoring have become a frontline public issue. In announcing plans to amend NSA practices, President Obama acknowledged that the government's use of privately held data to track Americans is unprecedented and poses novel constitutional questions.[160] Google has urged customers to push for legislative reform.[161] The debate over technology's impact on personal privacy has thus moved beyond identification of the problem; the only salient question is what to do about it.

---

153 *Id.* at 164.

154 *Id.*

155 *See id.* at 152, 158 (explaining how the prejudice that "overwhelms" manual surveillance is often programmed into automated surveillance systems).

156 *Id.* at 159.

157 *Id.*

158 Kirstie Ball, Elizabeth Daniel, Sally Dibb & Maureen Meadows, *Democracy, Surveillance and "Knowing What's Good for You": The Private Sector Origins of Profiling and the Birth of "Citizen Relationship Management," in* SURVEILLANCE AND DEMOCRACY 111, 113 (Kevin D. Haggerty & Minas Samatas eds., 2010).

159 Macnish, *supra* note 152, at 158.

160 *Obama's Speech on N.S.A. Phone Surveillance*, N.Y. TIMES, Jan. 17, 2014, http://www.nytimes.com/2014/01/18/us/politics/obamas-speech-on-nsa-phone-surveillance.html?_r=0.

161 *Google Take Action: Demand Real Surveillance Reform*, GOOGLE, https://takeaction.withgoogle.com/page/s/usa-freedom-act?utm_medium=social&utm_source=twitter (last visited Feb. 17, 2015).

III. OUTSOURCING, DATA INSOURCING, AND LEGISLATIVE REGIMES

When private contractors and corporations perform public functions, they confront far fewer statutory and regulatory restrictions than do government actors engaged in identical activities.[162] Contractors exercising outsourced public powers are not governed by the procedural restrictions that bind identical government conduct. Likewise, federal law leaves largely unregulated the private sector's collection of personal information.[163] As a result, the government and the private sector are able to collaborate on intelligence gathering in ways that "evade oversight and, at times, . . . defy the law."[164] In this regard, outsourcing and data insourcing are of a piece.[165] The executive

---

[162] *See* Michaels, *supra* note 64, at 718–19 (calling government contracts or contract provisions that enable an outsourcing agency to achieve goals that would be difficult or impossible in the course of ordinary public administration "workarounds"). Enhanced regulation is one way of addressing the need for accountability, but it creates incentives to maximize informality in outsourcing relationships. *See* Michaels, *supra* note 12, at 943 ("[P]lacing more legal requirements between the Executive and its intelligence aims will likely intensify the Executive's thirst for informality.").

[163] Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. CAL. L. REV. 241, 255 (2007). As a service to the public, the Electronic Frontier Foundation has published a chart summarizing the voluntary policies of "Internet service providers, e-mail providers, mobile communications tools, telecommunications companies, cloud storage providers, location-based services, blogging platforms, and social networking sites" regarding cooperation with the government and public transparency, including whether a company requires a warrant before turning over the content of communications and whether it informs customers of the existence of government requests for information. NATE CARDOZO ET AL., WHO HAS YOUR BACK? PROTECTING YOUR DATA FROM GOVERNMENT REQUESTS: THE ELECTRONIC FRONTIER FOUNDATION'S FOURTH ANNUAL REPORT ON ONLINE SERVICE PROVIDERS' PRIVACY AND TRANSPARENCY PRACTICES REGARDING GOVERNMENT ACCESS TO USER DATA 4, 18 (2014), *available at* https://www.eff.org/files/2014/05/15/who-has-your-back-2014-govt-data-requests.pdf.

[164] Michaels, *supra* note 12, at 901. *See generally* James X. Dempsey & Lara M. Flint, *Commercial Data and National Security*, 72 GEO. WASH. L. REV. 1459 (2004). Many of the voluntary agreements under which communications companies work with the NSA are reportedly so sensitive that "only a handful of people in a company know of them, and they are sometimes brokered directly between chief executive officers and the heads of the U.S.'s major spy agencies," which have reportedly traded access to classified intelligence for cooperation. *See* Michael Riley, *U.S. Agencies Said to Swap Data with Thousands of Firms*, BLOOMBERG BUS. (June 14, 2013, 12:01 AM), http://www.bloomberg.com/news/2013-06-14/u-s-agencies-said-to-swap-data-with-thousands-of-firms.

[165] *See* Michaels, *supra* note 12, at 904 (observing that the use of private data for surveillance a form of " 'privatization' in the guise of informal intelligence agreements with corporations").

branch can both outsource its functions and bootstrap private data for surveillance without with relative impunity.

A. OUTSOURCING—RELATED STATUTES

Within the administrative hierarchy, a wide range of standards apply to federal agencies by Congress, the President, and the courts for purposes of limiting the discretion exercised on behalf of the constitutional branches and for imposing transparency and modes of public participation. The Administrative Procedure Act (APA)[166] is the primary statutory source for public disclosure, public involvement in rule making, and judicial review of government decisionmaking.[167] Its Freedom of Information Act (FOIA) provisions mandate public disclosure of government activities.[168] The Federal Advisory Committee Act restricts and makes public the advice that federal advisory committees provide agencies.[169] The Government in the Sunshine Act makes statutorily defined agency meetings public.[170] The Federal Register Act requires publication of regulatory documents for public inspection,[171] and the Information Quality Act (also known as the Data Quality Act) directs OMB to issue government-wide guidance regarding the quality of information "disseminated by Federal agencies."[172] Executive Order 12,866 also requires OMB

---

[166] Administrative Procedure Act, Pub. L. No. 796-404, 60 Stat. 237 (1946) (codified as amended in scattered sections of 5 U.S.C.).

[167] *See infra* notes 168–70 (describing the APA's parts and protections); *see also* Gillian E. Metzger, *Privatization as Delegation*, 103 COLUM. L. REV. 1367, 1434 (2003) (noting that, whereas the APA applies only to agencies, regulations governing contractors focus on preventing fraud versus providing a way to challenge contractors' actions).

[168] Freedom of Information Act, 5 U.S.C. § 552 (2012). However, the Supreme Court has held that the government can withhold from public disclosure databases composed entirely of publicly available data, because there is a "distinction, in terms of personal privacy, between scattered disclosure of the bits of information . . . and revelation of the [information] as a whole." U.S. Dep't of Justice v. Reporters Comm., 489 U.S. 749, 764 (1989).

[169] Federal Advisory Committee Act, 5 U.S.C. app. § 2 (2012).

[170] Government in the Sunshine Act, 5 U.S.C. § 552(b) (2012).

[171] Federal Register Act, 44 U.S.C. §§ 1501–1511 (2012).

[172] Consolidated Appropriations Act, 2001, Pub. L. No. 106-554, app. C, § 515, 114 Stat. 2763A-153 to -154 (2000); *see Agency Information Quality Guidelines*, OFFICE OF MANAGEMENT AND BUDGET, http://www.whitehouse.gov/omb/inforeg_agency_info_quality_links (last visited Jan. 9, 2015) (noting § 515's popular name); *Data Quality Act*, CENTER FOR EFFECTIVE GOVERNMENT, http://www.foreffectivegov.org/node/3479 (last visited Fed. 15, 2015) (referring to § 515 as the Data Quality Act).

oversight of the regulatory process through its Office of Information and Regulatory Affairs.[173]

None of the foregoing statutory constraints on government conduct apply to private contractors exercising identical public functions, however. The APA, the FOIA, and other disclosure statutes do not cover private actors.[174] Nor are contractors subject to the same "pay caps, limits on political activity, and labor rules" that apply to government employees.[175] OMB Circular A-76 forbids the outsourcing of "inherently governmental" functions,[176] but agencies routinely overlook it[177] and lack the personnel to properly administer its requirements.[178] Although the Federal Activities Inventory Reform Act (FAIR) of 1998 codifies Circular A-76's definition of "inherently governmental function,"[179] it contains no method for challenging the decision to outsource itself.[180]

---

[173] Exec. Order No. 12,866, 58 Fed. Reg. 51,735 (Sept. 30, 1993), *reprinted as amended in* 5 U.S.C. § 601 note (2012); *see also* Paperwork Reduction Act, 44 U.S.C. §§ 3501–3521 (2012) (establishing the Office of Information and Regulatory affairs within the Office of Management and Budget); 2 JACOB A. STEIN, GLENN A. MITCHELL & BASIL J. MEZINES, ADMINISTRATIVE LAW § 7.09 (2014) (describing the Paperwork Reduction Act, which created the Office of Information and Regulatory Affairs).

[174] *See* 5 U.S.C. § 551(1) (2012) (defining "agency" for the purposes of the APA and its subparts).

[175] Guttman, *supra* note 14, at 338.

[176] OFFICE MGMT. & BUDGET, CIRCULAR NO. A-76 REVISED 1, A2 (2003) (stating this policy and criteria for determining what are "inherently governmental activities"). Circular A-76 predated the Federal Activities Inventory Reform Act of 1998, which codified A-76's definition of "inherently governmental function." 31 U.S.C. § 501 note (Federal Activities Inventory Reform) (2012) ("The term 'inherently governmental function' means a function that is so intimately related to the public interest as to require performance by Federal Government employees."). The statute then lists examples of the types of "functions included." *Id.*

[177] *See* Freeman & Minow, *supra* note 29, at 3 (noting that government agencies often lack the capacity to enforce contractual terms); *see also* Correction of Long-Standing Errors in Agencies' Unsustainable Procurements Act of 2009, S. 924, 111th Cong. § 3 (2009) (finding that inherently governmental functions "have been wrongly outsourced"); Concurrent Resolution on the Federal Budget for Fiscal Year 2010, S. Con. Res. 13, 111th Cong. § 502(5) (2009) (requiring the Department of Defense to "review the role that contractors play in its operations, including the degree to which contractors *are* performing inherently governmental functions . . ." (emphasis added)).

[178] PAUL R. VERKUIL, OUTSOURCING SOVEREIGNTY: WHY PRIVATIZATION OF GOVERNMENT FUNCTIONS THREATENS DEMOCRACY AND WHAT WE CAN DO ABOUT IT 128 (2007) ("The agency's designation of what is 'inherently government' is not subject to administrative review.").

[179] *See supra* note 176.

[180] 31 U.S.C. § 501 note (Federal Activities Inventory Reform Act).

Accordingly, there are no external checks on government outsourcing in the form of private rights of action to challenge outsourcing decisions or contractor compliance.[181] The Federal Acquisition Regulation (FAR)[182] governs the process by which the government purchases goods and services, but only disappointed bidders can challenge contract awards for noncompliance.[183] The FAR's conflict of interest provisions do take into consideration whether a contractor's aims are "at odds with the 'public interest,'" and existing rules can be waived for contracts deemed essential.[184] Although private tort and contract law might apply to abuses by government contractors, immunity defenses stymie lawsuits.[185] Only the government can sue private contractors under the Contract Disputes Act.[186] Moreover, it can contract out of normative protections in the negotiating process[187] and often lacks

---

[181] *See infra* notes 176–90 and accompanying text.

[182] The FAR is codified in Title 48 of the Code of Federal Regulations and is promulgated by the General Services Administration, the Department of Defense, and the National Aeronautics and Space Administration under the authority of the Office of Federal Procurement Policy Act of 1974. *See* Exec. Order No. 12,979, 60 Fed. Reg. 55, 171 (Oct. 25, 1995), *reprinted in* 41 U.S.C. § 3701 note (2012).

[183] *See* 31 U.S.C. § 3551(1)–(2) (2012) (giving "interested part[ies]" the right to file protests and defining the term). Bidders can either challenge the agency's failure to comply with Circular A-76 under the APA or file bid protests with the GAO under 31 U.S.C. § 3551 (2012). Robert H. Shriver III, *No Seat at the Table: Flawed Contracting Out Process Unfairly Limits Front-Line Federal Employee Participation*, 30 PUB. CONT. L.J. 613, 627 (2001) (citing CC Distribs. v. United States, 883 F.2d 146, 156 (D.C. Cir. 1989) (finding no constitutional standing to sue)); *see also* Verkuil, *supra* note 20, at 453 ("This leaves contractors themselves the most likely candidates to achieve judicial review and makes such review dependent upon the government denying rather than granting a request to privatize a government function."); *cf. id.* at 454 (suggesting that the Subdelegation Act might provide an avenue for judicial review of delegations to private parties).

[184] Guttman, *supra* note 19, at 898 (citing Organizational Conflicts of Interest, 48 C.F.R. pt. 2009.5 (1999)).

[185] *See, e.g.*, Bartell v. Lohiser, 215 F.3d 550, 557 (6th Cir. 2000) (applying immunity to private foster care contractor in action under federal disability laws); Pani v. Empire Blue Cross Blue Shield, 152 F.3d 67, 73 (2d Cir. 1998) (applying immunity to a private insurance company in a Medicare dispute); *cf.* Richard J. Pierce, Jr., *Outsourcing Is Not Our Only Problem*, 76 GEO. WASH. L. REV. 1216, 1228–29 (2008) (arguing that private contractors should not be immunized for government work performed).

[186] 41 U.S.C. §§ 7101–7109 (2012).

[187] *See* Freeman, *supra* note 42, at 591 (noting that even if "[private law] provided a basis for extending common law norms into contract law, parties could presumably minimize or avoid their new obligations by explicitly contracting out of them"). *But cf.* Jody Freeman, *Extending Public Law Norms Through Privatization*, 116 HARV. L. REV. 1285, 1296 (2003) (arguing that contracts should reflect public law values through a process of "publicization"); Wendy Netter Epstein, *Contract Theory and the Failures of Public-Private*

the resources or motivation to pursue common law remedies.[188] The False Claims Act (FCA)[189] enables *qui tam* suits to recover penalties from private contractors for fraud only so long as its formidable requirements are satisfied.[190]

In sum, the administrative law norms that exist within a government bureaucracy and constitutional democracy do not apply to private contractors.[191] Nor has Congress created private rights of action to constrain ultra vires outsourcing decisions or to enforce contract terms that do not involve false claim submissions within the meaning of the FCA. As a result, the government is largely left to self-regulate its outsourcing programs through use and sharing agreements that it may not decide to enforce.[192]

B. DATA INSOURCING—RELATED STATUTES

Federal surveillance laws bearing upon data insourcing—like the laws applicable to outsourcing—leave substantial gaps in both government and private sector accountability. The statutory landscape relating to surveillance data shifted substantially in response to global terrorism. Pre-9/11, Congress enacted the 1968 Wiretap Act,[193] the FISA of 1978,[194] the Electronic Communications

---

Contracting, 34 CARDOZO L. REV. 2211, 2254, 2256 (2013) (arguing a mandatory duty to act in furtherance of the public interest should be implied in all government outsourcing contracts and that "members of the public for whose benefit the service was being provided—and who are harmed when service provision is poor—should be permitted to sue as third-party beneficiaries for breach of the public interest duty").

[188] *See* Jody Freeman, *Extending Public Accountability Through Privatization: From Public Law to Publicization*, *in* PUBLIC ACCOUNTABILITY: DESIGNS, DILEMMAS AND EXPERIENCES 83, 97–98 (Michael W. Dowdle ed., 2006) (explaining how both the executive and legislative branches may lack the motivation to hold private actors accountable).

[189] 31 U.S.C. §§ 3729–3733 (2012).

[190] Laura A. Dickinson, *Public Values/Private Contract*, *in* GOVERNMENT BY CONTRACT: OUTSOURCING AND AMERICAN DEMOCRACY, *supra* note 18, at 335, 356.

[191] *See* Kimberly N. Brown, *"We the People," Constitutional Accountability, and Outsourcing Government*, 88 IND. L.J. 1347, 1361–64 (2013) (comparing accountability measures constraining government actors and the lack thereof regarding private contractors).

[192] *See supra* note 177 (explaining the current inadequacy of legislative, regulatory, and constitutional methods of oversight); *see also* Brown, *supra* note 191, at 1364–69.

[193] 18 U.S.C. §§ 2510–2520 (2012). The Wiretap Act was enacted as Title III of the Omnibus Crime Control & Safe Streets Act of 1968. Pub. L. No. 90-351, 82 Stat. 197 (codified at scattered sections of 18, 42 U.S.C.). *See* SOLOVE, ROTENBERG & SCHWARTZ, *supra* note 75, at 84–85 (noting "Wiretap Act" as the name of the statute).

[194] Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. §§ 1801–1811 (2012).

Privacy Act (ECPA) of 1986[195] (which contains the Stored Communications Act (SCA)),[196] and the Communications Assistance for Law Enforcement Act (CALEA) of 1994.[197] These laws largely authorized the interception and storage of wire, oral, and electronic communications under circumstances that may or may not require probable cause and a warrant. The FISA stands apart from the others because it applies to foreign—versus domestic—intelligence and is triggered by a relatively lesser showing on the government's part.[198]

Post-9/11, Congress passed the USA PATRIOT Act of 2001,[199] the Protect America Act (PAA) of 2007,[200] and the FISA Amendments Act (FAA) of 2008.[201] These statutes amended the FISA to provide the government with expanded authority that gave rise to the controversial Verizon order and the NSA's PRISM program, both of which effectively enabled the collection of Americans' communications data without probable cause and a warrant.[202]

1. Before 9/11. Pre-9/11 surveillance legislation restricted the government's ability to collect voice and electronic communications, both in-transit and from storage repositories. It also imposed civil and criminal liability for unilateral violations by

---

195 Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).

196 18 U.S.C. §§ 2701–2711 (2012).

197 47 U.S.C. §§ 1001–1010 (2012).

198 *See infra* notes 230–39 and accompanying text.

199 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) of 2001, Pub. L. No. 107-56, 115 Stat. 272 (codified as amended in scattered sections of 8, 15, 18, 22, 31, 42, 49, 50 U.S.C.). Notably, Congress allowed § 215 of the USA PATRIOT Act, a section that allows for bulk collection of U.S. citizens' cellphone data, to sunset in June of 2015. Jeremy Diamond, Patriot Act Provisions Have Expired: What Happens Now?, CNN POLITICS (June 1, 2015), http://www.cnn.com/2015/05/30/politics/what-happens-if-the-patriot-act-provisions-expire/ (explaining that the Senate allowed key provisions of the law to lapse, including the NSA's bulk data collection program).

200 Protect America Act of 2007, 50 U.S.C. §§ 1805a–1805c (2012).

201 FISA Amendment Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436 (codified as amended in scattered sections of 50 U.S.C.).

202 *See* BRENNAN CENTER FOR JUSTICE, ARE THEY ALLOWED TO DO THAT? A BREAKDOWN OF SELECTED GOVERNMENT SURVEILLANCE PROGRAMS (2013), *available at* http://www.brennancenter.org/sites/default/files/analysis/Government%20Surveillance%20Factsheet.pdf (providing a breakdown of the new government surveillance programs and explaining their statutory justifications).

the private sector, while immunizing third parties for cooperating with government investigations.

Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("the Wiretap Act")[203] made it illegal for anyone to intercept or disclose wire or oral communications,[204] which it defines as utterances "by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation."[205] The statute expressly covers the "contents" of communications, i.e., "any information concerning the substance, purport, or meaning of that communication."[206] It permits law enforcement to apply for a judicial wiretap order only upon a showing of probable cause that the target is involved in serious crimes that are enumerated in the statute.[207] The government must provide notice to the target and minimize collection of unrelated communications.[208] The statute also imposes civil and criminal liability for violations.[209]

The ECPA of 1986 expanded the Wiretap Act's protections for voice communications to ban the intentional interception, use, or disclosure of "electronic communications,"[210] which is defined in such a way as to cover e-mail and Internet activity.[211] The ECPA thus makes it unlawful for a third party to intercept someone

---

[203] *See supra* note 193 and accompanying text.

[204] 18 U.S.C. § 2511 (2012). This formulation reflects the seminal decision in *Katz v. United States*, 389 U.S. 347 (1967), which preceded the Wiretap Act by one year. *See* Freiwald, *supra* note 92, at 21–22. In *Katz*, the Supreme Court expressly declined to address whether a warrant is required in cases involving national security. 389 U.S. at 358 n.23; *see also* Mitchell v. Forsyth, 472 U.S. 511, 532 (1985) ("In the aftermath of *Katz*, Executive authority to order warrantless national security wiretaps remained uncertain.").

[205] 18 U.S.C. § 2510(2) (2012).

[206] *Id.* § 2510(8).

[207] *Id.* §§ 2518(3), 2516(1); *see also* Freiwald, *supra* note 92, at 23–25.

[208] 18 U.S.C. §§ 2518(5), 2518(8)(d).

[209] *Id.* §§ 2511, 2520.

[210] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.); *see also* 18 U.S.C. § 2511 (2012) (making it unlawful to intentionally intercept any "wire, oral, or electronic communication").

[211] *See* United States v. Councilman, 418 F.3d 67, 79 (1st Cir. 2005) ("[W]e conclude that the temporarily stored e-mail messages at issue here constitute electronic communications within the scope of the Wiretap Act . . . ."); Kerr, *supra* note 138, at 630 (stating that Congress expanded the Wiretap Act to the Internet in 1986 when it enacted the ECPA). The ECPA defines an "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce." 18 U.S.C. § 2510(12) (2012).

else's e-mail without his or her consent.[212] The ECPA contains the Stored Communications Act (SCA),[213] which protects stored communications such as those maintained by an individual's Internet service provider (ISP), and imposes criminal fines or imprisonment on anyone who intentionally accesses or discloses such communications without authorization.[214] It also contains the Pen Register Act,[215] which requires a court order before installation of a device for recording telephone numbers dialed (a "pen register") or telephone numbers from which incoming calls originate (a "trap and trace device").[216]

The ECPA and the SCA contain exceptions that make it possible for private parties to lawfully capture and store electronic communications and share them with the government. The ECPA contains a business use exception, whereby employees of electronic communications service providers may "intercept, disclose, or use" electronic communications in the normal course of employment for "mechanical or service quality control checks."[217] It also authorizes the government to obtain warrants requiring that providers "furnish . . . all information, facilities, and technical assistance necessary to accomplish . . . interception[s] unobtrusively."[218] Additionally, the ECPA authorizes third-party service providers to hand over information to the government pursuant to a FISA order or a certification by the Attorney General or a designee that no such order is required.[219] A similar provision in the Pen Register Act

---

[212] *See* 18 U.S.C. §§ 2511(2)–(5), 2520 (2012) (imposing criminal and civil liability for violations).

[213] *Id.* §§ 2701–2711.

[214] *Id.* § 2701(a)–(b).

[215] *Id.* §§ 3121–3127. The Pen Register Act governs the use of devices that trace what has been termed "envelope information" (including "addressing" and "routing" information for e-mail), *id.* § 3127(3), while the Wiretap Act and the SCA govern "content information," *see id.* § 2510(1), (4), (8), (12) (defining "intercept" under the Wiretap Act to mean "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device," and providing definitions for "wire communication," "contents," and "electronic communication").

[216] *Id.* § 3121(a); *see also id.* § 3127(3)–(4) (defining "pen register" and "trap and trace device").

[217] *Id.* § 2511(2)(a)(i); *see* Jarrod J. White, Commentary, *E-mail@Work.Com: Employer Monitoring of Employee E-mail*, 48 ALA. L. REV. 1079, 1086 (1997) (stating that 18 U.S.C. § 2511(2)(a)(i) (2012) is a source for the "business use exemption," which an employer may assert to monitor an employee's e-mail in the absence of express or implied consent).

[218] 18 U.S.C. § 2518.

[219] *Id.* § 2511(2)(a)(ii).

allows for ex parte orders requiring that service providers install surveillance equipment at the government's behest.[220]

For its part, the SCA empowers the government to obtain the contents of wire or electronic communications with a warrant or by subpoena with prior notice to the subscriber.[221] Non-content information may be obtained pursuant to a warrant or a court order that does not require probable cause.[222] The SCA exempts service providers from civil or criminal liability regardless of the purpose of the interception;[223] in this way, it differs from the Wiretap Act's narrower exemption for "activit[ies] which [are] a necessary incident to the rendition of his service."[224]

Law enforcement routinely makes use of ECPA and SCA exceptions to collect electronic data regarding private citizens. An internal DOJ "Electronic Surveillance Manual" indicates that the SCA is commonly used to obtain cell tower dump records,[225] which it can use to determine a cell phone's approximate location within a few hundred yards.[226] Recently, the government invoked the

---

[220] *Id.* § 3123.

[221] *Id.* § 2703(a)–(b)(1). There is a question as to whether the ECPA's requirements bind just the service provider or whether the government is precluded from making a request for information without complying with the ECPA first. In *McVeigh v. Cohen*, 983 F. Supp. 215, 218–19 (D.D.C. 1998), the Navy discharged an officer for homosexual conduct it derived from information it informally obtained from AOL. The Navy took the position—rejected by the court—that the ECPA contains no prohibitions relating to government conduct. *Id.* at 220. A service provider could arguably turn over information to other private parties without a warrant, subpoena, or a court order under the ECPA, as well.

[222] *See* 18 U.S.C. § 2703(d) (requiring "*reasonable grounds to believe* that the . . . records or other information sought, are relevant and material to an ongoing criminal investigation" (emphasis added)). Recently, in an appeal of a criminal conviction based in part on location records obtained from cell phone service providers under the SCA, the Eleventh Circuit found the statute unconstitutional to the extent that it allows the government to obtain such information without a warrant. United States v. Davis, 754 F.3d 1205, 1210–18 (11th Cir. 2014), *vacated en banc*, 573 F. App'x 925 (11th Cir. 2014) (mem.).

[223] 18 U.S.C. §§ 2701(c)(1), 2703(e).

[224] *Id.* § 2511(2)(a)(i).

[225] *See* U.S. DEP'T OF JUSTICE, ELECTRONIC SURVEILLANCE MANUAL, at ii, 162 (rev. 2005), *available at* http://www.justice.gov/criminal/foia/docs/elec-sur-manual.pdf (setting forth procedures "to obtain authorization to conduct electronic surveillance" and including a form application for a court order under 18 U.S.C. § 2703(d), which includes "cell site information" within the types of information the applicant can apply for disclosure of).

[226] Hon. Brian L. Owsley, *The Fourth Amendment Implications of the Government's Use of Cell Tower Dumps in Its Electronic Surveillance*, 16 U. PA. J. CONST. L. 1, 5 (2013). When a cell phone is turned on, the phone sends out a "signal testing" to the nearest cell site in order to initiate contact with the network. *Id.* When a call is placed, "it triggers a series of relays along the cell-site network." *Id.* at 4. Providers routinely collect information

SCA to obtain records from the Twitter accounts of individuals associated with the WikiLeaks organization.[227]

The SCA also allows law enforcement agencies to use National Security Letters (NSLs)[228] to obtain information from ISPs and telephone companies without a court order if the government certifies that the records it seeks are "relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities."[229] Google has reportedly received thousands of NSLs issued over the last few years, implicating tens of thousands of users and accounts.[230]

Congress passed the FISA in 1978, after Watergate raised public awareness of the executive branch's long history of warrantless surveillance for national security and political purposes.[231] Whereas the Wiretap Act, the ECPA, and the SCA are criminal statutes implicating domestic intelligence, the FISA was enacted to enhance the government's capacity to obtain "foreign intelligence information" by eavesdropping on people suspected of working with foreign governments on United States soil.[232] It thus has a "lower threshold for conducting surveillance

---

regarding the proximity of a particular phone to a particular cell tower, the position of the tower in relation to the phone, and the signal strength of the phone for billing and other purposes. *Id.* at 5.

[227] Scott Shane & John F. Burns, *U.S. Subpoenas Twitter Over WikiLeaks Supporters*, N.Y. TIMES, Jan. 9, 2011, at A1, *available at* http://www.nytimes.com/2011/01/09/world/09wiki.html; Glenn Greenwald, *DOJ Subpoenas Twitter Records of Several WikiLeaks Volunteers*, SALON (Jan. 7, 2011, 11:08 PM), http://www.salon.com/2011/01/08/twitter_2/.

[228] For background on NSLs, see SUSAN N. HERMAN, TAKING LIBERTIES: THE WAR ON TERROR AND THE EROSION OF AMERICAN DEMOCRACY 150–64 (2011).

[229] 18 U.S.C. § 2709(b). The statute states that "[a] wire or electronic communication service provider *shall* comply with a request for subscriber information and toll billing records information, or electronic communication transactional records in its custody or possession made by the Director of the Federal Bureau of Investigation under subsection (b) of this section." *Id.* § 2709(a) (emphasis added). In *In re National Security Letter*, 930 F. Supp. 2d 1064, 1075–77 (N.D. Cal. 2013), a federal district judge held the statute's provision prohibiting a recipient from disclosing the existence of an NSL, 18 U.S.C. § 2709(c), violated the First Amendment, and that the narrow and deferential provision for judicial review, *id.* § 3511(b), violated the First Amendment and the separation of powers.

[230] *Transparency Report: Requests For User Information*, GOOGLE, https://www.google.com/transparencyreport/userdatarequests/US/ (last visited Feb. 20, 2015).

[231] *See* Stephanie Cooper Blum, *What Really Is at Stake with the FISA Amendments Act of 2008 and Ideas for Future Surveillance Reform*, 18 B.U. PUB. INT. L.J. 269, 275 (2009) (describing pre-FISA history of governmental abuses).

[232] *See* 50 U.S.C. §§ 1801(e)–(f), 1802 (2012). The FISA makes numerous distinctions based on whether the surveillance target is foreign or a U.S. national and whether the

[that] reflects the inherent differences between obtaining surveillance for intelligence (e.g. prevention) purposes, as opposed to obtaining evidence to be used to convict an individual in a court of law."[233]

The FISA does not require that the government demonstrate probable cause that a search will reveal evidence of a crime so as to justify the issuance of a warrant by a magistrate judge.[234] It instead allows the government to apply to the Foreign Intelligence Surveillance Court (FISC)—a special panel of eleven federal district court judges[235]—for an ex parte order authorizing electronic surveillance of Americans for up to ninety days.[236] The government must show, *inter alia*, that "the target of the electronic surveillance is a foreign power or an agent of a foreign power" and that "a significant purpose" of the investigation is to obtain foreign intelligence.[237] Although no indication of criminal wrongdoing is required for foreign subjects, in order to obtain a warrant regarding a "United States person" the government must demonstrate probable cause to believe that the person is "knowingly" engaged in activities that "involve or may involve a violation of the criminal statutes of the United States."[238] The statute also mandates that the government craft "minimization procedures" to limit its collection, storage, and dissemination of

---

acquisition is by fiber optic cable or by wireless communication, such as radio, among other factors. *Id.*; *see also* Blum, *supra* note 231, at 279 (noting that "FISA seems to make arbitrary distinctions, based on technology, that are divorced from any privacy or reasonableness concerns of the Fourth Amendment").

233 Blum, *supra* note 231, at 276.

234 *See generally* William C. Banks, *Programmatic Surveillance and FISA: Of Needles in Haystacks*, 88 TEX. L. REV. 1633 (2010) (describing the "basic idea" of the FISA as allowing "[g]overnment [to] conduct intrusive electronic surveillance of Americans . . . without traditional probable cause . . . if it could demonstrate . . . reason to believe that targets of surveillance [were] acting on behalf of foreign powers" (citing 50 U.S.C. § 1805(a) (2012))).

235 50 U.S.C. § 1803(a); SOLOVE, ROTENBERG & SCHWARTZ, *supra* note 75, at 104. A separate court of review "ha[s] jurisdiction to review the denial of any application made under [FISA]." 50 U.S.C. § 1803(b).

236 50 U.S.C. §§ 1805, 1824(d)(1)–(2).

237 *Id.* §§ 1804(a)(3)(A), (a)(6)(B), 1805(a).

238 *Id.* § 1801(b)(1), (b)(2) (defining "agent of a foreign power" as requiring at least this showing if the target is a "United States person"); SOLOVE, ROTENBERG & SCHWARTZ, *supra* note 75, at 104.

non-foreign-intelligence information.[239] In certain circumstances, the FISA authorizes surveillance without a court order.[240]

In 1994, Congress passed the CALEA and President Bill Clinton signed it into law.[241] The CALEA was enacted in response to FBI complaints that advancing digital technologies were making it difficult to perform surveillance over telephone networks.[242] The statute requires telecommunications carriers to develop and modify their equipment, facilities, and services to ensure that they can comply with the FBI's electronic surveillance requirements.[243] Any interceptions conducted on the premises of a communications provider must be done pursuant to a court order.[244]

2. After 9/11. In the wake of 9/11, Congress passed the USA PATRIOT Act of 2001,[245] which amended the FISA in a number of important ways. For example, prior to the 2001 amendments, the government had to persuade the FISA court that "*the* purpose" of

---

[239] 50 U.S.C. §§ 1801(h), 1805(a)(3).

[240] *See id.* §§ 1802(a), 1805(f), 1809(a)(1), 1811; SOLOVE, ROTENBERG & SCHWARTZ, *supra* note 75, at 104. Fourth Amendment challenges to the FISA and its amendments have been unsuccessful. *See, e.g.*, United States v. Abu-Jihaad, 630 F.3d 102, 108 (2d Cir. 2010) (denying defendant's constitutional challenges to FISA after admission of evidence that defendant communicated national defense information and provided materials to terrorists); United States v. Warsame, 547 F. Supp. 2d 982, 984 (D. Minn. 2008) (finding that probable cause and particularity requirements of FISA satisfied reasonableness requirement of Fourth Amendment where defendant was charged with conspiracy and with providing material support and resources to terrorists).

[241] Communications Assistance of Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified as amended at 47 U.S.C. §§ 1001–1010 (2012)).

[242] FIGLIOLA, *supra* note 117, at 1 (noting that complaints by the FBI of increased difficulty accessing public telephone networks contributed to the enactment of CALEA).

[243] 47 U.S.C. §§ 1002, 1005 (2012).

[244] *Id.* § 1004.

[245] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) of 2001, Pub. L. No. 107-56, § 208(a), 115 Stat. 272 (codified as amended in scattered sections of 8, 15, 18, 22, 31, 42, 49, 50 U.S.C.). The USA Freedom Act, H.R. 3361, which passed the house in May 2014, would extend the USA Patriot Act to 2017. USA Freedom Act, H.R. 3361, 113th Cong. § 701(a) (2014); *see also H.R. 3361 (113th): USA FREEDOM Act*, GOVTRACK.US, https://www.govtrack.us/congress/bills/113/hn3361 (last visited Feb. 21, 2015) (noting that the bill passed the House but died in the Senate). Although it was designed to curtail the NSA's bulk collection of metadata, partly by shifting the retention of metadata to private firms, privacy advocates assailed the bill. Andrea Peterson, *NSA Reform Bill Passes House, Despite Loss of Support from Privacy Advocates*, WASH. POST, May 22, 2014, http://www.washingtonpost.com/blogs/the-switch/wp/2014/05/22/nsa-reform-bill-passes-house-despite-loss-of-support-from-privacy-advocates/.

its surveillance was to obtain foreign intelligence information.[246] Section 218 of the USA PATRIOT Act narrowed the government's burden to demonstrating that foreign intelligence is "a significant" purpose of the FISA surveillance.[247] It also expanded the government's ability to obtain ex parte orders authorizing physical searches,[248] pen registers, and trap and trace devices;[249] expanded the length of the FISA's surveillance periods;[250] and increased access to emergency surveillance.[251]

In addition, § 215 of the statute—which expired on May 31, 2015[252]—significantly enhanced the government's ability to obtain business records such as customer book lists, library patron records, and medical records from third-party telephone and ISP companies.[253] Although grand juries routinely issue subpoenas for business records in criminal investigations, no showing of probable cause was required under § 215.[254] Rather, the application only needed to include "a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation."[255] Moreover, companies served with § 215 orders were prohibited from disclosing that fact to anyone, including the subjects of the surveillance.[256] The FISA court's controversial order to Verizon in April of 2013, made public with the first of the Snowden leaks, was issued pursuant to § 215.[257] It broadly required Verizon to provide the NSA with

---

[246] 50 U.S.C. §§ 1804(a)(7)(B), 1823(a)(7)(B) (2000) (amended 2001) (emphasis added).

[247] USA PATRIOT Act, Pub. L. No. 107-56, § 218, 115 Stat. 272, 291 (2001).

[248] *Id.* §§ 206, 207, 115 Stat. at 282.

[249] *Id.* § 214, 115 Stat. at 286–87 (amending the FISA).

[250] *Id.* § 207(a), 115 Stat. at 282.

[251] *Id.* § 212(1), 115 Stat. at 284.

[252] *See* Diamond, *supra* note 199.

[253] *Id.* § 215, 115 Stat. at 287 (codified at 50 U.S.C. § 1861(a)(1) (2012)) (authorizing production of "any tangible things" related to "an investigation" regarding foreign intelligence not concerning United States persons or "to protect against international terrorism or clandestine intelligence activities"); *see* Donohue, *supra* note 137, at 128 n.32 (citing § 215 as increasing government access to certain business records).

[254] *See* 50 U.S.C. § 1861. The Executive must "fully inform" Congress as to the implementation of § 215 on an annual basis. *Id.* § 1862(a).

[255] *Id.* § 1861(b)(2)(a).

[256] *Id.* § 1861(d)(1).

[257] *In re Application of F.B.I. for an Order Requiring the Production of Tangible Things from Verizon*, FISA Ct. (2013), *available at* http://epic.org/privacy/nsa/Section-215-Order-to-Verizon.pdf.

telephone call metadata for the approximately 101.2 million wireless accounts in its systems for a three-month period.[258]

Although the FISA limited the government's ability to engage in warrantless spying on U.S. nationals,[259] after 9/11 President George W. Bush issued an executive order unilaterally authorizing the NSA to eavesdrop on Americans' e-mail and telephone communications if a person was believed to have terrorist links.[260] Under the Bush Administration's Terrorist Surveillance Program, the NSA conducted "vacuum cleaner surveillance" in conjunction with private telecommunications companies for purposes of identifying potential terrorist threats, and only then utilized the FISA procedures to further investigate.[261] In 2007, the FISA court condoned the program, "g[iving] the government access to nearly all of the international telecom traffic entering and leaving the United States."[262] The PAA was also enacted in 2007 to provide legislative backing for programmatic surveillance beyond the case-specific confines of the FISA.[263]

Upon the PAA's expiration in 2008, Congress passed the FAA.[264] Whereas the FISA tolerates interceptions of communications

---

[258] *Id.*; *see also Verizon Posts Double-Digit Earnings Growth and Continued Strong Operating Performance in 3Q: 3Q 2013 Highlights*, VERIZON.COM, http://www.verizonwireless.com/news/article/2013/10/93-2013-earnings.html (last visited Feb. 21, 2015) (noting Verizon's 101.2 million retail connections in 2013). The FISA court on February 26, 2015 approved an extension of a modified telephony metadata collection program until June 1, 2015, the date on which § 215 is set to expire. *Statement by the White House Press Secretary*, THE WHITE HOUSE OFFICE OF THE PRESS SECRETARY (Feb. 27. 2015), *available at* https://www.whitehouse.gov/the-press-office/2015/02/27/statement-press-secretary-reauthorization-collection-bulk-telephony-meta (commenting on the reauthorization of the Collection of Bulk Telephony Metadata Under Section 215 of the USA PATRIOT Act).

[259] JAMES G. MCADAMS, FED. LAW ENFORCEMENT TRAINING FACILITIES, FOREIGN INTELLIGENCE SURVEILLANCE ACT (FISA): AN OVERVIEW 1–2 (2007), *available at* https://www.fletc.gov/sites/default/files/imported_files/training/programs/legal-division/downloads-articles-and-faqs/research-by-subject/miscellaneous/ForeignIntelligenceSurveillanceAct.pdf.

[260] Blum, *supra* note 231, at 283; Banks, *supra* note 234, at 1641.

[261] Banks, *supra* note 234, at 1641–42.

[262] *Id.* at 1643.

[263] *Id.* at 1644; Blum, *supra* note 231, at 296–97.

[264] Gene Healy, *Our Continuing Cult of the Presidency*, *in* THE PRESIDENCY IN THE TWENTY-FIRST CENTURY 145, 153 (Charles W. Dunn ed., 2011). Section 702 of the FAA amended the FISA at 50 U.S.C. § 1881a. FISA Amendments Act of 2008, Pub. L. No. 110-261, § 702, 122 Stat. 2436, 2438. The FAA was reauthorized in 2012. H.R. Res. 5949, 112th Cong. (2012) (enacted). *See generally* EDWARD C. LIU, CONG. RESEARCH SERV., R42725, REAUTHORIZATION OF THE FISA AMENDMENTS ACT (2013) (discussing the reauthorization of the FAA).

involving persons on U.S. soil, the FAA only allows for the targeting of non-U.S. persons outside the United States.[265] However, it does not require an individualized determination by the FISC as a precondition to surveillance of a specific target.[266] The FAA instead empowers the U.S. Attorney General (AG) and the Director of National Intelligence (DNI) to obtain a so-called "certification order" from the FISC empowering them to jointly authorize, for up to one year, the surveillance of non-U.S. citizens outside of the United States for foreign intelligence purposes.[267] Rather than requiring—as the FISA does—that a target be an agent of a foreign power,[268] the FAA provides that the FISC "shall"[269] issue a certification order upon a showing, *inter alia,* that "a significant purpose of the acquisition is to obtain foreign intelligence information."[270] The court must approve "targeting" and "minimization" procedures in its certification order to ensure that only people "reasonably believed to be outside the United States" are targeted and to minimize any privacy impact.[271]

After the FISC issues a certification order, the AG and DNI can direct that electronic communications providers assist in surveillance in exchange for retroactive immunity.[272] An immunity provision is triggered if the AG certifies to one or more of five conditions.[273] In such cases, no civil action may be maintained "against any person for providing assistance to an element of the intelligence community."[274] Only companies served with FAA orders can challenge related requests for information before the FISC.[275]

---

[265] 50 U.S.C. § 1881a(b) (2012).

[266] NSA DIR. OF CIVIL LIBERTIES AND PRIVACY OFFICE, NSA'S IMPLEMENTATION OF FOREIGN INTELLIGENCE SURVEILLANCE ACT SECTION 702, at 2 (2014), *available at* http://www.fas.org/irp/nsa/clpo-702.pdf.

[267] 50 U.S.C. § 1881a(a).

[268] *Id.* §§ 1804(a)(3)(A), 1804(a)(6)(B).

[269] *Id.* § 1881a(i)(3)(A).

[270] *Id.* § 1881a(g)(2)(A)(v).

[271] *Id.* § 1881a(g)(2)(A).

[272] *Id.* §§ 1881a(a), 1885a(a); *see* Laura K. Donohue, *The Shadow of State Secrets*, 159 U. PA. L. REV. 77, 157 (2010) (discussing the arrangements).

[273] 50 U.S.C. 1885a(a).

[274] *Id.* § 1885a(a).

[275] *Id.* § 1881a(h)(4)(A) ("An electronic communication service provider receiving a directive issued pursuant to paragraph (1) may file a petition to modify or set aside such directive with

Commentators have criticized the FAA as "permitting the mass acquisition, without individualized judicial oversight or supervision, of Americans' international communications."[276] Section 702 of the FAA is the stated legal authority for the government's PRISM program,[277] under which the NSA "tap[ped] directly into the central servers of nine leading U.S. Internet companies," and extracted "photographs, e-mails, documents, and connection logs," along with audio and video data.[278] Those companies included Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, and Apple.[279] The NSA describes the PRISM program as "compel[ling]" service providers "to provide NSA with communications to or from" individuals identified as likely to communicate foreign intelligence information.[280] It also "compel[s]" service providers "to assist . . . in the lawful interception of electronic communications to, from, or about tasked selectors" under § 702.[281]

Once intercepted, "[c]ommunications provided to NSA under Section 702 are processed and retained in multiple NSA systems and data repositories."[282] There are no legal restrictions on the government's ability to search such data, which can operate as an end-run around the FAA's ban on surveillance of U.S. nationals.[283]

---

the Foreign Intelligence Surveillance Court, which shall have jurisdiction to review such petition.").

[276] Jameel Jaffer & Laura W. Murphy, *Oversight Hearing on the Administration's Use of FISA Authorities*, 14 ENGAGE: J. FEDERALIST SOC'Y PRAC. GROUPS 76, 78 (2013).

[277] 50 U.S.C. § 1881a(a) ("[T]he Attorney General and the Director of National Intelligence may authorize jointly, for a period of up to 1 year from the effective date of the authorization, the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information."); DONAHUE, *supra* note 40, at 2; Glenn Greenwald & Ewen MacAskill, *NSA Prism Program Taps in to User Data of Apple Google and Others*, THE GUARDIAN (June 7, 2013, 3:23 PM), http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data; *see* Gellman & Poitras, *supra* note 136, at A1 (stating that the FISA Amendments gave rise to the PRISM project).

[278] DONAHUE, *supra* note 40, at 1 (quoting Gellman & Poitras, *supra* note 136, at A1).

[279] Gellman & Poitras, *supra* note 136. Interestingly, the Government Communications Headquarters—Britain's equivalent of the NSA—had also been secretly gathering the same intelligence from these nine companies through an operation set up by the NSA, bypassing the formal legal process required under their own laws. *Id.*

[280] NSA DIR. OF CIVIL LIBERTIES AND PRIVACY OFFICE, *supra* note 266, at 5.

[281] *Id.*

[282] *Id.* at 6.

[283] *See* Donohue, *supra* note 137, at 160, 192 (noting how the "to, from, and about" language of § 702 has been misused).

Laura Donohue has identified numerous violations of the FAA resulting from the lack of FISC oversight over specific searches of the NSA's metadata databases.[284] Moreover, before the Snowden disclosures gave rise to the lower court decisions in *Klayman v. Obama*[285] and *ACLU v. Clapper*,[286] lawsuits brought by individuals challenging these surveillance schemes have failed because the secretive nature of the programs makes it difficult for plaintiffs to establish the requisite injury.[287] Commentators have thus assailed the FISA and the FAA as providing insufficient safeguards for individual privacy rights protected by the Constitution.[288]

IV. THE REACH OF POSSIBLE CONSTITUTIONAL FIXES

Despite its inadequacies, the prospect of new legislation remains the primary means of establishing limits on data insourcing and outsourcing.[289] The relevant constitutional law is ad hoc, with no coherent framework for minding constitutional tolerance of modern alterations to the structure of government. Moreover, no doctrine is particularly robust for purposes of confining the privatization of government, as all are premised on a flawed assumption that the public and private sectors are severable for purposes of constitutional law.

---

[284] DONAHUE, *supra* note 40, at 40–54 (discussing three important ways the NSA has side stepped statutory requirements).

[285] 957 F. Supp. 2d 1 (D.D.C. 2013). *See infra* notes 373–74 and accompanying text.

[286] No. 14-42-CV, 2015 WL 2097814 (D.C. Cir. May 7, 2015). *See infra* note 375 and accompanying text.

[287] *See* Clapper v. Amnesty Int'l, USA, 133 S. Ct. 1138, 1155 (2013) (holding that plaintiffs' failure to demonstrate present or impending injury barred standing to challenge the constitutionality of FISA); Am. Civil Liberties Union v. Nat'l Sec. Agency, 493 F.3d 644, 687 (6th Cir. 2007) (holding that the plaintiffs lacked standing).

[288] *E.g.*, Donohue, *supra* note 137, at 174–90, 202–06, 243–65 (arguing that the NSA's metadata mining programs violate the FISA and the Constitution); Banks, *supra* note 234, at 1656 ("[O]ne inevitable problem with the relaxed standard [of the FAA] is that . . . more warrantless surveillance of persons inside the United States will occur."); Alan Butler, *Standing Up to* Clapper*: How to Increase Transparency and Oversight of FISA Surveillance*, 48 NEW ENG. L. REV. 55, 63–67 (2013) (indicating that the main problem with the FISA is "inadequate transparency and public accountability").

[289] Butler, *supra* note 288, at 82–91; *see also supra* note 18 and accompanying text.

A. THE STATE ACTION DOCTRINE

In theory, the state action doctrine extends the Constitution to limit or remedy the negative effects of private behavior that is attributable to the government.[290] In practice, it converts private actors into state ones for purposes of suppressing evidence in criminal trials or attaching liability for violations of individual constitutional rights.[291] In *Shelley v. Kraemer*, Chief Justice Vinson famously stated that the Fourteenth Amendment "erects no shield against merely private conduct, however discriminatory or wrongful"[292]—unless, the Court later explained, "to some significant extent the State in any of its manifestations has been found to have become involved in [the conduct]."[293]

The traditional aims of the state action doctrine are twofold: first, to "preserve[ ] an area of individual freedom by limiting the reach of federal law and federal judicial power"[294] and, second, to "avoid[ ] the imposition of responsibility on a State for conduct it could not control."[295] The doctrine thus simultaneously seeks to maintain *private parties'* autonomy and freedom on the one hand, and to ensure that the *government* is responsible for matters that lie within its sphere of authority on the other. By necessity, it assumes that a meaningful dividing line exists between the public and private.

Legal commentators have critiqued the doctrine's task as impossible.[296] The Supreme Court itself has quipped that "[w]hat is

---

[290] *See infra* note 292 and accompanying text (explaining that private actors may be subject to the Constitution if the government is sufficiently involved in their conduct).

[291] Private parties may be subject to money damages for constitutional violations under 42 U.S.C. § 1983 only if they are found to be acting under "color of law." Flagg Bros. v. Brooks, 436 U.S. 149, 156 (1978). The Court has stated that "the state action and the under color-of-state-law requirements are obviously related." Lugar v. Edmondson Oil Co., 457 U.S. 922, 928 (1982); *see also* Verkuil, *supra* note 20, at 431 (observing that the state action doctrine " 'constitutionalizes' after-the fact delegations that amount to the exercise of public authority" rather than limiting them in the first instance).

[292] 334 U.S. 1, 13 (1948).

[293] Burton v. Wilmington Parking Auth., 365 U.S. 715, 722 (1961).

[294] *Lugar*, 457 U.S. at 936.

[295] Nat'l Collegiate Athletic Ass'n v. Tarkanian, 488 U.S. 179, 191 (1988); *see also* Brentwood Acad. v. Tenn. Secondary Sch. Athletic Ass'n, 531 U.S. 288, 306 (2001) (Thomas, J., dissenting) (describing these two aims of the state action doctrine as set forth in *Lugar* and *Tarkanian*).

[296] *See, e.g.*, Paul Brest, *State Action and Liberal Theory: A Casenote on* Flagg Brothers v. Brooks, 130 U. PA. L. REV. 1296, 1330 (1982) (arguing that the state action doctrine is

'private' action and what is 'state' action is not always easy to determine."[297] Yet the Court is entrenched in a formalistic approach to state action that is devoid of broader constitutional principles for steering the sorting process when it happens that the public and private roles blur. Instead, it has deemed courts' role as one of "sifting facts and weighing circumstances" in individual cases,[298] leaving a dizzying array of outcomes with few common threads. As a consequence, the doctrine mostly fails as such.

In *Lugar v. Edmondson Oil Co.*, the Court erected a two-part analysis for implementing the dual purposes of the state action doctrine,[299] although it has only intermittently employed both parts in subsequent cases.[300] The first prong—whether "the [challenged] deprivation [was] caused by the exercise of some right or privilege created by the State or by a rule of conduct imposed by the State or by a person for whom the State is responsible"[301]—is satisfied if the private actor, in effectuating a constitutional deprivation, acted "with the knowledge of and pursuant to" a law, person, or entity for which the state is responsible.[302] This factor thus requires that the private actor's conduct be in conformity with the rules of the state.[303]

The second part of the *Lugar* formulation does more doctrinal work than the first. It asks whether "the party charged with the deprivation [is] a person who may fairly be said to be a state

---

intellectually inconsistent); John Dorsett Niles, Lauren E. Tribble & Jennifer M. Wimsatt, *Making Sense of State Action*, 51 SANTA CLARA L. REV. 885, 889 (2011) ("[D]eveloping a comprehensive state action approach is impossible because the state action inquiry can arise in limitless factual situations and therefore defies definition.").

[297] Evans v. Newton, 382 U.S. 296, 299 (1966); *see also* Louis Michael Seidman, *The State Action Paradox*, 10 CONST. COMMENT. 379, 391 (1993) ("No area of constitutional law is more confusing and contradictory than state action.").

[298] *Burton*, 365 U.S. at 722.

[299] 457 U.S. at 937.

[300] *See generally Brentwood Acad.*, 531 U.S. at 306 (Thomas, J., dissenting) (noting that the Court has "used many different tests to identify state action").

[301] *Lugar*, 457 U.S. at 937.

[302] Am. Mfrs. Mut. Ins. Co. v. Sullivan, 526 U.S. 40, 50 (1999) (quoting Flagg Bros., Inc. v. Brooks, 436 U.S. 149, 156 (1978)).

[303] In *Lugar*, a corporate defendant was sued for obtaining and executing a writ of attachment of the plaintiff's property pre-judgment. *Lugar*, 457 U.S. at 924–25. The Court found state action for purposes of the plaintiff's due process claim, but not for a claim premised on "unlawful acts" for which "respondents were acting contrary to the relevant policy articulated by the State," as they lacked "the authority of state officials to put the weight of the State behind their private decision." *Id.* at 940.

actor."[304] For this step, the Court begins by identifying "the specific conduct of which the plaintiff complains."[305] Whether such conduct should be held to constitutional standards is then analyzed under two primary tests: (1) the "exclusive government function" or "public function" test which, the Sixth Circuit has explained, looks to whether "the private entity exercises powers which are traditionally exclusively reserved to the state, such as holding elections or eminent domain";[306] and (2) the "entanglement" test, which looks to whether the government compelled, encouraged, authorized, facilitated, or participated in private conduct.[307] Neither test relies on principles of the structural Constitution—such as the separation of powers or achieving government accountability—at any stage in the analysis. As a result, neither operates in a way that could conceivably capture the broader constitutional implications of government outsourcing or the insourcing of data for surveillance.

The highly formalistic public function test has been largely confined to holding elections,[308] empanelling juries,[309] running

---

[304] *Id.* at 937.

[305] *Sullivan*, 526 U.S. at 51 (quoting Blum v. Yaretsky, 457 U.S. 991, 1004 (1982)).

[306] Wolotsky v. Huhn, 960 F.2d 1331, 1335 (6th Cir. 1992) (citing Flagg Bros. Inc. v. Brooks, 436 U.S. 149, 149 (1978); Jackson v. Metro. Edison Co., 419 U.S. 345, 352 (1974)); *see also Flagg Bros., Inc.*, 436 U.S. at 157–62 (discussing the public function test); Nixon v. Condon, 286 U.S. 73, 88–89 (1932) (recognizing that the test is satisfied when parties are acting in matters "intimately connected with the capacity of government").

[307] ERWIN CHEMERINSKY, CONSTITUTIONAL LAW: PRINCIPLES AND POLICIES 529 (4th ed. 2011) (citing Brentwood Acad. v. Tenn. Secondary Sch. Ass'n, 531 U.S. 288 (2001)). Professor Chemerinsky characterizes public function and entanglement as "exceptions" to the ban on holding private actors constitutionally accountable. *Id.* He also identifies a possible third exception—"entwinement," which is entanglement without government encouragement and springs from the Court's decision in *Brentwood Academy*. *Id.* Other scholars have developed taxonomies of state action that divide the entanglement test into multiple separate tests. *See, e.g.*, Julie K. Brown, *Less is More: Decluttering the State Action Doctrine*, 73 MO. L. REV. 561, 564–67 (2008) (identifying seven tests for state action, including the "state agency," the "joint participation," the "state compulsion," and the "symbiotic relationship" tests). Jody Freeman divides entanglement into "joint participation" and "nexus," with the latter governing circumstances in which the private actor is heavily regulated. Freeman, *supra* note 42, at 577.

[308] *See* Terry v. Adams, 345 U.S. 461, 468–70 (1953) (Black, J., plurality) (applying the public function test to elections in which public officials are selected).

[309] *See* Edmondson v. Leesville Concrete Co., 500 U.S. 614, 622 (1991) (holding that the exercise of peremptory challenges in civil cases is state action).

municipalities,[310] and (possibly) operating prisons.[311] Technically, it is limited to circumstances in which the government delegates "an exclusive prerogative of the sovereign" to a private entity,[312] a standard that the Court has not clarified except to hold that the provision of education does not qualify.[313] In *Rendell-Baker v. Kohn*, the Court found that a private, nonprofit school was not a state actor because the state legislature had given the executive branch the option of providing educational services publicly; education was thus not an "exclusive" function of the state.[314]

For its part, the "entanglement test" is not a true test, but an amalgamation of considerations—some factual, some subjective.[315] They include (1) whether the government regulated or licensed the private party, (2) whether the state exercised coercive power over the private party, (3) whether the state encouraged or participated in the private activity in question or otherwise had a "symbiotic relationship" with the private party, and (4) whether the functions and motivations of the private actor were at odds with those of the government.[316] In *Skinner v. Railway Labor Executives Ass'n*, the Court explained that this "nexus" inquiry "necessarily turns on the degree of the Government's participation in the private party's activities, a question that can only be resolved 'in light of all the circumstances.' "[317]

---

[310] *See* Marsh v. Alabama, 326 U.S. 501, 505–06 (1946) (holding that town that was wholly-owned by a corporation was a state actor).

[311] *See* Richardson v. McKnight, 521 U.S. 399, 413 (1997) (holding that privately employed prison guards were not entitled to qualified immunity under 42 U.S.C. § 1983, but reserving the question of whether they acted under color of state law in the first instance).

[312] Flagg Bros., Inc. v. Brooks, 436 U.S. 149, 160 (1978) (holding that warehousemen's proposed sale of goods entrusted to him for storage was not a state action).

[313] *See* Rendell-Baker v. Kohn, 457 U.S. 830, 842 (1982) (holding that education of maladjusted high school students is not the exclusive province of the state).

[314] *Id.* Michele Gilman has thus observed that if the legislature allows functions to be outsourced, "it is hard to see how a privatized service can ever satisfy this interpretation of the public function test." Michele Estrin Gilman, *Legal Accountability in an Era of Privatized Welfare*, 89 CALIF. L. REV. 569, 614 (2001).

[315] Although scholars have subdivided the entanglement approach into numerous distinct tests for state action, *see supra* note 307, the Supreme Court has not formulated it that way. *See* Brentwood Acad. v. Tenn. Secondary Sch. Athletic Ass'n, 531 U.S. 288, 296 (2001) ("Our cases have identified a host of facts that can bear on the fairness of such an attribution.").

[316] *See generally* CHEMERINSKY, *supra* note 307, at 539–51 (explaining these and other considerations to determine the "degree of government involvement" in the action).

[317] 489 U.S. 602, 614 (1989) (quoting Coolidge v. New Hampshire, 403 U.S. 443, 487 (1971)) (citations omitted).

The "totality-of-the-circumstances" nature of the entanglement test has produced inconsistent results. The Court found no state action in *Rendell-Baker*,[318] for example, in which employees sued a nonprofit school after being terminated for engaging in political speech.[319] Even though the school received most of its funding from the state, the Court reasoned, the rationale behind the firings did not pertain to the educational purpose of the public function.[320] In *Brentwood Academy v. Tennessee Secondary School Ass'n*, in contrast, the Court declared a private regulator of public high school athletics a state actor by virtue of school officials' "entwinement . . . in the structure of the association," which was comprised of public school officials and employees eligible for membership in the state retirement system.[321] In dissent, Justice Thomas criticized the majority's finding of state action because the association performed no public function; it was neither created, controlled, or coerced by the state; and it fulfilled no government objective.[322]

The entanglement test incentivizes the government to hand off immense discretion to private parties.[323] The less the government coerces or substantially involves itself in a private activity, the less likely there will be state action and constitutional liability for either party under the test. Indeed, the Supreme Court in *Blum v. Yaretsky* pointed to the *absence* of coercion to justify rejecting a state action argument in the face of other indicia of government influence.[324] *Blum* involved a class of Medicaid recipients seeking

---

318 457 U.S. 830, 843 (1982).

319 *Id.* at 831–35.

320 *Id.* at 840–42.

321 531 U.S. 288, 291, 300 (2001).

322 *Id.* at 309–11 (Thomas, J., dissenting).

323 *See* Metzger, *supra* note 167, at 1424–26. In her exhaustive analysis of government outsourcing under the state action doctrine, Gillian Metzger concludes that the test's essential focus on "close government involvement" fails to account for private parties acting "as independent decisionmakers" under the auspices of government authority. *Id.* at 1424. When government contractually delegates its powers to private parties and *fails* to retain sufficient oversight or control, it "eviscerat[es] the fundamental requirement of constitutional accountability." *Id.* at 1422. Professor Metzger has therefore urged that the focus of state action analysis "shift[ ] to assessing the powers wielded by private entities and away from identifying surreptitious government action," an intriguing approach that is not easily supportable by case law. *Id.* at 1424.

324 457 U.S. 991, 1004–05 (1982) (explaining that the government is "responsible for a private decision only when it has exercised coercive power or has provided such significant

notice and an opportunity for a hearing before a private nursing home could transfer them to another facility.[325] Although the state subsidized the cost of the home, licensed and extensively regulated its operations, and paid for most patients' medical expenses, the physicians and nursing home administrators ultimately made the transfer decisions.[326] The decisions were not "require[d]" by the state, so there was no state action.[327]

The decision in *Burdeau v. McDowell*[328] similarly supports the notion that the government can employ private parties to do what it cannot constitutionally do unilaterally, so long as it distances itself from the act in question. In *Burdeau*, the Supreme Court rejected a criminal defendant's attempt to constitutionally challenge prosecutors' use of books and papers received from a private party who had stolen them.[329] Because "no official of the Federal Government had anything to do with the wrongful seizure of the petitioner's property, or any knowledge thereof until several months after the property had been taken from him," the seizure was not attributable to the government.[330] *Burdeau* thus treats the private and the public spheres as distinct: because a private party—not the government—unlawfully took the defendant's property, the Constitution does not apply to the government's use of that material in a criminal prosecution. It also validates the government's use of the private sector's extra-constitutional status to achieve objectives it could not achieve on its own absent constitutional scrutiny.

B. THE PRIVATE DELEGATION DOCTRINE

The private delegation doctrine offers another approach to limiting the government's ability to partner with the private sector for purposes of engaging in government functions, including

---

encouragement, either overt or covert, that the choice must in law be deemed to be that of the State").

[325] *Id.* at 993.

[326] *Id.* at 994–96.

[327] *Id.* at 1005, 1008–10.

[328] 256 U.S. 465 (1921).

[329] *Id.* at 475–76.

[330] *Id.* at 475. The theory behind *Burdeau* coalesces with the Fourth Amendment's third-party doctrine to essentially insulate the government from constitutional constraints to the extent that it uses the private sector and its data to search or regulate private individuals.

surveillance. In theory, it insists that the powers vested by the Constitution in Congress must be exercised by that branch of government and cannot be transferred elsewhere.[331] Such a claim featured prominently in post-New Deal litigation around the propriety of the burgeoning administrative state.[332] In *Panama Refining Co. v. Ryan*, the Court struck down a provision of the National Industrial Recovery Act (NIRA)[333] that empowered the President to manage a prohibition on interstate shipment of petroleum on the grounds that Congress had set "no criterion to govern the President's course."[334] The Supreme Court has since declined to apply the doctrine on the theory that Congress has broad delegation authority so long as its enabling legislation includes an "intelligible principle" to guide the exercise of discretion.[335] The Court's landmark decision in *Chevron U.S.A., Inc. v. Natural Resources Defense Council, Inc.*[336]—which requires courts to defer to agency constructions of ambiguous statutory text[337]—effectively shores up Congress's authority to hand off legislative power with vague directives to agencies charged with administering a statute.[338]

Two cases challenging congressional attempts to delegate legislative powers to *private* parties reached the Supreme Court around the same time as *Panama Refining*, with similar results. In *A.L.A. Schechter Poultry Corp. v. United States*,[339] the Court held unconstitutional NIRA's authorization of private trade and

---

331 *See* Mistretta v. United States, 488 U.S. 361, 371–72 (1989) ("The nondelegation doctrine is rooted in the principle of separation of powers that underlies our tripartite system of Government. . . . Congress generally cannot delegate its legislative power to another Branch." (citing Field v. Clark, 143 U.S. 649, 692 (1892))).

332 *E.g.*, A.L.A. Schechter Poultry Corp. v. United States, 295 U.S. 495, 537–39, 542 (1935); Pan. Ref. Co. v. Ryan, 293 U.S. 388, 420–21, 425–28, 430 (1935); Metzger, *supra* note 167, at 1437–45 (discussing nondelegation cases in the Supreme Court following the New Deal).

333 15 U.S.C. § 703 (2006).

334 *Pan. Ref. Co.*, 293 U.S. at 415.

335 *Mistretta*, 488 U.S. at 372 (quoting J.W. Hampton, Jr., & Co. v. United States, 276 U.S. 394, 409 (1928)).

336 467 U.S. 837, 843 (1984).

337 *Id.*

338 *See* Richard J. Pierce, Jr., Chevron *and Its Aftermath: Judicial Review of Agency Interpretations of Statutory Provisions*, 41 VAND. L. REV. 301, 305 (1988) (calling the issue of Congress delegating with ambiguous directives the "more controversial point" in *Chevron*).

339 295 U.S. at 495.

industrial groups to draft codes of fair competition—subject to the President's approval—for the sale of chickens.[340] The legislation violated the separation of powers because it enabled businesses "[to] roam at will and the President [to] approve or disapprove their proposal as he may see fit."[341] Congress, the Court explained, "is not permitted to abdicate or to transfer to others the essential legislative functions with which it is thus vested."[342]

In *Carter v. Carter Coal Co.*,[343] the Court again applied the private delegation doctrine to strike down the Bituminous Conservation Coal Act, which authorized coal miners and producers to establish wages and maximum labor hours for mine workers.[344] The statute required no governmental imprimatur before the provisions took effect.[345] "This is legislative delegation in its most obnoxious form," the Court wrote, "for it is not even delegation to an official or an official body, presumptively disinterested, but to private persons whose interests may be and often are adverse to the interests of others in the same business."[346] Grasping for a public-private dividing line, the Court reasoned that "[t]he difference between producing coal and regulating its production is, of course, fundamental. The former is a private activity; the latter is necessarily a governmental function . . . ."[347]

Since the New Deal cases, the Supreme Court has consistently upheld delegations to agencies and private parties alike.[348] Thus,

---

[340] *Id.* at 521–23 & n.4, 542.

[341] *Id.* at 538.

[342] *Id.* at 529.

[343] 298 U.S. 238 (1936).

[344] *Id.* at 278, 310–11.

[345] *Id.* at 310.

[346] *Id.* at 311. The Court further suggested that the delegation violated due process by allowing private parties to regulate competitors. *Id.* This argument is problematic to the extent that it applies procedural due process protections to a legislative versus adjudicative decision. *See* Bi-Metallic Inv. Co. v. State Bd. of Equalization, 239 U.S. 441, 445–46 (1915) (holding that "a general determination" affecting a large number of people in unexceptional ways is not bound by due process).

[347] *Carter Coal*, 298 U.S. at 311.

[348] *See, e.g.*, Whitman v. Am. Trucking Assocs., 531 U.S. 457, 472–74 (2001) (holding that the phrase, "requisite to protect the public health," was sufficiently determinate to guide the EPA's establishment of national ambient air quality standards under the Clean Air Act); Currin v. Wallace, 306 U.S. 1, 15–16 (1939) (upholding statute requiring two-thirds of regulated industry to approve regulations before they could take effect); Sunshine

as Jody Freeman has observed, "[r]esurrecting the nondelegation doctrine to invalidate private delegations on the theory that some 'public' functions are nondelegable would . . . require heavy conceptual lifting."[349] Yet she and others have called private delegations more troubling "than the broadest delegations to public agencies."[350] If private delegations were not especially noxious, *Carter Coal* would call into question the propriety of legislative delegations to administrative agencies—and thus the viability of the federal regulatory state itself. In its present form, the private delegation doctrine does not answer the threshold question of whether the Constitution can be read to ban the outsourcing of legislative power to private parties, however defined, while preserving the rulemaking function of modern executive branch agencies.

C. THE FOURTH AMENDMENT

In litigation pending across the country, the primary doctrinal battleground for challenging the NSA's use of third-party data for surveillance has been the Fourth Amendment, rather than the state action or private delegation doctrines.[351] This stands to reason. The Supreme Court has recognized that "[t]he overriding function of the Fourth Amendment is to protect personal privacy and dignity against unwarranted intrusion by the State."[352] In *Mapp v. Ohio*, the Court went so far as to characterize it as establishing a "*right* to privacy, no less important than any other right carefully and particularly reserved to the people."[353] The Fourth Amendment grew out of the Framers' concern "that indiscriminate searches and seizures conducted under the

---

Anthracite Coal Co. v. Adkins, 310 U.S. 381, 388, 393 (1940) (upholding statute that allowed coal industry members to fix prices in accordance with statutory standards).

[349] Freeman, *supra* note 42, at 584.

[350] *Id.* at 583–84 (citing Harold J. Krent, *Fragmenting the Unitary Executive: Congressional Delegations of Administrative Authority Outside the Federal Government*, 85 NW. U. L. REV. 62, 69 n.17 (1990); David M. Lawrence, *The Private Exercise of Governmental Power*, 61 IND. L.J. 647, 649–50 (1986)).

[351] *See NSA Surveillance Lawsuit Tracker*, PROPUBLICA, http://projects.propublica.org/graphics/surveillance-suits#In%20re%20National%20Security%20Letter%202011 (last visited Feb. 22, 2015) (listing pending cases). As noted previously, this Article does not analyze the statutory, First Amendment or due process challenges to NSA surveillance programs.

[352] Schmerber v. California, 384 U.S. 757, 767 (1966).

[353] 367 U.S. 643, 656 (1961) (emphasis added).

authority of 'general warrants' were . . . immediate evils" to be avoided by, first, "protecting the basic right to be free from unreasonable searches and seizures" and, second, "requiring that warrants be particular and supported by probable cause."[354]

Originally construed as the physical invasion of a person or property, a search within the meaning of the Fourth Amendment occurs "when the government violates a subjective expectation of privacy that society recognizes as reasonable."[355] The reasonable expectation of privacy trigger is a tricky means of confining the government's collection and use of third party data for surveillance, however. The reason for this mirrors the problem plaguing the state action and private delegation doctrines: the illusion that the public and private spheres are severable for purposes of constitutional law. In essence, prevailing Fourth Amendment doctrine treats the existence of a third party intermediary as a waiver of constitutional protections, in two ways. First, the Court has long declared that "[w]hat a person knowingly exposes to the public, even in his home or office, is not a subject of Fourth Amendment protection."[356] Thus, there is no reasonable expectation of privacy in abandoned property, like garbage left out for collection,[357] or in the movements of an automobile on public thoroughfares,[358] because it is available for members of the public to view.[359]

Second, the Court has repeatedly held that "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government

---

[354] Payton v. New York, 445 U.S. 573, 583–84 (1980). The Fourth Amendment provides that

> [t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. CONST. amend. IV.

[355] Kyllo v. United States, 533 U.S. 27, 31–33 (2001). A search also occurs if there is physical trespass. *See* Olmstead v. United States, 277 U.S. 438, 466 (1928), *overruled in part by* Katz v. United States, 389 U.S. 347 (1967); Berger v. New York, 388 U.S. 41 (1967).

[356] Katz v. United States, 389 U.S. 347, 351 (1967).

[357] California v. Greenwood, 486 U.S. 35, 37 (1988).

[358] United States v. Knotts, 460 U.S. 276, 281 (1983).

[359] *Id.* at 281–82.

authorities."[360] The Court has thus found no Fourth Amendment ban on the use of information obtained through government informants.[361] Most notably, it found in *Smith v. Maryland* that there is no reasonable expectation of privacy in phone numbers dialed[362] because callers "voluntarily convey numerical information to the phone company and 'expose[ ]' that information . . . in the ordinary course of business."[363] Providing tax documents to an accountant similarly relinquishes Fourth Amendment protections.[364] The Court has held that bank customers have no reasonable expectation of privacy in records "contain[ing] only information voluntarily conveyed . . . and exposed to [bank] employees in the ordinary course of business."[365] Nor is the Fourth Amendment violated if a physician provides the state with copies of medical information.[366]

With the advent of the Internet, some lower courts have applied the third party doctrine to authorize warrantless government access to shared computer files, information sent or received through the Internet and stored on a third party server,[367] and

---

[360] United States v. Miller, 425 U.S. 435, 443 (1976) (citing United States v. White, 401 U.S. 745, 752 (1971); Hoffa v. United States, 385 U.S. 293, 302 (1966); Lopez v. United States, 373 U.S. 427, 437–39 (1963)). The Supreme Court has also held that "a party incriminated by evidence produced by a third party sustains no violation of his own Fifth Amendment rights." Cal. Bankers Ass'n v. Shultz, 416 U.S. 21, 55 (1974) (citing Johnson v. United States, 228 U.S. 457, 458 (1913); Couch v. United States, 409 U.S. 322, 328 (1973)). Hence, the Fifth Amendment does not protect against subpoenas for a person's records and papers held by third parties. *Couch*, 409 U.S. at 328, 333–35.

[361] United States v. White, 401 U.S. 745, 748–49 (1971); *see also* Hoffa v. United States, 385 U.S. 293, 302 (1966) (no Fourth Amendment protection for conversations with a colleague who turns out to be a government agent); Lewis v. United States, 385 U.S. 206, 211 (1966) (same regarding interactions with secret agent sent by the government to purchase narcotics from defendant); *Lopez*, 373 U.S. at 437–39 (same regarding agent's use of electronic recording equipment).

[362] Smith v. Maryland, 442 U.S. 735, 741–42 (1979).

[363] *Id.* at 744.

[364] *Couch*, 409 U.S. at 335–36.

[365] *Miller*, 425 U.S. at 442; *see also* United States v. Payner, 447 U.S. 727, 728–32 (1980) (holding that a criminal defendant had no standing to suppress documents illegally seized from a briefcase of an officer of a Bahamian bank because he had no privacy interest in them); *Cal. Bankers Ass'n*, 416 U.S. at 54 (holding that regulatory mandates that banks keep customer records for government scrutiny did not violate the Fourth Amendment).

[366] Whalen v. Roe, 429 U.S. 589, 604 n.32 (1977).

[367] Junichi P. Semitsu, *From Facebook to Mug Shot: How the Dearth of Social Networking Privacy Rights Revolutionized Online Government Surveillance*, 31 PACE L. REV. 291, 338 & nn.814–85 (2011) (citing cases).

individual subscriber information from an ISP.[368] In the words of the Ninth Circuit, the rationale is that "computer surveillance techniques that reveal the to/from addresses of e-mail messages, the IP addresses of websites visited and the total amount of data transmitted to or from an account . . . are constitutionally indistinguishable from the use of a pen register that the Court approved in *Smith*."[369]

Lower courts are also split on the question of whether the third party doctrine enables the government to capture electronic information about an individual's location at a specific time—such as cell phone tower data—without a warrant. Following the Third Circuit, the Eleventh Circuit in *United States v. Davis* held that the Fourth Amendment applies to cell phone location information because " 'a cell phone customer has not "voluntarily" shared his location information with a cellular provider in any meaningful way' " and is likely " '[un]aware that . . . cell phone providers collect and store historical location information.' "[370] The court rejected the reasoning of the Fifth Circuit,[371] which had previously applied *Smith* to find no reasonable expectation of privacy in cell phone records on the rationale that "[c]ell phone users . . . understand that their service providers record their location information when they use their phones at least to the

---

[368] *See, e.g.*, United States v. Perrine, 518 F.3d 1196, 1204 (10th Cir. 2008) (noting also that "[e]very federal court to address th[e] issue has held that subscriber information . . . [from an ISP] is not protected by the Fourth Amendment[ ] . . ."); *see also* Semitsu, *supra* note 367, at 338 n.186 (2011) (citing cases).

[369] United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2007). The Sixth Circuit in *Warshak v. United States* reached the opposite conclusion, although the decision was vacated on other grounds. 490 F.3d 455, 473 (6th Cir. 2007) (holding that a sender of electronic mail has a reasonable expectation of privacy in messages residing with an ISP), *vacated in part*, 532 F.3d 521, 525–26 (6th Cir. 2008) (en banc) (finding that the question whether government should be enjoyed from searching criminal suspect's e-mails without a warrant was not ripe).

[370] 754 F.3d 1205, 1217 (11th Cir. 2014), *reh'g granted*, 573 Fed. App'x 925 (2014) (quoting *In re* Application of U.S. for an Order Directing a Provider of Elec. Comm'n Serv. to Disclose Recs. to Gov't, 620 F.3d 304, 317 (3d Cir. 2010)); *see also In re* Application of U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d 113, 119–20 (E.D.N.Y. 2011) (concluding that a law enforcement request for cell site information raises even greater privacy concerns than installation of a GPS device on a vehicle because "cell-site-location records . . . enable 'mass' or 'wholesale' electronic surveillance" of the "vast majority of Americans").

[371] *Davis*, 754 F.3d at 1211–12, 1217.

same extent landline users in *Smith* understood that the phone company recorded the numbers they dialed."[372]

Another open question is whether *Smith* bars Fourth Amendment scrutiny of the NSA's data surveillance programs. In *Klayman v. Obama*,[373] the U.S. District Court for the District of Columbia concluded that "the relationship between the NSA and telecom companies [has] become so thoroughly unlike those considered by the Supreme Court thirty-four years ago that a precedent like *Smith* simply does not apply."[374] In contrast, in an opinion that was vacated on other grounds, the Southern District of New York construed *Smith* as strictly holding "that individuals have 'no legitimate expectation of privacy' regarding the telephone numbers they dial because they knowingly give that information to telephone companies."[375]

Together with the state action doctrine and the private delegation doctrine, the Fourth Amendment's third party doctrine leaves open the question whether the Constitution can be meaningfully invoked when the government outsources its responsibilities to the private sector—either overtly or by capturing private sector surveillance for its own use. The next Part maps out a method for constitutionalizing how the government structures its reliance on the private sector for its own functions.[376]

V. TOWARDS A RELEVANT CONSTITUTION IN AN ERA OF OUTSOURCING AND DATA INSOURCING

Scholars have recognized that prevailing constitutional doctrine has left technology-related privacy protections largely in the hands

---

[372] *In re* Application of U.S. for Historical Cell Site Data, 724 F.3d 600, 613 (5th Cir. 2013) (citing Smith v. Maryland, 442 U.S. 735 (1979); United States v. Madison, No. 11-60285-CR, 2012 WL 3095357, at *8 (S.D. Fla. July 30, 2012)).

[373] 957 F. Supp. 2d 1 (D.D.C. 2013).

[374] *Id.* at 31.

[375] ACLU v. Clapper, 959 F. Supp. 2d 724, 479 (S.D.N.Y. 2013), *vacated and remanded*, No. 14-42, 2015 WL 2097814 (2d Cir. May 7, 2015).

[376] To be sure, there are policy reasons for confining constitutional doctrine to its current boundaries; this Article sets the doctrinal groundwork for the debate without fully engaging the normative implications.

of legislators and regulators.[377] But legislative responses to the government's increasing reliance on the private sector should not evolve in a constitutional vacuum. Viable arguments exist for reworking existing constitutional doctrine to require that the government structure its outsourcing and data insourcing programs so as to preserve its own accountability to the people.[378]

A. PRESUMPTIONS AND THE STRUCTURAL CONSTITUTION

Commentators briskly debate the need for and proper approach to legislative reform of surveillance laws,[379] and strong arguments exist for leaving privacy protections to Congress. Judges lack the technological expertise to understand the full implications of a Fourth Amendment case within a vast array of rapidly evolving technologies and, in understanding them further, are constrained by the arguments and evidence presented to them by lawyers.[380] Courts are also confined to operate within outdated doctrinal rules. Legislatures and regulators, by contrast, can seek input from experts on a macro level, unrestrained by the facts and issues in a particular case.[381] They are more procedurally flexible than courts, and thus capable of responding to technological change more swiftly and adeptly.[382]

Without a constitutional anchor to drive further reforms, however, legislative solutions to the problems associated with outsourcing and data insourcing remain dependent on the

---

[377] *See* Kerr, *supra* note 138, at 630 ("Congress has responded to this constitutional vacuum with a series of laws that offer relatively strong (although hardly perfect) legislative privacy protections.").

[378] In the aftermath of the Snowden scandal, outraged politicians, the ACLU, telecommunications companies, and concerned citizens have invoked the courts to obtain constitutional redress for perceived overreaching by the NSA despite the statutory backdrop to its actions. *NSA Surveillance Lawsuit Tracker*, *supra* note 351.

[379] *See, e.g.*, Kerr, *supra* note 138, at 638–42 (arguing that criticisms of the USA PATRIOT Act's pen register amendments are misplaced).

[380] *See* Riley v. California, 134 S. Ct. 2473, 2497–98 (2014) (Alito, J., concurring) ("Legislatures, elected by the people, are in a better position than we are to assess and respond to the changes that have already occurred and those that almost certainly will take place in the future."); Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 807 (2004) (arguing that Congress—and not the courts interpreting the Constitution—is a better responder to the privacy threats of emerging technologies).

[381] Kerr, *supra* note 380, at 807–08.

[382] *Id.*

providence of political coalitions and congressional will. The Constitution is not so fickle. Its importance as a backstop for legislative protections of important rights like privacy derives from the structure of the national government. As Judge J. Harvie Wilkinson III of the Fourth Circuit has observed, "[i]f the courts are to function as interpreters of constitutional rights, they must necessarily function as arbiters of constitutional structure."[383] James Madison understood this, explaining in *The Federalist No. 10* that the "proper structure of the Union" operates to protect minorities from dangerous factions.[384] The Supreme Court has relied on the Constitution's structure—as distinct from its enumerated government functions and provisions enshrining individual rights—to uphold states' immunity from suit,[385] the President's appointment power,[386] limits on federal control of state law enforcement officers,[387] and Congress's powers under the Commerce Clause,[388] to name only a few examples.[389]

One such principle of constitutional structure is the foundational assumption that the government is accountable to the people.[390] Madison wrote in *The Federalist No. 49* that "the people are the only legitimate fountain of power."[391] In *The Federalist No. 78*, he argued that legislative acts "contrary to the Constitution" are invalid because "[t]o deny this, would be to affirm, that the deputy is greater than his principal; that the servant is above his master; that the representatives of the people are superior to the people themselves."[392] The Supreme Court has consistently reinforced the notion that government exercises only delegated powers channeled from the people through the

---

383 J. Harvie Wilkinson III, *Our Structural Constitution*, 104 COLUM. L. REV. 1687, 1690–91 (2004).

384 THE FEDERALIST NO. 10, at 47–53 (James Madison) (Ian Shapiro ed., 2009).

385 Alden v. Maine, 527 U.S. 706, 713 (1999).

386 Freytag v. Comm'r, 501 U.S. 868, 870, 878 (1991).

387 Printz v. United States, 521 U.S. 898, 935 (1997).

388 Garcia v. San Antonio Metro. Transit Auth., 469 U.S. 528, 555–56 (1985).

389 *See generally* Aziz Z. Huq, *Standing for the Structural Constitution*, 99 VA. L. REV. 1435, 1443–48 (2013) (describing structural constitutional litigation in federal court).

390 *See generally* Brown, *supra* note 8, at 456–57 (proposing a constitutional accountability doctrine that would tether the exercise of federal power to the people).

391 THE FEDERALIST NO. 49, *supra* note 384, at 256 (James Madison).

392 THE FEDERALIST NO. 78, *supra* note 384, at 393 (James Madison).

Constitution.[393] Accountability and the idea of government by the people are inextricable: because the people retain the ultimate power of government, those who hold public power must be accountable to the populace. Likewise, in order for there to be accountability under our Constitution, the source of federal power—the people—must have some say in its exercise.

Under outsourcing regimes, the relational hierarchies that exist within a government bureaucracy and constitutional democracy are replaced by the happenstance of contractual terms. Private contractors are consequently less accountable to the voting public than government actors functioning within the umbrella of the executive branch and under an ongoing threat of judicial review.[394] Blind spots in applicable laws keep the scope of the government's access to private sector surveillance data beyond public view, compromising voters' ability to hold legislators and the executive branch accountable.[395] The viability of a political solution also depends on a functioning Congress, the relative priority of other

---

[393] *See* McCulloch v. Maryland, 17 U.S. 316, 403 (1819) ("The government proceeds directly from the people; is 'ordained and established' in the name of the people . . . ."); Downes v. Bidwell, 182 U.S. 244, 359 (1901) (Fuller, C.J., dissenting) ("[N]o utterance of this court has intimated a doubt that in its operation on the people, by whom and for whom it was established, the national government is a government of enumerated powers, the exercise of which is restricted to the use of means appropriate and plainly adapted to constitutional ends, and which are 'not prohibited, but consist with the letter and spirit of the Constitution.' " (quoting *McCulloch*, 17 U.S. at 421)); Hawke v. Smith, 253 U.S. 221, 226–27 (1920) ("[t]he Constitution of the United States was ordained by the people," who "grant" authority to Congress, and "[i]t is not the function of courts or legislative bodies, national or state, to alter the method which the Constitution has fixed"); U.S. Term Limits, Inc. v. Thorton, 514 U.S. 779, 821 (1995) ("[T]he Framers, in perhaps their most important contribution, conceived of a Federal Government directly responsible to the people, possessed of direct power over the people, and chosen directly, not by States, but by the people."); *see also* INS v. Chadha, 462 U.S. 919, 951 (1983) ("When any Branch acts, it is presumptively exercising the power the Constitution has delegated to it."); Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 640 (1952) (Jackson, J., concurring) ("[T]he Federal Government as a whole, possesses only delegated powers. The purpose of the Constitution was not only to grant power, but to keep it from getting out of hand."); Reynolds v. Sims, 377 U.S. 533, 568 (1964) (relying on the Gettysburg Address formulation of "government of the people, by the people, for the people" to constitutionally require roughly equal representation of voters in state legislative districts); Harper v. Va. State Bd. of Elections, 383 U.S. 663, 667 (1966) (observing that in *Reynolds* the Court noted that the Equal Protection Clause "is an essential part of the concept of a government of laws and not men" and "is at the heart of Lincoln's vision of 'government of the people, by the people, [and] for the people' " (quoting *Reynolds*, 377 U.S. at 568)).

[394] *See* Brown, *supra* note 191, at 1351–52.

[395] *See supra* notes 163–65 and accompanying text.

issues competing for political attention, and the power of interested lobbying groups to influence the legislative process.[396] Such factors have little bearing on the legitimacy of the privacy concerns created by the expansion of data-related surveillance and as a consequence the concerns are left unaddressed.

Importantly, privacy rights are not grounded in Congress's discretionary exercise of its constitutional powers—but in the Constitution itself. The Supreme Court has acknowledged that the Bill of Rights reflects the Framers' concern for protecting specific aspects of physical privacy,[397] such as privacy of speech and assembly (First Amendment);[398] privacy of the home against demands that it be used to house soldiers (Third Amendment);[399] privacy of the person and possessions against unreasonable searches (Fourth Amendment);[400] and informational privacy (Fifth Amendment privilege against self-incrimination).[401]

Under prevailing doctrine, however, the private nature of the government's data source dictates whether constitutional privacy guarantees apply to surveillance conducted using that data.[402] The government can effectively hide behind the private sector's extra-constitutional status and evade accountability for an unprecedented level of prying. The same phenomenon holds true

---

396 *See* Matthew A. Cahn, *The Players: Institutional and Noninstitutional Actors in the Policy Process*, *in* PUBLIC POLICY: THE ESSENTIAL READINGS 201–11 (Stella Z. Theodoulou & Matthew A. Cahn eds., 1995) (indicating that the political process is much more complicated than it appears, involves a number of actors, and that "[t]he role each actor plays, in combination with the relationship between actors in both policy bureaucracies, is what ultimately determines policy outcomes").

397 *See* Griswold v. Connecticut, 381 U.S. 479, 484 (1965) (recognizing a right to decisional privacy on the theory that "the specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance," and that some of those guarantees "create zones of privacy"); Whalen v. Roe, 429 U.S. 589, 599 n.25 (1977) (quoting *Griswold*, 381 U.S. at 484, in a Fourth Amendment context); Cal. Bankers Ass'n v. Shultz, 416 U.S. 21, 78–79 (1974) (Powell, J., concurring) ("Financial transactions can reveal much about a person's activities, associations, and beliefs. At some point, governmental intrusion upon these areas would implicate legitimate expectations of privacy."). In subsequent decisions, the privacy right has come to encompass matters such as child rearing, procreation, and termination of medical treatment as a matter of due process. *See* Bowers v. Hardwick, 478 U.S. 186, 190 (1986) (listing the cases that have protected activities on the grounds of privacy).

398 U.S. CONST. amend. I.

399 *Id.* amend. III.

400 *Id.* amend. IV.

401 *Id.* amend. V.

402 *See supra* notes 15–18 and accompanying text.

for government outsourcing. Decisions to outsource are made without constitutional restraint, and once a function is outsourced, the Constitution does not apply to confine how private parties carry it out. Constitutional accountability should instead operate as a structural principle that limits how government outsourcing and data insourcing occurs, shifting courts away from the public-versus-private focus that has stagnated evolution of the law to date. Such a functional principle of constitutional accountability is already at play in state action, private delegation, and Fourth Amendment doctrine.

B. STATE ACTION AS A DOCTRINE OF GOVERNMENT ACCOUNTABILITY

State action doctrine is ostensibly a means of holding private actors accountable for constitutional violations.[403] It is a quasi-jurisdictional doctrine that helps define the breadth of the Constitution's reach when it comes to government actions taken in tandem with the private sector.[404] The substantive obligations enforced via the state action doctrine come from the substance of the Constitution itself.[405] As currently applied, the state action doctrine is an "all-or-nothing approach."[406] A private actor is a state actor under the doctrine for all purposes, including financial liability for damages to individual constitutional rights.[407] If the state action doctrine were softened to recognize that public-private relationships operate on a continuum,[408] with no clear line dividing the public and the private sectors, it could be recalibrated to prompt a narrower remedy in appropriate cases, i.e., an order

---

[403] *See* Metzger, *supra* note 167, at 1410 ("State action doctrine remains the primary tool courts use to ensure that private actors do not wield government power outside of constitutional constraints.").

[404] *See id.* at 1501 (noting that the current doctrine targets government involvement or persuasive entwinement with private actors).

[405] *See* Kimberly N. Brown, *Government by Contract and the Structural Constitution*, 87 NOTRE DAME L. REV. 491, 504 (2011) (noting that the doctrine asks when "private parties should be treated as government actors" and "susceptible to liability for violations of individual constitutional rights").

[406] Metzger, *supra* note 167, at 1431 & n.223.

[407] *See id.* ("If state action is found, constitutional requirements directly apply in full force to the private entity.").

[408] *See* Brown, *supra* note 405, at 507–12 (arguing that public-private relationships fall on a constitutional continuum).

directing that *the government* structure outsourcing relationships in ways that ensure government accountability.

In *Lugar v. Edmonson Oil Co.*,[409] the Court described the state action doctrine's twin aims as preserving private autonomy and freedom and relieving the state of responsibility for conduct that *the state cannot control*.[410] The Court identified the first question in a state action analysis as whether "the deprivation [was] caused by the exercise of some right or privilege created by the State or by a rule of conduct imposed by the State or by a person for whom the State is responsible."[411] The second factor—whether "the party charged with the deprivation . . . may fairly be said to be a state actor"—exists because, "[w]ithout a limit such as this, private parties could face constitutional litigation whenever they seek to rely on some state rule governing their interactions with the community surrounding them."[412]

The *Lugar* formulation accordingly hinges on a determination that unconstitutional conduct is, in the first instance, the product of some activity for which the state is responsible. Ultra vires action by a private party is not state action. By the same token, the test "avoids imposing on the State, its agencies or officials, responsibility for conduct for which they cannot fairly be blamed."[413]

In *Lugar*, a private party used a prejudgment attachment procedure to secure property in satisfaction of a debt.[414] The procedure required only an ex parte petition that the creditor believed that the owner might dispose of the property to defeat his creditors.[415] The debtor sued the creditor under 42 U.S.C. § 1983, alleging that it had acted jointly with the state to deprive him of due process.[416] The Court dismissed the count of the complaint challenging the creditor's "malicious" and "wanton" acts because

---

409 457 U.S. 922 (1982).

410 *Id.* at 936 (advocating "careful adherence" to the doctrine to achieve these aims).

411 *Id.* at 937.

412 *Id.*

413 *Id.* at 936.

414 *Id.* at 924.

415 *Id.* (describing the prejudgment attachment procedure requirement).

416 *Id.* at 925. The Court held that the state action inquiry is identical to the "under color of state law" inquiry for purposes of § 1983. *Id.* at 935.

they were not attributable to the state.[417] As for the claim that the prejudgment attachment procedures themselves were insufficient, however, the creditor was a state actor.[418] The Court explained: "While private misuse of a state statute does not describe conduct that can be attributed to the State, the procedural scheme created by the statute obviously is the product of state action."[419] Thus, it concluded, "Petitioner did present a valid cause of action under § 1983 insofar as he challenged the constitutionality of the Virginia statute."[420] By contrast, in *Moose Lodge No. 107 v. Irvis*,[421] a private club's refusal to serve an African-American was not attributable to the state by virtue of a regulatory scheme enforced by the state liquor board because "there [wa]s no suggestion . . . that the Pennsylvania statutes and regulations governing the sale of liquor [we]re intended either overtly or covertly to encourage discrimination."[422]

In the traditional public service contract scenario, the government has levers of control over private contractors that it can employ if it so chooses. It can require stiffer contract terms to define and restrict a contractor's responsibilities or outline meaningful consequences in the event of a breach.[423] Or it can impose additional regulatory requirements on the contracting process, such as APA-type procedures and FOIA transparency.[424] If the remedies available under the state action doctrine were recalibrated to require that *the government* structure its relationships with the private sector in ways that protect the public interest, there could be pressure on government—through the courts—to remedy problems with compliance and accountability in creative ways.

---

[417] *Id.* at 940.

[418] *Id.* at 940–42.

[419] *Id.* at 941.

[420] *Id.* at 942.

[421] 407 U.S. 163 (1972).

[422] *Id.* at 164–65, 173; *see also Lugar*, 457 U.S. at 937–38 (distinguishing *Moose Lodge* based on the disconnect between state law and the defendant's discriminatory policies in that case).

[423] *See* Metzger, *supra* note 167, at 1372–73 & n.10 (noting scholars who have proposed greater contractual controls on private entities to increase accountability).

[424] *See id.* (noting scholars who have proposed regulatory approaches).

The opinion in *Skinner v. Railway Labor Executives Ass'n*[425] demonstrates how the state action doctrine might operate to prompt injunctions requiring that the government structure outsourcing relationships to establish lines of constitutional accountability. In *Skinner*, labor groups brought suit to enjoin regulations promulgated by the Federal Railroad Administration (FRA) that authorized railroads to conduct drug and alcohol testing on employees.[426] The FRA argued that the Fourth Amendment did not apply because private railroads were responsible for implementing the regulatory provisions on testing, which were not mandatory.[427] The Supreme Court disagreed, holding that "[a] railroad that complies with the . . . regulations does so by compulsion of sovereign authority, and the lawfulness of its acts is controlled by the Fourth Amendment."[428] Thus, the Court found state action even though the tests were not compulsory.[429] Although it found no Fourth Amendment violation on the merits, the Court indicated that the case could have been resolved by requiring the government to include greater protections for railroad workers in its implementing regulations. On the facts before it, the Court reasoned, enjoining the government to add a regulatory warrant requirement "would add little to the assurances of certainty and regularity already afforded by the regulations, while significantly hindering, and in many cases frustrating, the objectives of the Government's testing program."[430] The Court's underlying premise, consistent with the *Lugar* formulation, was that the government could have been directed as a matter of the state action doctrine to properly dictate the terms of the private party's service—terms that it could control.

Similarly, in *Blum v. Yaretsky*,[431] the Court could have directed *the state* to amend its regulations bearing on private nursing homes to avoid violations of constitutional rights. In *Blum*, Medicaid recipients challenged private decisions to transfer or

---

425 489 U.S. 602 (1989).

426 *Id.* at 610–12.

427 *Id.* at 614.

428 *Id.*

429 *Id.* at 614–16 (describing the quasi-compulsory factors of the regulation).

430 *Id.* at 624.

431 457 U.S. 991 (1982).

discharge them, arguing that they were entitled to notice and a hearing as a matter of due process.[432] The Court found no state action because the decisions to transfer or discharge "ultimately turn[ed] on medical judgments made by private parties according to professional standards."[433] An order enjoining the state to amend its regulations to provide notice and a hearing prior to a transfer or termination decision—an action over which the state has control under the *Lugar* rationale for the state action doctrine—would not have disturbed the private actors' ability to exercise their professional discretion.[434] Hence, *Blum* coalesces with the idea that the state action doctrine could be applied to "find[ ] public accountability in the circumstances."[435] On this theory, plaintiffs suing the government for injunctive relief could seek an order forcing it to alter the terms of its outsourcing relationships to ensure accountability for the exercise of its functions.[436]

By way of example, suppose that DHS enters into a contract with Booz Allen to "assist Homeland Security in developing a bio-defense and health-preparedness infrastructure to ensure the security of the nation."[437] Suppose further that the contract specifically directs Booz Allen to develop training and security protocols for United States medical personnel in the event of a

---

[432] *Id.* at 995–96.

[433] *Id.* at 1008.

[434] *See id.* at 1008–09 (analogizing the medical professionals' discretion to that of a public defender); Gilman, *supra* note 314, at 612–17 (arguing that requiring the state in *Blum* to change the regulations to provide for notice and a hearing would be more consistent with the purposes of the state action doctrine than the Court's finding of no state action).

[435] Brentwood Acad. v. Tenn. Secondary Sch. Athletic Ass'n, 531 U.S. 288, 303 (2001). The Court in *Brentwood Academy* noted that "[e]ven facts that suffice to show public action (or, standing alone, would require such a finding) may be outweighed in the name of some value at odds with finding public accountability in the circumstances," *id.*, such as the public defender's need to retain an adversarial posture vis-à-vis the State, *id.* at 304 (citing Polk Cty. v. Dodson, 454 U.S. 312, 323 n.3 (1981)).

[436] Whether plaintiffs would have Article III standing to sue for such an injunction is an important question that is beyond the scope of this Article. Nor does this Article address the intersections with the law governing facial versus as-applied constitutional challenges to statutes and regulations. *See* Michael C. Dorf, *Facial Challenges to State and Federal Statutes*, 46 STAN. L. REV. 235, 239 (1994) (observing that the bar for succeeding on a facial challenge is higher than for as-applied challenges).

[437] *Homeland Security*, BOOZ ALLEN, http://www.boozallen.com/consultants/civilian-government/homeland-security-consulting/dhs-strategy-technology-management (last visited Feb. 23, 2015).

bioterrorist attack involving an infectious disease pathogen such as the pneumonic plague. Booz Allen's protocols ultimately exclude a certain class of health care workers from first-line antibiotic treatment in the event of a mass exposure. Janet Schmendrick is a hospital attendant who would not be eligible for the first round of antibiotic treatments under Booz Allen's protocols. She sues DHS and Booz Allen for an injunction mandating revision of the protocols.[438] Janet's substantive constitutional claim is that the existing protocols violate equal protection, as the vast majority of workers affected are women. To be sure, Booz Allen exercises discretion in devising the protocols, much like the medical personnel in *Blum*.[439] Under the prevailing construction of state action, therefore, the suit against Booz Allen could be dismissed on the grounds that Booz is a private actor that is not operating under the compulsion of the state. On a constitutional accountability approach to state action, however, Janet could rely on *Skinner* and the first prong of the *Lugar* test to argue that, for purposes of her facial challenge,[440] Booz is a state actor functioning pursuant to government directives, which DHS should amend to conform to the Equal Protection Clause. The state action doctrine's objective of protecting Booz Allen from liability for money damages is no longer at stake if the all-or-nothing approach to state action is revised to limit the relief available to Janet.[441] Nor is there a viable concern that the government will be held liable for conduct it cannot control.

The Court's decision in *Shelley v. Kraemer*[442] is particularly instructive for purposes of evaluating how a repackaging of state action remedies might apply to data insourcing. Suppose again that Janet Schmendrick separately sues the NSA along with a host of private companies for an injunction imposing mandatory protocols regarding how her personal data is collected, used, stored, and shared. Fearing that she is being constantly tracked, Janet raises a

---

438 She might face standing and ripeness problems, but they are beside the point made here.

439 *See supra* notes 327, 431–34 and accompanying text.

440 *See supra* notes 425–30 and accompanying text.

441 To be sure, whether it would be appropriate and advisable to recalibrate the state action doctrine to enable a continuum of possible relief requires further thought, including an analysis of what level of state involvement would trigger the full panoply of money damages.

442 334 U.S. 1 (1948).

host of possible constitutional theories, such as equal protection (arbitrary surveillance), the First Amendment (chilled speech and association rights), the Fourth Amendment (unreasonable general warrant), and the Fifth Amendment (informational privacy).[443] Janet might use *Shelley* to argue that, for purposes of obtaining injunctive relief, the government's use of her data transformed its collection by the private sector into state action. In *Shelley*, the Court held that judicial enforcement of private covenants restricting the sale of property to Caucasians was state action even though the covenants were voluntarily entered into by private parties: "It is clear that but for the active intervention of the state courts, supported by the full panoply of state power, petitioners would have been free to occupy the properties in question without restraint."[444] The Court invalidated lower court judgments enforcing the covenants, finding that they violated equal protection.[445] Thus, the relief granted was essentially injunctive—non-enforcement of a lower court judgment.

Janet might justify her request for injunctive relief on the theory that state action exists because the NSA's use of her data caused her constitutional deprivation. Although the government sourced the data from private parties who collected it from her voluntarily, these factors—private action devoid of government compulsion—existed in *Shelley*.[446] In effect, such an analysis subsumes the second prong of the *Lugar* formation (i.e., is the private actor a state one) within the first (i.e., whether the deprivation was caused by the State). The second prong's purpose of protecting private parties from constitutional liability for money damages when they rely on rules of the State loses its resonance.[447] Instead, the state action doctrine would highlight an objective that is implicit in the first prong of *Lugar*: ensuring that the government does not evade its constitutional obligations on the pretense that the public and private sectors are severable for

---

[443] This Article takes no position on the viability or strength of these theories beyond the Fourth Amendment discussion contained herein.

[444] *Shelley*, 334 U.S. at 19.

[445] *Id.* at 20.

[446] *See id.* at 4–6 (describing the restrictive covenants adopted by private parties).

[447] *See* Lugar v. Edmondson Oil Co., 457 U.S. 922, 937 (1982) (stating that the two principles "collapse into each other when the claim of constitutional deprivation is directed against a party whose official character is such as to lend the weight of the state to his decisions").

purposes of the structural Constitution. To be sure, superimposing state action on a private party whose data is insourced into government coffers significantly stretches the state action from its current doctrinal posture.[448] But its potential for imposing constitutional limits on big data surveillance activity that surely warrants such boundaries is formidable.

C. THE PRIVATE DELEGATION DOCTRINE, *DEPARTMENT OF TRANSPORTATION V. ASS'N OF AMERICAN RAILROADS*, AND CONSTITUTIONAL ACCOUNTABILITY

The so-called private and non-delegation doctrines have long been considered moribund as a meaningful check on government decisions to hand off sovereign powers to private parties.[449] Yet just recently, in *Department of Transportation v. Ass'n of American Railroads*,[450] a faction of the Court signaled a willingness to employ the private delegation doctrine to hold the government accountable when it attempts to pass off powers to independent entities.[451] Although not express in the Constitution, the concept of government accountability emerges from *Ass'n of American Railroads* as a galvanizing principle that is both embodied in the Constitution's design and central to individual liberty.

The case involved Amtrak's preferential access to national rail lines under the Passenger Rail Investment and Improvement Act of 2008 (PRIIA).[452] In 1970, Congress created Amtrak[453] as a

---

[448] The analysis is admittedly at odds with *Burdeau v. McDowell*, 256 U.S. 465 (1921). *See supra* notes 328–30 and accompanying text; *see also* Flagg Bros., Inc. v. Brooks, 436 U.S. 149, 151–54, 163–64 (1978) ("[E]xpress[ing] no view as to the extent, if any, to which a city or State might be free to delegate to private parties the performance of such functions and thereby avoid the strictures of the Fourteenth Amendment.").

[449] Alexander Volokh argues that delegations are constitutional so long as the enacting legislation contains an intelligible principle. *See* Alexander Volokh, *The New Private-Regulation Skepticism: Due Process, Non-Delegation, and Antitrust Challenges*, 37 HARV. J.L. & PUB. POL'Y 931, 979 (2014) (arguing that the scarcity of cases where the Court has struck down a statute on non-delegation grounds makes the doctrine useless for constraining government delegation to private parties).

[450] 721 F.3d 666 (D.C. Cir. 2013), *vacated*, 131 S. Ct. 2355 (2015).

[451] Dep't of Transp. v. Ass'n of Am. R.Rs., 131 S. Ct. 2355 (2015).

[452] Passenger Rail Investment and Improvement Act of 2008, Pub. L. No. 110-432, Div. B, 122 Stat. 4848, 4907 (codified at 49 U.S.C. § 24101 note (2012)), *invalidated by* Ass'n of Am. R.Rs. v. U.S. Dep't of Transp., 721 F.3d 666 (D.C. Cir. 2013), *vacated*, 131 S. Ct. 2355 (2015).

[453] Rail Passenger Service Act of 1970, Pub. L. No. 91-518, § 301, 84 Stat. 1327, 1330 (repealed 1994); *see also* Ass'n of Am. R.Rs. v. Dep't of Transp., 865 F. Supp. 22, 25 (D.D.C.

"private, for-profit corporation" to save the passenger train industry, which had suffered as a result of increased competition from air travel and improved highway systems.[454] Under the statute, private railroads could transfer their unprofitable passenger service to Amtrak but were required in exchange to lease their tracks back to Amtrak, which would have preferred access.[455] Amtrak and the railroads subsequently entered into operating agreements establishing rates that Amtrak would pay to use the private tracks and facilities, as well as other conditions.[456]

In 2008, Congress sought to standardize the operating agreements by empowering Amtrak and the FRA to jointly "develop new or improve existing metrics and minimum standards for measuring the performance and service quality of intercity passenger train operations, including . . . on-time performance and minutes of delay."[457] Under the statute, if Amtrak and the FRA cannot agree on metrics and standards, they can petition the Surface Transportation Board (STB)—an independent agency within the Department of Transportation—for binding arbitration.[458] Moreover, "[t]o the extent practicable, Amtrak and its host rail carriers [must] incorporate the metrics and standards . . . into their access and service agreements."[459] If Amtrak fails to provide "on-time performance," the STB may start an investigation to determine fault.[460] If it finds that a freight carrier failed "to provide preference to Amtrak over freight transportation as required," it can impose damages.[461]

2012), *rev'd*, 721 F.3d 666 (D.C. Cir. 2013), *vacated*, 131 S. Ct. 2355 (2015) (noting that the National Railroad Passenger Corporation is better known as Amtrak).

[454] *Ass'n of Am. R.Rs.*, 865 F. Supp. 2d at 25 (quoting Nat'l R.R. Passenger Corp. v. Atchison, Topeka and Santa Fe Ry. Corp., 470 U.S. 451, 454 (1985)); *see* 49 U.S.C. § 24301(a).

[455] 49 U.S.C. § 24308(a), (c).

[456] *Ass'n of Am. R.Rs.*, 865 F. Supp. 2d at 25.

[457] 49 U.S.C. § 24101 note; *Ass'n of Am. R.Rs.*, 721 F.3d 666; *see Metrics & Standards for Intercity Passenger Rail Service Under Section 207 of the Passenger Rail Investment and Improvement Act of 2008*, 75 Fed. Reg. 26,839 (May 12, 2010) (explaining that § 207 of the PRIIA charged the FRA and Amtrak with developing new and improving existing metrics). Standards were promulgated in 2010. *Id.* (explaining that the FRA and Amtrak developed new standards that went into effect May 11th, 2010).

[458] 49 U.S.C. § 24101 note.

[459] *Id.*

[460] *Id.* § 24308(f)(1). The STB must do so if Amtrak or a railroad brings a complaint. *Id.*

[461] *Id.* § 24308(f)(2).

Upset with Amtrak's enhanced powers, the Association of American Railroads (AAR) initiated a lawsuit on behalf of its freight railroad members, seeking an order declaring unconstitutional the portion of the PRIIA giving Amtrak dual authority to promulgate standards governing the freight rail industry.[462] Reversing the judgment of the district court, the D.C. Circuit found that "Amtrak is a private corporation with respect to Congress's power to delegate . . . authority" and, as such, it cannot be given the "regulatory power prescribed in [the PRIIA]" under the private delegation doctrine.[463]

The Supreme Court reversed, deeming Amtrak a governmental entity for purposes of the Constitution and remanding the case for consideration, *inter alia,* of whether the PRIIA's provision for appointment of an arbitrator " 'is a plain violation of the nondelegation principle.' "[464] Writing for the majority, Justice Kennedy emphasized that "[t]reating Amtrak as governmental" avoids what would otherwise amount to "an unbridled grant of authority to an unaccountable actor."[465] Among other things, "[t]he political branches . . . have imposed substantial transparency and accountability mechanisms [on Amtrak], and, for all practical purposes, set and supervise its annual budget."[466] Such " 'structural principles secured by the separation of powers,' " he added, " 'protect the individual as well.' "[467]

Justices Alito and Thomas each wrote separately that the PRIIA is unconstitutional under the private delegation doctrine. Importantly, they both underscored the separation of powers implications of privatized policymaking, which include, in Justice Alito's words, "a vital constitutional principle [that] must not be forgotten: Liberty requires accountability."[468]

---

[462] *Ass'n of Am. R.Rs.*, 721 F.3d at 670.

[463] *Id.* at 677.

[464] Dep't of Transp. v. Ass'n of Am. R.Rs., 1335 S. Ct. 1225, 1234 (2015). The Court also instructed the D.C. Circuit to consider whether "Congress violated the Due Process Clause by 'giv[ing] a federally chartered, nominally private, for-profit corporation regulatory authority over its own industry.' " *Id.* For an explanation of the due process claim, see *supra* note 303 and accompanying text.

[465] *Ass'n of Am. R.Rs.*, 1335 S. Ct. at 1233.

[466] *Id.*

[467] *Id.* (quoting Bond v. United States, 131 S. Ct. 2355, 2365 (2011)).

[468] *Id.* at 1234 (Alito, J., concurring).

In making the case for why outsourcing powers to private parties is unconstitutional, Justice Alito characterized governmental power as uniquely belonging to government actors who "are set apart from ordinary citizens. Because they exercise greater power, they are subject to special restraints," such as swearing an oath of office.[469] Government actors, in turn, must be accountable to the people. Otherwise, "[w]hen citizens cannot readily identify the source of legislation or regulation that affect their lives, Government officials can wield power without owning up to the consequences," such as by "passing off a Government operation as an independent private concern."[470] Because "a private person" can be appointed an arbitrator under the PRIIA, Justice Alito concluded, "this law is unconstitutional."[471]

As support, Justice Alito cited the post-New Deal decisions in *Schechter Poultry* and *Panama Refining*, which have long been dismissed by scholars as lifeless relics of the past. The non-delegation doctrine, he explained, "exists to protect liberty."[472] "[B]y careful design," the structural Constitution "prescribes a process for making law, [with] many accountability checkpoints."[473] "It would dash the whole scheme," he quipped, "if Congress could give its power away to an entity that is not constrained by those checkpoints."[474] Justice Alito maintained leeway for preserving executive branch rulemaking even if private sector lawmaking is unconstitutional. Whereas "the other branches of Government have vested powers of their own that can be used in ways that resemble lawmaking," he explained, "[w]hen it comes to private entities . . . there is not even a fig leaf of constitutional justification."[475]

In his concurrence, Justice Thomas adopted a more rigidly formalist approach to Article I that would "require that the Federal Government create generally applicable rules of private

---

[469] *Id.* at 1235.

[470] *Id.* at 1234–35.

[471] *Id.* at 1237–38.

[472] *Id.* at 1237 (citing U.S. CONST. art. I, § 1; Wayman v. Southard, 10 Wheat. 1, 42–43 (1825); A.L.A. Schechter Poultry Corp. v. United States, 295 U.S. 495 (1935); Panama Refining Co. v. Ryan, 293 U.S. 495 (1935)).

[473] *Id.*

[474] *Id.*

[475] *Id.*

conduct only through the constitutionally prescribed legislative process."[476] "Because a private entity is neither Congress, nor the President or one of his agents, nor the Supreme Court or an inferior court established by Congress," he added, "the Vesting Clauses would categorically preclude it from exercising the legislative, executive, or judicial powers of the Federal Government."[477] But Justice Thomas ventured further than Justice Alito to argue that Congress cannot allocate power to "an ineligible entity, whether governmental or private."[478] This view is radical to the extent it would render unconstitutional vast swaths of the federal administrative bureaucracy, leaving many segments of the economy unregulated.

Like Justice Alito, Justice Thomas fastened his analysis on the concept of government accountability,[479] adding with irony that "[w]e never even glance at the Constitution to see what it says about how this authority must be exercised and by whom"—a searing insight regarding the way in which the privatization movement (and, indeed, the growth of the administrative state) has vastly outpaced the courts—and thus the law.[480] On this point, Justice Thomas decried the Court as having "sanctioned the growth of an administrative system that concentrates the power to make laws . . . in the hands of a vast and unaccountable administrative apparatus that finds no comfortable home in our constitutional structure."[481]

Ass'n of American Railroads leaves at least two significant constitutional issues for possible future consideration by the Supreme Court. First, as the concurring opinions by Justices Alito and Thomas indicate, the proposition that private delegations are per se unconstitutional, is not yet well settled. The federal government has repeatedly outsourced regulatory functions to

---

[476] *Id.* at 1242 (Thomas, J., concurring).

[477] *Id.* at 1240.

[478] *Id.*

[479] *See id.* at 1234 ("Confronted with a statute that authorizes a putatively private market participant to work hand-in-hand with an executive agency to craft rules that have the force and effect of law, our primary question . . . is whether that market participant is subject to an adequate measure of control by the Federal Government." *Id.* at 1240 (Thomas, J., concurring)).

[480] *Id.* at 1240.

[481] *Id.* at 1254.

private parties without meaningful constitutional checks, a practice that reinvigoration of the private delegation doctrine could call into question.[482]

Second, the case legitimates as doctrinally relevant the question of whether the structural Constitution forbids delegations to private parties that render the government democratically unaccountable. If adopted, a doctrine of constitutional accountability could operate to confine the manner in which outsourcing arrangements are structured—at least to the extent that legislative power is involved. Such an approach would advantageously adhere to the nondelegation doctrine's origins, which derive from notions of popular sovereignty. John Locke[483] explained that "the legislative cannot transfer the power of making laws to any other hands; for it being but a delegated power from the people, they who have it cannot pass it over to others."[484] Chief Justice Rehnquist similarly argued—in a concurring opinion that condemned the Occupational Safety and Health Act of 1970 as an impermissible delegation of broad agency authority to establish exposure limits for carcinogens—that "the nondelegation doctrine . . . ensures to the extent consistent with orderly governmental administration that important choices of social policy are made by Congress, the branch of our Government most responsive to the popular will."[485] Requiring that private

---

[482] *See* Sarah Shik Lamdan, *Sunshine For Sale: Environmental Contractors and the Freedom of Information Act*, 15 VT. J. ENVTL. L. 1, 16 (2014) ("As early as 1989, it was uncovered during Senate hearings that EPA contractors were drafting budget documents, overseeing field investigators, drafting responses to public comments during the rulemaking process and writing regulation preambles, and organizing and conducting public hearings." (quoting Steven J. Kelman, *Achieving Contracting Goals and Recognizing Public Concerns: A Contracting Management Perspective*, *in* GOVERNMENT BY CONTRACT: OUTSOURCING AND AMERICAN DEMOCRACY, *supra* note 18, at 153, 177)).

[483] Locke was a political philosopher whose ideas heavily influenced the Framers. *See* LEONARD WILLIAMS LEVY, ORIGINAL INTENT AND THE FRAMERS' CONSTITUTION 276 (1988) (describing Locke's view of property as encompassing the "right to rights," including "the pursuit of happiness").

[484] JOHN LOCKE, THE SECOND TREATISE OF GOVERNMENT 81 (Thomas P. Peardon ed., The Liberal Arts Press, Inc. 1952) (1690).

[485] Indus. Union Dep't v. Am. Petroleum Inst. (The Benzene Case), 448 U.S. 607, 685 (1980) (Rehnquist, J., concurring). Rather than strike down the legislation on nondelegation grounds, the majority construed the statutory language narrowly to confine agency discretion. *Id.* at 639–40. *Cf.* Loving v. United States, 517 U.S. 748, 758 (1996) (observing that "[t]he clear assignment of power to a branch . . . allows the citizen to know who may be called to answer for making, or not making, those delicate and necessary

delegations be structured to retain accountability to the people would serve the doctrine's purposes without unraveling the administrative and contractual bureaucracies that are essential to a functioning modern government.

Justice Thomas offered a two-part test for analyzing legislative delegations: "The first step [would] be to classify the power that [a statute] purports to authorize" an entity other than Congress to exercise.[486] If that power includes the ability to give content to or decide the applicability of rules governing private conduct, the first step is satisfied.[487] "The second step [would] be to determine whether the Constitution's requirements for the exercise of that power have been satisfied."[488] For Justice Alito, this line might be drawn at government actors who take an oath of office, whereas Justice Thomas would find unconstitutional any legislation that authorized the exercise of such power in a manner other than bicameralism and presentment under Article I of the Constitution.[489]

Common to both approaches under step two is a principle of constitutional accountability, i.e., that the power of government can only be exercised by actors who are accountable to the people by virtue of a transparent process that the President can control. Framed this way, constitutional accountability begins to take doctrinal shape. Suppose, once again, that DHS contractually engages Booz Allen to develop bioterrorist protocols. This time, the contract specifies that Booz Allen must draft rules that are later incorporated into official agency guidelines, satisfying step

---

decisions essential to governance" and stating that the nondelegation doctrine "developed to prevent Congress from forsaking its duties"); Arizona v. California, 373 U.S. 546, 626 (1963) (Harlan, J., dissenting in part) ("The principle that authority granted by the legislature must be limited by adequate standards . . . insures that the fundamental policy decisions in our society will be made not by an appointed official but by the body immediately responsible to the people."); Ginsburg & Menashi, *supra* note 26, at 254–55 ("Once the people had delegated the lawmaking power to the legislature, it could pass no further lest it elude the people's oversight."); Cass R. Sunstein, *Is the Clean Air Act Unconstitutional?*, 98 MICH. L. REV. 303, 335–36 (1999) (arguing that the nondelegation doctrine promotes "the kind of accountability that comes from requiring specific decisions from a deliberative body reflecting the views of representatives from various states of the union").

[486] Dep't of Transp. v. Ass'n of Am. R.Rs., 1335 S. Ct. 1225, 1253 (2015) (Thomas, J., concurring).

[487] *See id.*

[488] *See id.*

[489] *See id.* at 1254.

one of Justice Thomas's standard. A public accountability approach to private delegation would forbid this delegation because it allows the government to evade responsibility for its legislative functions under step two. The process is opaque and not within the clear command of the President. A court employing an accountability rationale might remand the case with instructions to the government to amend the contract to include terms that require transparent, comprehensive DHS review of the proposed rules with the objective of fostering good government and enabling public scrutiny of the rulemaking process.[490] Optimally, a functionalist approach to private delegation—grounded in ensuring that the government remains accountable under the Constitution without evading its protections via non-governmental agents—might transfer to other doctrinal contexts in which futile public-versus-private distinctions currently dominate.

D. CONFINING DATA INSOURCING AFTER *RILEY V. CALIFORNIA*

For the first time in history, privately developed technology is driving government surveillance.[491] By insourcing data, the government bootstraps the private sector's extra-constitutional status for purposes of the Fourth Amendment and thereby evades public accountability for surveillance derived from that data. This is because, as with the state action doctrine, the Fourth Amendment's third party doctrine bifurcates the public and private spheres for purposes of triggering constitutional protections, frustrating the Fourth Amendment objective of maintaining a separation between the government and individual zones of privacy.[492] Much like the concept of constitutional

---

[490] Unlike a state action claim, moreover, such a lawsuit would not require that the plaintiff allege an underlying violation of individual constitutional rights.

[491] *See* Michaels, *supra* note 12, at 902 ("[T]he private sector['s] comparative advantage over the government in acquiring vast amounts of potentially useful data is a function both of industry's unparalleled access to the American public's intimate affairs—access given by all those who rely on businesses to facilitate their personal, social, and economic transactions—and of regulatory asymmetries insofar as private organizations can at times obtain and share information more easily and under fewer legal restrictions than the government can when it collects similar information on its own.").

[492] *See supra* Part IV.C. Numerous scholars have thus argued for the third party doctrine's retirement, offering various justifications within the confines of existing law. *E.g.*, Susan W. Brenner & Leo L. Clarke, *Fourth Amendment Protection for Shared Privacy Rights in Stored Transactional Data*, 14 J.L. & POL'Y 211, 214–15 (2006) (arguing for the

accountability has infiltrated the Court's dialogue around private delegation, however, the prerogative of maintaining an accountable government appears in recent Fourth Amendment cases as a constitutional value that may overshadow the historical vagaries of existing doctrine in an era of ubiquitous big data surveillance.

In *United States v. Jones*[493] and *Riley v. California*,[494] the Supreme Court wrestled with the disconnect between the permeating police surveillance made possible by new technologies and outdated doctrinal barriers to Fourth Amendment scrutiny, without overtly disturbing them. In both cases, the Court applied the Fourth Amendment to constrain law enforcement's ability to capitalize on the unprecedented surveillance capacity of today's technology on the theory, articulated in *Jones*, that the Court "must 'assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.' "[495] For its part, the unanimous *Riley* Court held that the police may not search digital information on a cell phone incident to arrest.[496] Commentators have heralded *Riley* as a case that "brings the Fourth Amendment into the digital age"[497] and

---

elimination of the third party doctrine on the theory that data is protected under *Katz*'s reasonable expectation of privacy test); Elspeth A. Brotherton, *Big Brother Gets a Makeover: Behavioral Targeting and the Third-Party Doctrine*, 61 EMORY L.J. 555, 592–96 (2012) (discussing the problems with the third-party doctrine and arguing for the imposition of a "competing-interests test"); Erik E. Hawkins, *No Warrants Shall Issue But Upon Probable Cause: The Impact of the Stored Communications Act on Privacy Expectations*, 4 WAKE FOREST J.L. & POL'Y 257, 270–73 (2014) (discussing the need for an exception to the third-party doctrine in the information age); Stephen E. Henderson, *Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too*, 34 PEPP. L. REV. 975, 1025 (2007) (advocating for the elimination of the strict third-party doctrine and only applying it on a case-by-case basis). *Cf.* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 600 (2009) ("The third party doctrine serves two important roles: blocking substitution effects that upset the technological neutrality of Fourth Amendment law and furthering clarity of Fourth Amendment rules.").

493 132 S. Ct. 945 (2012).

494 134 S. Ct. 2473 (2014).

495 *Jones*, 132 S. Ct. at 950 (quoting Kyllo v. United States, 533 U.S. 27, 34 (2001)).

496 *Riley*, 134 S. Ct. at 2493 (holding that "a warrant is generally required before such a search, even when a cell phone is seized incident to arrest").

497 Mark Rotenberg & Alan Butler, *Symposium: In* Riley v. California, *a Unanimous Supreme Court Sets Out Fourth Amendment for Digital Age*, SCOTUSBLOG (June 26, 2014, 6:07 PM), http://www.scotusblog.com/2014/06/symposium-in-riley-v-california-a-unanimous-supreme-court-sets-out-fourth-amendment-for-digital-age/.

sets the stage for substantially reconfiguring the third party doctrine.[498]

Like the D.C. Circuit's decision in *Ass'n of American Railroads*, *Riley* is noteworthy for a different reason: the Court's overt rejection of a "mechanical application" of Fourth Amendment doctrine, which it conceded "might well support the warrantless searches at issue."[499] Instead, it took a functionalist approach to restricting excessive government power, which focused on the values underlying the Fourth Amendment.[500] Writing for the unanimous Court, Chief Justice Roberts first emphasized that the "element of pervasiveness that characterizes cell phones but not physical records" means greater surveillance power in the hands of government.[501] This is because ready government access to cell phone data is quantitatively and qualitatively different than physical searches of the past.[502] A cell phone search, he wrote,

> would typically expose to the government far *more* than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is.[503]

---

[498] *See Riley*, 134 S. Ct. at 2491 (observing that a cell phone is unlike a storage container as it "is used to access data located elsewhere," such as "on remote servers rather than on the device itself").

[499] *Id.* at 2484. In particular, the Court applied the search incident to arrest doctrine, which requires assessment of, " 'on the one hand, the degree to which [a warrantless search] intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests.' " *Id.* (quoting Wyoming v. Houghton, 526 U.S. 295, 300 (1999)).

[500] *Id.* at 2484–91; *see* Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1087 (2002) (proposing an "architecture of power" to balance government power with that of the people); *see also* Kerr, *supra* note 380, at 802–04 & n.7 (citing numerous scholars for "the view that the Fourth Amendment should be interpreted broadly in response to technological change").

[501] *Riley*, 134 S. Ct. at 2490.

[502] *Id.* at 2489–91.

[503] *Id.* at 2491. In this way, a search of a cell phone harkens back to the reviled writ of assistance, "which were in essence open-ended search warrants, allowing officers to search any premises they chose," and were used by British authorities for decades until they expired in 1760 with the death of George II. James Otis, *Against the Writs of Assistance (1761)*, *in* 1 DOCUMENTS OF AMERICAN CONSTITUTIONAL & LEGAL HISTORY: FROM THE

Second, Chief Justice Roberts suggested that the government must be accountable for long-term, comprehensive monitoring—by whatever means achieved. To be sure, the third-party doctrine per se was not before the Court because the existence of a search was not in question.[504] Nonetheless, "[t]he United States concede[d] that the search incident to arrest exception may not be stretched to cover a search of files accessed remotely—that is, a search of files stored in the cloud."[505] The Chief Justice likened the government's access to the cloud via a cell phone to the search of a house by virtue of "finding a key in a suspect's pocket."[506] Surely, he indicated, the latter would be intolerable under the Fourth Amendment;[507] the former is thus unthinkable, as well. In *Riley*, cell phones' capacity to access data stored remotely—presumably on private third-party servers—was thus held up as a reason *for* Fourth Amendment scrutiny.

There is a crucial distinction between the "cloud" for data storage and an individual's private residence, however: the cloud does not exist within the confines of a home. The government has described a category of cloud infrastructures as "provisioned for open use by the general public . . . owned, managed and operated by a business, academic, or government organization, or some combination of them," and "exist[ing] on the premises of the cloud provider."[508] Under *Smith v. Maryland*,[509] a colorable argument can be made that a consumer's decision to store personal data on a third-party cloud server operates as a waiver of Fourth Amendment protections.[510] Yet the public-private distinction—so

---

FOUNDING TO 1896, at 38 (Melvin I. Urofsky & Paul Finkelman, eds., 3d ed. 2008). *See generally* NELSON B. LASSON, THE HISTORY AND DEVELOPMENT OF THE FOURTH AMENDMENT TO THE UNITED STATES CONSTITUTION 51–78 (discussing writs of assistance).

504 *Riley*, 134 S. Ct. at 2480 (stating the issue to assume the cell phones have been searched).

505 *Id.* at 2491.

506 *Id.*

507 *Id.*

508 NAT'L INST. OF STANDARDS AND TECH., U.S. DEP'T OF COMMERCE, Special Publ'n 800-145; PETER MELL & TIMOTHY GRANCE, THE NIST DEFINITION OF CLOUD COMPUTING: RECOMMENDATIONS OF THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY 3 (2011), *available at* http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

509 442 U.S. 735 (1979); *see also supra* notes 362–63 and accompanying text.

510 *See Smith*, 442 U.S. at 741–42 (finding no legitimate expectation of privacy in the numbers dialed on a person's phone).

central to Fourth Amendment doctrine to date—was missing from the *Riley* opinion.

Lastly, Chief Justice Roberts underscored the overriding purpose of the Fourth Amendment to justify the somewhat extraordinary outcome in the case. He characterized the Founders' objective as a "response to the reviled 'general warrants' and 'writs of assistance' " which were "driving forces behind the Revolution itself."[511] Rejecting technical doctrinal distinctions in favor of this broader principle, the Chief Justice insisted that "[t]he fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought."[512] He went so far as to mock the government's argument that it could develop "protocols" to address cell phone access to cloud data, retorting that it was "[p]robably a good idea, but the Founders did not fight a revolution to gain the right to government agency protocols."[513]

Chief Justice Roberts's reliance on first principles is reminiscent of Justice Brandeis's famous dissent in *Olmstead v. United States*,[514] in which the majority upheld warrantless wiretapping of telephone conversations.[515] Foreshadowing modern surveillance technology, Justice Brandeis expressed concern that "[w]ays may someday be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home," including "unexpressed beliefs, thoughts and emotions."[516] He posed the question rhetorically, "Can it be that the Constitution affords no protection against such invasions of individual security?"[517] The answer to such questions, he suggested, must lie "in giving effect to the principle underlying the Fourth Amendment" and "refus[ing] to

---

[511] *Riley*, 134 S. Ct. at 2494.

[512] *Id.* at 2495.

[513] *Id.* at 2491.

[514] 277 U.S. 438, 471 (1928) (Brandeis, J., dissenting); *see* Rotenberg & Butler, *supra* note 497 (discussing Justice Brandeis's veiled influence on the *Riley* opinion).

[515] *Olmstead*, 277 U.S. at 466–69.

[516] *Id.* at 474.

[517] *Id.*

place an unduly literal construction upon it."[518] Specifically, the Framers "sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations" and thus "conferred, as against the government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men."[519] "To protect that right," he added, "every unjustifiable intrusion by the government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment."[520]

Big data mining enables the kind of unjustifiable intrusions on privacy that Justice Brandeis envisioned. Before the age of big data, technological limitations prevented intrusive surveillance unless the government secured a warrant to search a home, an order to wiretap, or both.[521] Chief Justice Roberts explained: "In Riley's case, . . . it is implausible that he would have strolled around with video tapes, photo albums, and an address book all crammed into his pockets" in the "pre-digital" era.[522] The tracking capacity of new technology creates dangers that exceed the Founders' worst fears.[523] Yet the four corners of the third party and public view doctrines render it technically beyond the Fourth Amendment's strictures. Recognizing this irony, the *Riley* Court echoed Justice Brandeis's admonition that underlying constitutional principles must override narrower interpretations if citizens are to be protected from government overreaching.[524]

In her concurring opinion in *United States v. Jones*, Justice Sotomayor suggested that constitutional accountability is one such

---

[518] *Id.* at 476.

[519] *Id.* at 478. Justice Brandeis distinguished *Burdeau v. McDowell*, 256 U.S. 465 (1921), on the grounds that

> [t]here only a single lot of papers was involved. They had been obtained by a private detective while acting on behalf of a private party, without the knowledge of any federal official, long before any one had thought of instituting a federal prosecution. Here the evidence . . . was obtained at the government's expense, by its officers, while acting on its behalf.

Olmstead, 277 U.S. at 481–82.

[520] *Olmstead*, 277 U.S. at 478–79.

[521] *See* United States v. Jones, 132 S. Ct. 945, 963 (2012) (noting that in the pre-computer age, surveillance was difficult and costly).

[522] Riley v. California, 134 S. Ct. 2473, 2493 (2014).

[523] *See id.* at 2495 (noting that technological advances do not make personal information unworthy of the protection for which the Founders fought).

[524] *Id.* at 2493.

principle.[525] While modern surveillance affords the government unprecedented access to personal information, she argued, it is accompanied by an unprecedented *lack* of accountability.[526] *Jones* involved installation of a global positioning system (GPS) on an automobile for tracking purposes.[527] Concurring in the majority's finding that law enforcement's use of the GPS constituted a Fourth Amendment search, Justice Sotomayor emphasized that today's technology "is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously," thereby "evad[ing] the ordinary checks that constrain abusive law enforcement practices: 'limited police resources and community hostility.' "[528] She underscored the Constitution's role in ensuring that the *government's* capacity for surveillance is curtailed: "Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse."[529] Moreover, Justice Sotomayor warned, "[t]he Government can store [these] records and efficiently mine them for information years into the future."[530] The consequence of "making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track," Justice Sotomayor observed, is that modern surveillance technology "may 'alter the relationship between citizen and government in a way that is inimical to democratic society.' "[531]

As in the state action context, a constitutional accountability principle could be applied in Fourth Amendment cases to confine how the government structures the processes by which it insources and uses third-party data. Requiring a warrant every time the government utilizes third-party data is not feasible. But the

---

[525] *See Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring) (considering the Fourth Amendment's goal "to curb arbitrary exercise of police power").

[526] *See id.* (noting that "the Government's unrestrained power to assemble . . . private aspects of identity is susceptible to abuse").

[527] *Id.* at 947–49 (majority opinion).

[528] *Id.* at 956 (Sotomayor, J., concurring) (quoting Illinois v. Lidster, 540 U.S. 419, 426 (2004)).

[529] *Id.*

[530] *Id.* at 955–56 (citing United States v. Pineda-Moreno, 617 F.3d 1120, 1124 (9th Cir. 2010) (Kozinski, C.J., dissenting from the denial of rehearing en banc)).

[531] *Id.* at 956 (quoting United States v. Cuevas-Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring)).

structural Constitution might be imposed to force the government to enact and follow protocols that protect individual privacy and ensure sufficient public oversight when it conducts big data searches without a warrant.[532]

Suppose, for example, that by mining publicly-available data and matching it with information contained in government databases (such as satellite and closed circuit video data), the NSA learns that Janet Schmendrick has interacted with an individual who is suspected of having ties to a member of the Islamic State of Iraq and Syria (ISIS). As a consequence, the NSA begins watching Janet's every move. The NSA's ability to track Janet using information she willingly posted on the Internet or provided to commercial third parties, as well as any images obtained as a result of her movement in public spaces, might not trigger Fourth Amendment protections under current doctrine. Yet, assuming *arguendo* that Janet could satisfy constitutional standing, a public accountability approach to the Fourth Amendment might give rise to an injunction requiring lesser privacy protection measures as a matter of constitutional necessity. Under the *Riley* Court's functionalist approach to technology and the Fourth Amendment, the effect of the government's big data usage—omnipresent surveillance reminiscent of a general warrant—would itself justify application of constitutional limits, regardless of the private status of the entities that sourced the data in the first place.

To be sure, this Article does not make specific recommendations other than to posit that a plaintiff suing the NSA over its data collection efforts might seek a range of injunctive relief on a public accountability theory that appropriately balances law enforcement and national security interests with individual privacy protections. Such protections might include imposition of consent protocols; transparency requirements; limits on wide-scale collection, retention, use and sharing of data; methods for ensuring the accuracy, relevance, and completeness of data used for governmental purposes; and the establishment of security safeguards against the risk of loss or unauthorized use,

---

[532] These could come in the form of legislative amendments to existing data-insourcing related statutes, *see supra* Part III.B, or through informal or even non-legislative rulemaking.

destruction, modification, or disclosure of data.[533] In any event, a public accountability gloss on the Fourth Amendment would afford a more nuanced—and potentially more comprehensive—approach to the challenges of modern surveillance methods than do legislative options, which leave constitutional privacy interests vulnerable. Applying a constitutional accountability principle to reconcile modern technology with existing Fourth Amendment doctrine would also chip away at the unhelpful pretense that the public and the private spheres are functionally distinct for purposes of constitutional law.

VI. CONCLUSION

The private sector's development of massive data banks, biometric technology, and unprecedented online monitoring diminishes the need for the government to extract information from individuals on its own. The result is an end-run around the constitutional limits on the government's surveillance abilities. This Article drew parallels between the government's use of private data to perform surveillance on the one hand, and its use of private parties to perform its constitutional functions through outsourcing on the other. The net effect of both phenomena is a marginalization of the Constitution's role in protecting fundamental guarantees. Private entities hold the reins on surveillance technology for the first time in history, and they are driving society towards the Orwellian state that research shows many Americans fear.

This reconfiguration of the Constitution's impact on protecting privacy from governmental intrusion is not a result of careful theoretical analysis by the Supreme Court, the President or Congress regarding the government's constitutional obligations when it acts in partnership with the private sector. It is a product of outdated constitutional case law in the form of the Fourth

---

[533] *See* CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 74–76 (2007) (proposing modifications of Title III to make the provisions applicable to visual surveillance); THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY 1–10 (2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf (proposing a consumer privacy bill of rights).

Amendment's third-party doctrine, the state action doctrine, and the private delegation doctrine. The constitutional blind spot created by the government's reliance on the private sector for its own functions can, however, be addressed through a reframing of existing doctrine in ways that show fidelity to the preservation of government accountability under the structural Constitution.