All the President's Spies: Private-Public Intelligence Partnerships in the War on Terror

Jon D. Michaels†

INTRODUCTION

The "War on Terror" has dramatically increased the nation's need for intelligence, and the federal government is increasingly relying, as it does in so many other contexts, on private actors to deliver that information. While private-public collaboration in intelligence gathering is not new, what is novel today—and what drives this inquiry—is that some of these collaborations are orchestrated around handshakes rather than legal formalities, such as search warrants, and may be arranged this way to evade oversight and, at times, to defy the law.

Unable to target or repel terrorists using conventional military tactics and munitions alone, the United States is acutely aware that today's pivotal battlefield is an informational one. Teams of U.S. intelligence agents, acting as eavesdroppers, infiltrators, interrogators, and data-miners, must race against the clock to anticipate terrorists' actions, frustrate their missions, and dismantle their infrastructure.[1] Because the U.S. government does not know the *who*,

† Acting Professor, UCLA School of Law. Law Clerk to the Hon. David H. Souter, U.S. Supreme Court, 2005-06. Law Clerk to the Hon. Guido Calabresi, U.S. Court of Appeals for the Second Circuit, 2004-05. J.D., Yale Law School, 2003. The author wishes to thank Bruce Ackerman, Guido Calabresi, Sewell Chan, Josh Civin, Patrick Curran, Nestor Davidson, Jack Goldsmith, Oona Hathaway, Robert Hockett, Orin Kerr, Allison Orr Larsen, Marty Lederman, Ronald Lee, Jerry Mashaw, Raj Nayak, Anne Joseph O'Connell, Susan Rose-Ackerman, Steven Schooner, Paul Schwartz, Nikhil Shanbhag, Reva Siegel, Alexander Slater, David Sklansky, Jeffrey Smith, Daniel Solove, Jake Sullivan, David Super, and Meredith Desautels and Marc Pilotin of the *California Law Review*. Special thanks, as always, to Toni Michaels. The views expressed herein are solely those of the author.

1. *See* PHILIP B. HEYMANN, TERRORISM, FREEDOM, AND SECURITY: WINNING WITHOUT WAR 61-65 (2003) (noting the importance of tactical and strategic intelligence, which "allow[s] prevention by incapacitating a critical group of the terrorists or denying them the resources or

what, *where*, and *when* of the next terrorist strike, but recognizes that the plot might be hatched on domestic soil, its first step must be to cast a wide net to gather all sorts of data points,[2] any one of which might be the clue that leads intelligence agents to prevent another September 11-like catastrophe.[3] In this regard, there is no better ally than the private sector. Its 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.[4]

---

access their plan requires. That necessitates identifying a sufficient and critical set of participants and learning their plan"); PATRICK RADDEN KEEFE, CHATTER: DISPATCHES FROM THE SECRET WORLD OF GLOBAL EAVESDROPPING 228 (2005); RON SUSKIND, THE ONE PERCENT DOCTRINE: DEEP INSIDE AMERICA'S PURSUIT OF ITS ENEMIES SINCE 9/11, at 26, 63 (2006); NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., THE 9/11 COMMISSION REPORT (2004); U.S. DEPARTMENT OF DEFENSE, QUADRENNIAL DEFENSE REVIEW REPORT (2006); Jack M. Balkin & Sanford Levinson, *The Process of Constitutional Change: From Partisan Entrenchment to the National Surveillance State*, 75 FORDHAM L. REV. 489, 520-22 (2006); Seth F. Kreimer, *Watching the Watchers: Surveillance, Transparency, and Political Freedom in the War on Terror*, 7 U. PA. J. CONST. L. 133, 133 (2004); *see also* Peter P. Swire, *Privacy and Information Sharing in the War on Terrorism*, 51 VILL. L. REV. 951, 955 (2006) ("[P]rogress in information technology offers the most effective response to the new [terrorist] threat.").

2. *See* HEYMANN, *supra* note 1, at 62; RICHARD A. POSNER, PREVENTING SURPRISE ATTACKS: INTELLIGENCE REFORM IN THE WAKE OF 9/11, at 99 (2005) [hereinafter POSNER, PREVENTING]; Anne Joseph O'Connell, *The Architecture of Smart Intelligence: Structuring and Overseeing Agencies in the Post-9/11 World*, 94 CALIF. L. REV. 1662-63, 1665 (2006); TODD MASSE, CONG. RESEARCH SERV., HOMELAND SECURITY INTELLIGENCE: PERCEPTIONS, STATUTORY DEFINITIONS, AND APPROACHES (2006), *available at* http://www.fas.org/sgp/crs/intel/RL33616.pdf; JEFFREY W. SEIFERT, CONG. RESEARCH SERV., DATA MINING AND HOMELAND SECURITY: AN OVERVIEW (2007), *available at* http://www.fas.org/sgp/crs/intel/RL31798.pdf; *see also* Jeffrey Rosen, *The Naked Crowd: Balancing Privacy and Security in an Age of Terror*, 46 ARIZ. L. REV. 607, 610 (2004) (describing data mining as the "consolidat[ion] and analy[sis of] public and private data in the hope of unearthing unusual patterns that might predict suspicious activity").

3. William C. Banks, *And the Wall Came Tumbling Down: Secret Surveillance After the Terror*, 57 U. MIAMI L. REV. 1147, 1151 (2003) ("A major component of our counterterrorism strategy is interdiction – taking efforts to stop the terrorists before they strike. An effective capability to conduct secret intelligence collection is of critical importance in combating terrorism."); Peter P. Swire, *The System of Foreign Intelligence Surveillance Law*, 72 GEO. WASH. L. REV. 1306, 1343 (2004) [hereinafter Swire, *System*] ("In a world of asymmetrical warfare, greater surveillance can detect and respond to newly emerging threats.").

4. *See* DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 166 (2004) [hereinafter SOLOVE, DIGITAL PERSON] ("Personal information [mined from business databases] can help the government detect fraud, espionage, fugitives, drug distribution rings, and terrorist cells. Information about a person's financial transactions, purchases, and religious and political beliefs can assist the investigation of suspected criminals and can be used to profile people for more thorough searches at airports."); JAY STANLEY, AM. CIVIL LIBERTIES UNION, THE SURVEILLANCE-INDUSTRIAL COMPLEX: HOW THE AMERICAN GOVERNMENT IS CONSCRIPTING BUSINESSES AND INDIVIDUALS IN THE CONSTRUCTION OF A

Seeking to bridge the private sector's data-gathering capabilities and the nation's need for homeland security is an Executive with a voracious appetite for intelligence and correspondingly little patience for anything that might interfere with its efforts to neutralize the terrorist threat. The Executive is institutionally predisposed to act decisively and unilaterally during times of national crisis, even if it means bypassing legal restrictions, skirting congressional and judicial oversight, and encroaching on civil liberties.[5] As Justice Souter remarked in *Hamdi v. Rumsfeld*:

> deciding . . . on what is a reasonable degree of guaranteed liberty whether in peace or war (or some condition in between) is not well entrusted to the Executive Branch of Government, whose particular responsibility is to maintain security. For reasons of inescapable human nature, the branch of the Government asked to counter a serious threat is not the branch on which to rest the Nation's entire reliance in striking the balance between the will to win and the cost in liberty on the way to victory; the responsibility for security will naturally amplify the claim that security legitimately raises.[6]

Unilateral executive policymaking of this sort has figured prominently in post-September 11 national-security policies and is reflected in the United States' approach to military detainees, interrogation tactics, battlefield contractors, and, of course, intelligence operations.[7]

SURVEILLANCE SOCIETY 1 (2004), *available at* http://www.aclu.org/FilesPDFs/surveillance_report.pdf ("The ongoing revolution in communications, computers, databases, cameras and sensors means that the *technological* obstacles to the creation of a truly nightmarish 'surveillance society' have now been overcome."); Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9, 11-12 (2004) (noting that extensive personal data is available via the Internet); Daniel J. Solove & Chris Jay Hoofnagle, *A Model Regime of Privacy Protection*, 2006 U. ILL. L. REV. 357, 359 (indicating that private companies often have fewer legal restrictions placed upon them vis-à-vis accessing other people's personal information than the government does); Orin S. Kerr, *Internet Surveillance Law After the USA PATRIOT Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 607, 610 (2003) [hereinafter Kerr, *Internet Surveillance*]; James X. Dempsey & Lara M. Flint, *Commercial Data and National Security*, 72 GEO. WASH. L. REV. 1459 (2004) [hereinafter Dempsey & Flint, *Commercial Data*].

5. *See, e.g.*, David Golove & Stephen Holmes, *Terrorism & Accountability: Why Checks and Balances Apply Even in "The War on Terrorism,"* N.Y.U. REV. L. & SECURITY, Apr. 2004, at 2, 2 ("Executive power, by its very nature, seeks to undercut constitutional rules that make it accountable to other branches of government. This is a universal tendency . . . [and] derives from the executive's conviction that it can solve important problems most effectively when unconstrained by meddling courts and many-headed debating societies such as Congress."); Harold Edgar & Benno C. Schmidt, Jr., Curtiss-Wright *Comes Home: Executive Power and National Security Secrecy*, 21 HARV. C.R.-C.L. L. REV. 349, 353-54 (1986); Neal Kumar Katyal, *Internal Separation of Powers: Checking Today's Most Dangerous Branch from Within*, 115 YALE L.J. 2314, 2319-22 (2006); Hamdan v. Rumsfeld, 126 S. Ct. 2749 (2006); Hamdi v. Rumsfeld, 542 U.S. 507 (2004); Cheney v. U.S. Dist. Court, 542 U.S. 367 (2004); Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579 (1952).

6. *Hamdi*, 542 U.S. at 545 (Souter, J., concurring in part).

7. *See, e.g.*, *Hamdan*, 126 S. Ct. at 2749; JACK GOLDSMITH, THE TERROR PRESIDENCY: LAW AND JUDGMENT INSIDE THE BUSH ADMINISTRATION (2007); SUSKIND, *supra* note 1; JOHN YOO, WAR BY OTHER MEANS: AN INSIDER'S ACCOUNT OF THE WAR ON TERROR (2006); Jon D.

Although the Bush Administration's intelligence policy has garnered no shortage of interest and criticism, much of the focus has been on what seems to be the Administration's own willingness to defy applicable law, and not on the particular role that corporations play in facilitating these operations.[8]

To date, the Executive's apparent practice of identifying and then courting private actors, persuading, coaxing, and sometimes deceiving them to enter into "informal" intelligence-gathering partnerships that often are inscrutable to Congress and the courts, has gone largely unexamined by policymakers and scholars alike. These "handshake agreements,"[9] which spawned the now-notorious National Security Agency (NSA) warrantless eavesdropping and call-data programs, as well as a range of lesser-known collaborations with the likes of FedEx and Western Union, have enabled the Executive to operate outside of the congressionally imposed framework of court orders and subpoenas, and also outside of the ambit of inter-branch oversight. In the process, these informal collaborations may unduly threaten privacy rights, separation of powers, the rule of law, and the legitimacy and vitality of bypassed government institutions. In addition, these private-public partnerships may undermine the integrity of the marketplace and weaken consumer trust in key industries.

Transcending these particular concerns are questions of national security accountability[10]—how "privatization," in the guise of informal intelligence agreements with corporations, can help the Executive direct broad swaths of intelligence policy without having to seek ex ante authorization or submit to meaningful oversight. This evasion leaves Congress and the courts ill-equipped to weigh in on important policy considerations regarding the proper scope and calibration of counterterrorism and homeland security operations, not to mention ill-equipped to intervene to remedy individual instances or patterns of injustice. Whether intentional or not, working around the legislative and judicial branches through shadowy collaborations is especially troubling given that many of today's surveillance programs rely on brand-new technologies and cut more broadly and deeply into the domestic fabric than ever before. Thus,

---

Michaels, *Beyond Accountability: The Constitutional, Democratic, and Strategic Problems with Privatizing War*, 82 WASH. U. L.Q. 1001 (2004) [hereinafter Michaels, *Beyond Accountability*].

8. *See, e.g.*, Balkin & Levinson, *supra* note 1, at 520-33; Erwin Chemerinsky, *The Assault on the Constitution: Executive Power and the War on Terrorism*, 40 U.C. DAVIS L. REV. 1 (2006); HEYMANN, *supra* note 1, at 90, 103, 160.

9. I use the terms "informal" and "handshake agreements" figuratively, to evoke the sense in which the agreements are first-and-foremost *non-statutorily* based, and are entered into by the Executive in a way that tends to bypass the usual outside oversight restrictions placed on "formal" partnerships by coordinate branches.

10. For these purposes, I adopt Martha Minow's definition of accountability as meaning "being answerable to authority that can mandate desirable conduct and sanction conduct that breaches identified obligations." Martha Minow, *Public and Private Partnerships: Accounting for the New Religion*, 116 HARV. L. REV. 1229, 1260 (2003). For a discussion of the various meanings of accountability, see generally Jerry L. Mashaw, *Accountability and Institutional Design: Some Thoughts on the Grammar of Governance*, *in* PUBLIC ACCOUNTABILITY: DESIGNS, DILEMMAS AND EXPERIENCES 115-56 (Michael W. Dowdle ed., 2006).

the need for careful consideration by the full range of government actors, especially those further removed from the immediate responsibility of hunting terrorists, is particularly acute. Greater scrutiny is essential both to ensure fidelity to existing laws and to determine whether new, informal surveillance and data-mining practices operating in the interstices of the extant legal framework warrant legislative or administrative responses to fill in those regulatory gaps. In other words, with respect to initiatives that are not currently regulated (and not readily observable), these lawmakers, regulators, and judges need accurate information to determine whether, normatively speaking, the *un*regulated terrain is in fact *under*regulated.[11]

It is the aim of this Article to propose procedural reforms to (1) bolster compliance with existing legal requirements; (2) increase the amount and frequency of information funneled to responsible agents of oversight and policymaking; (3) fashion mechanisms for those actors to have opportunities to weigh in on intelligence operations and, when necessary, correctively intervene; and, (4) to do so in a way that does not overly chill innovative and potentially fruitful collaborations.[12] Until such procedural reforms are in place, we should remain agnostic as to what substantive intervention is actually needed and thus ought not to wade too deeply into the "security versus liberty" debate at this time.[13]

Achieving these procedural reforms will, however, be difficult, especially

---

11. *See* Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 637 (1952) (Jackson, J., concurring) (noting an intermediate zone of shared constitutional authority where Congress has neither endorsed nor prohibited activity, but could well legislate in the domain); *see also* Heidi Kitrosser, *"Macro-Transparency" as Structural Directive: A Look at the NSA Surveillance Controversy*, 91 MINN. L. REV. 1163, 1195, 1202-03 (2007) (indicating that "[i]n [*Youngstown*'s intermediate zone] . . . Congress may not know which questions to ask or which information to request to conduct effective oversight unless the executive branch regularly provides Congress with basic information" and intimating that Congress, in order to exercise its legislative powers in this domain, needs to be kept informed); Harold Hongju Koh, *Setting the World Right*, 115 YALE L.J. 2350, 2368-73 (2006) [hereinafter Koh, *Setting*] (suggesting that though the Executive may initiate activity in the interstices of a statutory framework, the mere fact of presidential activity, particularly after *Hamdan*, does not beget a presumption that the interstitial operation is legally valid).

12. Elsewhere I have discussed the importance of situating national-security powers within the larger framework of limited and democratic government, one that envisions a non-trivial and concurrent role for Congress and the courts to play. *See* Michaels, *Beyond Accountability*, *supra* note 7, at 1050-83; *see also* LOUIS FISHER, PRESIDENTIAL WAR POWER 1-5 (1995); HAROLD HONGJU KOH, THE NATIONAL SECURITY CONSTITUTION: SHARING POWER AFTER THE IRAN-CONTRA AFFAIR 83 (1990); William Michael Treanor, *Fame, the Founding, and the Power to Declare War*, 82 CORNELL L. REV. 695, 700 (1997); Note, *Recapturing the War Power*, 119 HARV. L. REV. 1815 (2006).

13. *See, e.g.*, Samuel Issacharoff & Richard H. Pildes, *Between Civil Libertarianism and Executive Unilateralism: An Institutional Process Approach to Rights During Wartime*, 5 THEORETICAL INQUIRIES L. 1 (2004), *available at* http://www.bepress.com/til/default/vol5/iss1/art1 (noting that resolving security-liberty tensions in times of crisis begins in no small part with first addressing institutional and process-oriented questions, such as whether Congress can meaningfully participate in policy deliberations).

because the current legal requirements to obtain authorization to conduct intelligence operations and to submit reports to Congress (even when adhered to) provide only the most modest accountability checks.[14] If the Executive is willing to maneuver around the congressional and judicial limitations on its exercise of its intelligence-gathering pursuits now, when so-called "formality" does not impose many real obstacles, there is a danger that its intelligence officers will be even more likely to cultivate informal, unobservable partnerships when the rigors of compliance and reporting are made correspondingly greater.

To address the complex problems of weak compliance with existing laws, limited oversight opportunities even when the laws are followed, and, perhaps most importantly, that these current laws might not adequately blanket the waterfront of needed legal structures to regulate intelligence-gathering policy, reform must run along two axes, which converge on the critical and counterintuitive role that private actors play in intelligence operations.

First, whereas the Executive may be particularly unlikely to eschew informality (in part because it craves operational flexibility and in part because it is relatively immune from political and legal sanction for proceeding ultra vires), corporations—more institutionally detached from the War on Terror—have much less of an incentive to embrace informality in the first place; the corporations are also highly susceptible to legal and financial pressure that could be applied by Congress and the courts to force the firms to condition cooperation on the Executive's compliance with legal formalities. Thus, this Article proposes to flip the private-public partnerships on their heads, converting the privatization schemes from the handmaidens of inscrutable intelligence policy into the guarantors of a new counterterrorism regime built on legality, legitimacy, and accountability.[15]

Second, to improve the overall robustness of intelligence policy and to ensure that currently unregulated practices are subject to meaningful oversight, mechanisms must be put into place to give actors in all three branches of government opportunities to review ongoing initiatives.[16] Accepting, for

14. Moreover, there is also the question of political will, or lack thereof, which I will address in Part IV.

15. For discussions of privatization as a threat to accountability, see Matthew Diller, *Form and Substance in the Privatization of Poverty Programs*, 49 UCLA L. REV. 1739 (2002), Jon Michaels, *Deforming Welfare: How the Dominant Narratives of Devolution and Privatization Subverted Federal Welfare Reform*, 34 SETON HALL L. REV. 573 (2004) [hereinafter Michaels, *Deforming Welfare*], Steven L. Schooner, *Contractor Atrocities at Abu Ghraib: Compromised Accountability in a Streamlined, Outsourced Government*, 16 STAN. L. & POL'Y REV. 549 (2005), and Paul R. Verkuil, *Public Law Limitations on Privatization of Government Functions*, 84 N.C. L. REV. 397 (2006).

16. Those mechanisms will be, of course, consistent with the government officials' constitutional powers (and limitations on those powers). That means that while information about specific algorithms and targeting decisions would not be subject to legislative oversight (just as Congress could not expect to be allowed to micromanage military strategy, such as what hill the

reasons to be described below,[17] that simply ratcheting up ex ante evidentiary requirements may be self-defeating from both a compliance and security standpoint, but also recognizing that the current framework fails to provide adequate avenues for corrective intervention, corporations should be required to act as legal gatekeepers and as agents of disclosure. That is, the corporations must be made, by force of law, to insist on being served with the appropriate instruments of ex ante legal compulsion (e.g., warrants, subpoenas), and must moreover be obligated to provide their own descriptive accounts of the collaborations, both to the congressional oversight committees and to the inspectors general of the partnering agencies. Additionally, all operations, regardless of what, if any, authorization is necessary at the ex ante stage, should be subject to periodic reauthorization before an independent magistrate. Finally, in an effort not to overly deter innovative partnerships, safe-harbor civil-immunity protections should be accorded to those private entities that act as agents of disclosure and legal gatekeepers.

Thus, by leveraging the Executive's dependence on privatization to boost compliance and by creating additional mechanisms for regulating intelligence partnerships on an ongoing basis, the currently incomplete and oft-bypassed governing legal framework for intelligence operations can be considerably strengthened, a predicate step for ensuring the full range of government actors can contribute to the substantive development of our still-nascent, post-September 11 intelligence policy agenda.

My inquiry begins by laying out the Article's three fundamental postulates, which I address in Parts I, II, and III, respectively. First, the intelligence agencies depend greatly on private actors for information gathering. Second, the Executive is institutionally predisposed to act decisively and unilaterally during times of crisis, even if that means bypassing legal restrictions, skirting congressional and judicial oversight, and encroaching on civil liberties. Third, to the extent corporations currently are (or can be made to be) willing partners, the Executive may choose to conduct intelligence policy through informal collaborations, notwithstanding the legal, political, and structural collateral harms these inscrutable bargains may generate.

These first three building blocks of the Article provide the foundation for

---

Marines should storm), broader policy-level inquiries about the nature of intelligence operations ought to be shared with oversight actors and committees (just as Congress expects to know about military training initiatives, equipment standards, disciplinary structures, and troop deployments). *See, e.g.*, William Van Alstyne, *The President's Powers as Commander-in-Chief Versus Congress' War Power and Appropriations Power*, 43 U. MIAMI L. REV. 17, 47 (1988) ("Congress . . . also has a distinct enumerated power to provide for armies and navies, and to prescribe the uses to be made for them. There is nothing inconsistent between this proposition and . . . the proposition that under those circumstances in which Congress has affirmatively embraced a commitment to belligerent activities overseas on a sustained basis, it may not presume to dictate the minute strategy and tactics of the President's conduct of the authorized enterprise.").

17. *See, e.g.*, *infra* note 210 and accompanying text.

my analysis in Part IV, where I describe how the Executive's reliance on privatization could actually enhance accountability and ultimately serve to engender a more dynamic model for effective policymaking.

I
EXECUTIVE RELIANCE ON PRIVATE-PUBLIC INTELLIGENCE PARTNERSHIPS

Technological advances and the concomitant universal reliance on such innovations to communicate and to conduct personal and business transactions electronically have generated an unprecedented number of data points about individuals who use email, surf the web, speak via telephone, wire money, bank, travel commercially, and transact business via the Internet.[18] All of the information about particular electronic transactions (and all of the background details people supply to subscribe to shopping or frequent-traveler membership clubs or to gain access to websites' content) is possessed in large measure by private firms involved in commerce, finance, and telecommunications.[19] With high-powered computers and increasingly sophisticated software,[20] analysts can mine these stores of data and detect particularly significant patterns of behavior, including activities ostensibly indicative of terrorist planning.[21]

People simply do not interface with the government in the same ways or with the same frequency as they do with the private sector, and thus the intelligence agencies find themselves particularly drawn to, and in some respects dependent upon, private data resources.[22]

Coupled with the private sector's attractiveness as a convenient repository of information is its legal allure, notably in instances when private data gathering is subject to less stringent regulation than what the government faces. That is, federal law-enforcement and intelligence-gathering offices (along with, for example, health and labor departments) are at times comparatively hamstrung in their direct ability to collect and catalog private, personal information about U.S. persons.[23] The reasons for this asymmetry include

18. *See* Dempsey & Flint, *Commercial Data*, *supra* note 4, at 1459-61; Freiwald, *supra* note 4, at 11-12; Stan Karas, *Enhancing the Privacy Discourse: Consumer Information Gathering as Surveillance*, 7 J. TECH. L. & POL'Y 3 (2002); Kerr, *Internet Surveillance*, *supra* note 4, at 610; Stanley, *supra* note 4, at 1.

19. Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1084 (2002) [hereinafter Solove, *Digital Dossiers*]; *see also* Stanley, *supra* note 4, at 1-2.

20. *See* Fred H. Cate, *Legal Standards for Data-Mining*, *in* EMERGENT INFORMATION TECHNOLOGIES AND ENABLING POLICIES FOR COUNTER-TERRORISM 393 (Robert L. Popp & John Yen eds., 2006); Kreimer, *supra* note 1, at 161; K.A. Taipale, *Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data*, 5 COLUM. SCI. & TECH. L. REV. 2 (2003).

21. *See* Ira S. Rubenstein, Ronald D. Lee & Paul M. Schwartz, *Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches*, 75 U. CHI. L. REV. 261 (2008).

22. *See, e.g.*, SOLOVE, DIGITAL PERSON, *supra* note 4, at 165-66; Solove, *Digital Dossiers*, *supra* note 19, at 1084, 1090-95.

23. *See, e.g.*, Cate, *supra* note 20, at 394 (noting how when the government receives information on a voluntary basis from third parties, constitutional and statutory laws that

legislative happenstance, consumer convenience, and the assumption that private businesses can do less "harm" with personal information than the government can. But if 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.

Some examples of private-public partnerships may be elucidating. While disclaiming any attempt at comprehensiveness, which would be virtually impossible in an area of public policy so shrouded in secrecy, the case studies below nevertheless provide a foundation for exploring, in subsequent parts, a variety of the critical political, legal, and economic characteristics undergirding these informal collaborations.[24]

---

otherwise restrict government data collection may no longer apply); Dempsey & Flint, *Commercial Data*, *supra* note 4, at 1473 & nn. 47-48 (describing how *United States v. Miller*, 425 U.S. 435 (1976), and *Smith v. Maryland*, 442 U.S. 735 (1979), created gaps in the constitutional privacy landscape by rejecting claims that telephone and bank customer records were constitutionally protected and could not be turned over by telecommunications firms and banks to the government absent legal compulsion); Solove & Hoofnagle, *supra* note 4, at 365-67 (describing how some of the restrictions on data collection pursuant to the Privacy Act of 1974 and the Fair Credit Reporting Act of 1970 can be bypassed if information is first privately gathered); *see also, e.g.*, *infra* notes 59, 127 (comparing stricter regulations imposed on the U.S. Postal Service vis-à-vis assisting law-enforcement investigations with lighter ones placed on private parcel companies); *infra* note 271 (indicating that as a legal matter the government can more easily acquire private information from a commercial data broker than if it were to try to obtain the information directly). *See generally* JAMES DEMPSEY & LARA FLINT, CTR. FOR DEMOCRACY & TECH., PRIVACY'S GAP: THE LARGELY NON-EXISTENT LEGAL FRAMEWORK FOR GOVERNMENT MINING OF COMMERCIAL DATA, May 28, 2003, *available at* http://www.cdt.org/security/usapatriot/030528cdt.pdf [hereinafter DEMPSEY & FLINT, PRIVACY'S GAP]; SOLOVE, DIGITAL PERSON, *supra* note 4, at 165-68; Rubenstein et al., *supra* note 21, at 273-74.

24. Although the focus of this Article is on corporate-government relationships, it should be noted that the Executive has sought, and continues to seek, the help of average citizens, too. For example, the Terrorist Information and Prevention System (TIPS) was designed to be "a nationwide program giving millions of American truckers, letter carriers, train conductors, ship captains, utility employees, and others a formal way to report suspicious terrorist activity" and to "serve as extra eyes and ears for law enforcement," Editorial, *What Is Operation TIPS?*, WASH. POST, July 14, 2002, at B6; *see also* STANLEY, *supra* note 4, but Congress passed legislation defunding the project in its infancy. *See* Homeland Security Act of 2002, Pub. L. No. 107-296, § 880, 116 Stat. 2135, 2245 ("Any and all activities of the Federal Government to implement the proposed . . . Operation TIPS . . . are hereby prohibited."). While acknowledging that it might well be a vigilant truck driver or longshoreman who has unique access to a missing clue that enables the government to thwart a terrorist attack, and also while acknowledging that the government's encouragement of a citizens corps raises its own set of important legal and normative questions, I am primarily interested here in examining the ways in which repeat corporate players with vast amounts of data are linked to what Jack Balkin and Sanford Levinson call the national surveillance state. *See* Balkin & Levinson, *supra* note 1. These corporations are far more likely than individual citizens to be in a position to aid intelligence agents' efforts to subvert congressional and judicial oversight. But it is also true that, under the right conditions, these corporations are well-placed to resist those efforts and insist on greater fidelity to the law.

A. NSA Warrantless Eavesdropping: The Terrorist Surveillance Program

Perhaps the most infamous private-public intelligence partnership has involved the major telecommunications companies granting the NSA warrantless access to monitor international telephone calls and electronic correspondences, even when at least one of the targeted parties was a U.S. person acting on American soil.[25] Under the so-called Terrorist Surveillance Program (TSP), which President Bush reportedly authorized in a secret executive order,[26] the NSA listened in on "as many as five hundred people in the United States at any given time,"[27] cumulatively spying on millions of Americans' telephone calls and email correspondences.[28]

Evidently, among other things, the NSA "secretly arranged with top officials of major telecommunications companies to gain access to large telecommunications switches carrying the bulk of America's telephone calls,"[29] and the companies granted that access "without warrants or court orders."[30]

The TSP revelation caught many off guard. Prior to the public disclosure of the program in December 2005, the intelligence agencies were widely assumed to have been in compliance with the authorization regime that came into effect with the passage of the Foreign Intelligence Surveillance Act (FISA) of 1978.[31] At the time the TSP was initiated, FISA required intelligence agents to obtain ex ante authorization from a special FISA Court judge before conducting foreign-intelligence electronic surveillance, so long as the surveillance targeted the communications of U.S. persons.[32] Moreover, the Bush Administration had given no public indication that its statutory surveillance powers, which incidentally were markedly expanded both in the

25. *See* ACLU v. NSA, 438 F. Supp. 2d 754 (E.D. Mich. 2006), *vacated on standing grounds*, 493 F.3d 644 (6th Cir. 2007), *cert. denied*, 128 S. Ct. 1334 (2008); Hepting v. AT&T Corp., 439 F. Supp. 2d 974 (N.D. Cal. 2006).

26. *See* James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A1.

27. JAMES RISEN, STATE OF WAR: THE SECRET HISTORY OF THE CIA AND THE BUSH ADMINISTRATION 44 (2006).

28. *Id.* at 48; *see also* Leslie Cauley & John Diamond, *Telecoms Let NSA Spy on Calls*, USA TODAY, Feb. 6, 2006, at A1.

29. RISEN, *supra* note 27, at 54; *see also* John Markoff & Scott Shane, *Documents Show Link Between AT&T and Agency in Eavesdropping Case*, N.Y. TIMES, Apr. 13, 2006, at A17 (noting allegations that "AT&T had an agreement with the federal government to systematically gather information flowing on the Internet through the company's network").

30. Cauley & Diamond, *supra* note 28. In 2007, the Bush Administration signaled its intent to secure court orders and seek congressional support rather than continue proceeding with the TSP. *See* Eric Lichtblau & David Johnston, *Court To Oversee U.S. Wiretapping in Terror Cases*, N.Y. TIMES, Jan. 18, 2007, at A1; *infra* notes 86 and 132 (describing Administration efforts in furtherance of securing enhanced legislative authority).

31. Pub. L. No. 95-511, 92 Stat. 1783 (1978) (codified as amended in scattered sections of 50 U.S.C.); *see* Risen & Lichtblau, *supra* note 26; Scott Shane, *White House Retreats Under Pressure*, N.Y. TIMES, Jan. 18, 2007, at A22.

32. For a detailed discussion of FISA's requirements and the structure and content of U.S. intelligence-gathering and surveillance law, see *infra* note 86.

immediate aftermath of September 11,[33] and in subsequent years,[34] were inadequate.[35] Thus, the fact that firms were willing to facilitate such wide-scale eavesdropping simply "on the basis of oral requests from senior government officials"[36] led the *New York Times*'s James Risen to conclude: "[t]he secret decision by the president has opened up America's domestic telecommunications network to the NSA in unprecedented and deeply troubling new ways, and represents a radical shift in the accepted policies and practices of the modern U.S. intelligence community."[37]

The TSP required two to tango, and observers were equally surprised by the telecommunications companies' complicity. Prior to the TSP revelation, it had been believed, at least since the passage of FISA,[38] that the telecommunications industry had always conditioned its surveillance assistance on the production of the requisite court orders.[39] Given the role industry almost invariably plays as a technical middleman[40] (and potential legal gatekeeper) in

---

33. *See, e.g.*, USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (among other things, authorizing "roving" wiretaps and permitting FISA applications even where foreign-intelligence gathering is not the primary purpose of the investigation,); *In re* Sealed Case, 310 F.3d 717 (FISA Ct. Rev. 2002).

34. *See, e.g.*, Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638 (codified at 50 U.S.C. § 1801(b)(1)) (creating "lone wolf" FISA surveillance authority to target unaffiliated foreign persons who may pose terrorist threats).

35. *See* FREDERICK A.O. SCHWARZ, JR. & AZIZ Z. HUQ, UNCHECKED AND UNBALANCED: PRESIDENTIAL POWER IN A TIME OF TERROR 126-27 (2007) ("Along with the President, key officials responsible for surveillance echoed the message that FISA provided the necessary tools to deal with terrorism. . . . They suggested that all government wiretap surveillance was being carried out pursuant to the FISA rules for warrants."); Craig S. Lerner, *The USA PATRIOT Act: Promoting the Cooperation of Foreign Intelligence Gathering and Law Enforcement*, 11 GEO. MASON L. REV. 493, 504-06 (2003); Stephen J. Schulhofer, *The New World of Foreign Intelligence Surveillance*, 17 STAN. L. & POL'Y REV. 531, 535-40 (2006).

36. Cauley & Diamond, *supra* note 28.

37. RISEN, *supra* note 27, at 44 (2006) (noting that the telecommunications companies have given the NSA "direct access to key telecommunications switches that carry many of America's daily phone calls and e-mail messages").

38. *See Intelligence Activities: The National Security Agency and Fourth Amendment Rights: Hearings Before the Select Comm. to Study Governmental Operations with Respect to Intelligence Activities*, 94th Cong. (1976) [hereinafter *Church Committee*] (documenting unrestrained, unmonitored covert intelligence operations); KATHRYN S. OLMSTED, CHALLENGING THE SECRET GOVERNMENT: THE POST-WATERGATE INVESTIGATIONS OF THE CIA AND FBI (1996); *see also* Freiwald, *supra* note 4, at 12 (describing the pre-FISA history of government-phone company secret collaborations).

39. *See, e.g.*, Scott Shane, *Attention in N.S.A. Debate Turns to Telecom Industry*, N.Y. TIMES, Feb. 11, 2006, at A11.

40. Throughout much of the Cold War period, international telephone conversations were beamed around the world via satellites, and the NSA could use its own radio receivers to pluck calls out of the sky. *See, e.g.*, JAMES BAMFORD, BODY OF SECRETS: ANATOMY OF THE ULTRA-SECRET NATIONAL SECURITY AGENCY: FROM THE COLD WAR THROUGH THE DAWN OF A NEW CENTURY 367-70 (2001); John Sims, *What NSA Is Doing . . . And Why It's Illegal*, 33 HASTINGS CONST. L.Q. 105 (2006); Declan McCullagh & Anne Broache, *NSA Eavesdropping: How It Might Work*, CNET News.Com, Feb. 7, 2006, http://news.com.com/NSA+eavesdropping+How+it+might+work/2100-1028_3-6035910.html?tag=st.num. Now that fiber optics has replaced satellite technology, however, the government can no longer as readily

facilitating electronic eavesdropping, one cannot overstate the significance of this seeming reversal in corporate attitude.[41] Yet, as I will discuss below, now that the program has been leaked to the press and now that the telecommunications firms have clamored for retroactive immunity for their role in the TSP, one cannot help but also appreciate that this seeming reversal in attitude is at least partially contingent on guarantees that they will not suffer adverse consequences as a result of their informal cooperation.[42]

B. NSA Call-Data Program

A second major government-telecommunications partnership, first publicly reported in May 2006, has involved an arrangement whereby telecommunications companies agreed to transfer vast amounts of telephone and Internet information, even of purely domestic telephone calls and emails, to the NSA. This "call-data" program is different from the TSP. Whereas the TSP gave the NSA access to the *content* of international communications, the NSA Call-Data Program purportedly has provided only what is known as metadata or *envelope* information, meaning names, lists of calls and emails placed and received, and call duration.[43] This information can then be used to piece together otherwise seemingly disparate relationships and, presumably, lead to more direct surveillance measures.

Although the identities of participating providers and the extent of their cooperation is still disputed, at least two (AT&T and Verizon) and possibly one more (BellSouth) of the major telecommunication companies voluntarily gave this information to the NSA.[44] Qwest, however, "was uneasy about the legal implications of handing over customer information to the government without warrants" and thus refused to cooperate.[45]

---

intercept calls on its own. Instead, it finds itself increasingly dependent on industry's assistance to gain access. *See* McCullagh & Broache, *supra. See generally* Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (1994).

41. *See* Shane, *supra* note 39.

42. *See infra* notes 86, 115, 197-199 and accompanying text.

43. *See* Kerr, *Internet Surveillance*, *supra* note 4, at 611 ("[E]very communications network features two types of information: the contents of communications, and the addressing and routing information that the networks use to deliver the contents of communications. The former is 'content information,' and the latter is 'envelope information.'").

44. *See* Leslie Cauley, *NSA Has Massive Database of Americans' Phone Calls*, USA TODAY, May 11, 2006, at A1 (naming all three companies); Matt Richtel, *Newspaper Hedges on Report of Phone Companies and Data*, N.Y. TIMES, July 1, 2006, at A13 (suggesting that *USA Today* could not confirm BellSouth or Verizon's participation). Recently, Verizon has acknowledged informal collaboration that began at least as early as January 2005, prior to the public reporting of this practice, and that continued at least through the fall of 2007. Verizon purports to collaborate only when informed that an emergency situation exists and "does not determine the requests' legality or necessity because to do so would slow efforts to save lives in criminal investigations." Ellen Nakashima, *Verizon Says It Turned over Data Without Court Orders*, WASH. POST, Oct. 16, 2007, at A1.

45. Cauley, *supra* note 44.

Through a mixture of carrots and sticks, the government allegedly tried to entice corporate cooperation. For example,

> [i]n one meeting, an NSA representative suggested that Qwest's refusal to contribute to the database could compromise national security. . . . In addition, the agency suggested that Qwest's foot-dragging might affect its ability to get future classified work with the government. Like other big telecommunications companies, Qwest already had classified contracts and hoped to get more.[46]

Indeed, Qwest's former CEO now explicitly alleges that the NSA retaliated against his uncooperative firm by canceling contracts worth hundreds of millions of dollars.[47]

As with the TSP, observers were surprised by the extent of the corporations' acceptance of such legally informal arrangements: "Historically, AT&T and the regional telephone companies . . . required law enforcement agencies to present a court order before they would even consider turning over a customer's calling data. . . . Ma Bell's bedrock principle—protection of the customer—guided the company for decades."[48]

---

46. *Id.*; *see also* Saul Hansell & Eric Lichtblau, *U.S. Wants Internet Companies To Keep Web-Surfing Records*, N.Y. TIMES, June 2, 2006, at A15 (noting that the FBI met with Internet executives from AOL, Microsoft, Google, Verizon, and Comcast, and asked them to maintain records on customer web-surfing patterns); Mark Hosenball & Evan Thomas, *Hold the Phone; Big Brother Knows Whom You Call*, NEWSWEEK, May 22, 2006, at 22 ("[I]t has been noted that [the phone companies] were paid for their cooperation . . . [and may have been] pressured by threats to withhold valuable federal contracts.").

47. Ellen Nakashima & Dan Eggen, *Former CEO Says U.S. Punished Phone Firm*, WASH. POST, Oct. 13, 2007, at A1. It is worth noting that Qwest was reportedly first approached by the government in early 2001, months before the attacks of September 11. *See* Scott Shane, *Former Phone Chief Says Spy Agency Sought Surveillance Help Before 9/11*, N.Y. TIMES, Oct. 14, 2007, at A27.

48. Cauley, *supra* note 44; *see also* John Markoff, *Questions Raised for Phone Giants in Spy Data Furor*, N.Y. TIMES, May 13, 2006, at A1 (quoting one of the lawyers suing Verizon as saying, "Americans expect their phone records to be private. That's our bedrock governing principle of our phone system"); Tom Zeller, Jr., *Qwest Goes from the Goat to the Hero*, N.Y. TIMES, May 15, 2006, at C3 (describing the surge in Qwest's popularity, notwithstanding its perceived substandard service, in response to the news that it refused to comply with the NSA request, and noting that Qwest's decision turned "a beleaguered regional phone company . . . into a gleaming political touchstone and a beacon of consumer protection"); *but see* Arshad Mohammed & Terence O'Hara, *NSA Program Further Blurs Line on Privacy*, WASH. POST, May 13, 2006, at D1 (noting that 63% of Americans polled said that they found the Call-Data Program to be an acceptable way to investigate terrorism). The firms' cooperation has prompted lawsuits alleging violations of state and federal privacy laws as well as breaches of the corporations' own privacy policies. *See* David G. Savage, *Phone Firms Questioned*, L.A. TIMES, May 13, 2006, at A9 (noting that the Electronic Communications Privacy Act of 1986 does not make it illegal for the government to ask for phone records, but makes it illegal in certain instances for the phone companies to divulge them); Markoff, *supra* (reporting on a $5 billion civil damages suit brought by customers against Verizon); Andrew Harris, *U.S. To Ask Courts To Toss Phone Suits*, WASH. POST, June 8, 2006, at D3 (noting the existence of at least twenty suits against the phone companies); Hosenball & Thomas, *supra* note 46, at 22 ("[T]he phone companies that cooperated with the NSA . . . will be hauled into court, accused by their customers of violating . . . federal communications laws.").

C. Western Union

Western Union's history of assisting American intelligence officials dates as far back as the Civil War.[49] Perhaps most notable was Western Union's agreement during World War II to forward copies of all international cables to U.S. intelligence operatives.[50] This partnership, dubbed Operation Shamrock, outlasted the war by approximately thirty years, over which time the government reviewed countless confidential diplomatic and military dispatches, as well as personal and business communiqués. Once publicly exposed in the 1970s, Operation Shamrock was brought to an abrupt end.[51]

The Western Union-government partnership is evidently back in business. U.S. officials have again asked the venerable telegraph company to serve as America's eyes and ears, reporting on suspicious wire transfers of money, providing historical data of transactions involving persons of interest, and sending real-time photographs of those wiring money from Western Union storefronts.[52]

Describing Western Union, and its parent company, First Data, as "universal passport[s]," because they have the capacity to provide the government with all sorts of useful information, members of the Bush Administration have courted Western Union executives since September 11.[53] For example, shortly after the terrorist attacks, then-CIA director George Tenet invited Western Union executives to his office and told them that "this country is in a fight for its survival. What I'm asking is that you and your company be patriots."[54] In some instances, and for some intelligence requests, it seems as if subpoenas were issued;[55] but, it also appears—at least from the details that have trickled into the public domain—that for other intelligence transfers, it was informal cooperation rather than legal compulsion that characterized the relationship.[56]

D. FedEx

Before September 11, FedEx would hardly have been considered a

49. *See* SUSKIND, *supra* note 1, at 35.

50. *See id.* at 35-36; BAMFORD, *supra* note 40, at 22 (noting that many foreign affairs dispatches between ambassadors stationed in the United States and their home foreign ministries were intercepted via this program); Laura K. Donahue, *Anglo-American Privacy and Surveillance*, 96 J. CRIM. L. &. CRIMINOLOGY 1059, 1080-81 (2006) (describing Operation Shamrock).

51. *See Church Committee*, *supra* note 38; *see also* BAMFORD, *supra* note 40, at 440; SUSKIND, *supra* note 1, at 36.

52. *See* SUSKIND, *supra* note 1, at 208-11; *see also* Robert Block, *Private Eyes: In Terrorism Fight, Government Finds a Surprising Ally: FedEx*, WALL ST. J., May 26, 2005, at A1 [hereinafter Block, *Private Eyes*] (describing the government's appreciation of Western Union's counterterrorism assistance).

53. SUSKIND, *supra* note 1, at 38

54. *Id.* at 211.

55. *See id.* at 231-33.

56. *See* Block, *Private Eyes*, *supra* note 52.

dependable ally of America's law-enforcement agencies. Citing customer privacy concerns, FedEx routinely refused to grant the government access to its databases and frequently denied law-enforcement requests to lend uniforms and delivery trucks to agents for undercover operations.[57] But since September 11, the courier company has reportedly placed its databases at the government's disposal and, among other things, demonstrated a willingness to open suspicious packages at the government's informal request (i.e., without a warrant),[58] something that the United States Postal Service (USPS) cannot legally do,[59] and something that United Parcel Service (UPS) reportedly has refused to do.[60]

Confirming FedEx's apparent change of heart, its CEO announced his company's commitment to cooperating with the government "up to and including the line on which we would be doing a disservice to our shareholders."[61] And, one cannot help but notice that over the past few years (and perhaps partially in exchange for its assistance), FedEx has received a range of government perks. For instance, FedEx has been afforded special access to government security databases, presumably giving it a range of advantages over non-cooperating competitors.[62] It has also been awarded a prized seat on the FBI's regional terrorism task force (it is the only private company so represented) and thus has even more insider access to international security threats, again presumably well before its competitors receive such warnings.[63] Moreover, FedEx has received an exceptional license from the State of Tennessee to develop an internal police force with powers to

57. *Id.*

58. *Id.*

59. *See* United States v. Van Leeuwen, 397 U.S. 249, 251 (1970) ("It has long been held that first-class mail such as letters and sealed packages subject to letter postage . . . is free from inspection by postal authorities, except in the manner provided by the Fourth Amendment."); *see also* Dan Eggen, *Bush Warned About Mail-Opening Authority*, WASH. POST, Jan. 5, 2007, at A3 (noting widespread opposition to President Bush's "signing statement" in which he said that law-enforcement agents already had the authority to open packages entrusted to the USPS).

60. *See* Block, *Private Eyes*, *supra* note 52; Corky Siemaszko, *FedEx Delivers – Info to the Feds*, DAILY NEWS (N.Y.), June 5, 2005, at 24 (citing both UPS and the USPS's unwillingness to cooperate); *see also* Gary Fields, *FedEx Takes Direct Approach to Terrorism – Carrier Sets Up Its Own Police Force, Gaining Seat on Regional Task Force Overseen by FBI*, WALL ST. J., Oct. 9, 2003, at A4 (quoting a UPS spokesman as saying: "We rely on the government to protect the nation's borders. We deliver packages."). Moreover, UPS has discouraged its employees from participating in any of the Bush Administration's citizen-vigilance programs, including the Terrorist Information and Prevention System. *See supra* note 24; Butch Traylor, Editorial, *Delivery Guys Won't Spy*, N.Y. TIMES, July 31, 2002, at A19 (contending that asking UPS workers to spy "threatens the trust we've built in the communities we serve every day"); *see also* Isaac Baker, *Little Support for TIPS*, NEWSDAY, July 21, 2002, at A25 (describing that the USPS announced its employees would not participate in the Terrorist Information and Prevention System).

61. Block, *Private Eyes*, *supra* note 52.

62. *Id.*

63. *Id.*

investigate crimes, request warrants, and make arrests.[64]

The government's partnership with FedEx is also particularly interesting as an example of an informal, counterterrorism collaboration that can veer off in non-national-security directions. For example, in one instance, FedEx was helping the government pursue a terrorist lead and ended up opening a handful of packages containing bootlegged CDs—ordinary contraband that the government nevertheless seized and used to prosecute the parties involved.[65] Presumably, FedEx's initial basis for cooperating did not include the continuation of intrusive investigations once it became clear that there was no national-security threat.[66] Yet it is always difficult to turn a blind eye to clear evidence of criminality and thus there is great temptation and pressure to countenance so-called "mission creep," i.e., tangential law-enforcement forays, especially if there are no clear limiting guidelines (e.g., minimization procedures[67]) or expectations of vigilant oversight that are sometimes institutionalized precisely to check those temptations.[68]

E. SWIFT

Sometime after September 11, the U.S. government gained unprecedented access to the world's banking databases through its new relationship with the Society for Worldwide Interbank Financial Telecommunications (SWIFT). SWIFT is a Belgium-based cooperative that serves as "the central nervous system of international banking."[69] It carries information for nearly 8,000 financial institutions on up to 12.7 million financial transactions a day,[70]

64. *Id.*; *see also* Fields, *supra* note 60. Fields describes the regional task forces as being "entrusted with more-sensitive and specific data regarding terrorist threats than businesses usually receive. . . . [T]he FedEx representative can signal the company to take preventative actions. If the task force learns certain kinds of explosives are being used by terrorists in Asia, for instance, the representative can alert the company to install specialized explosives detectors there." *Id.*

65. *See* Block, *Private Eyes*, *supra* note 52.

66. *See* John Schwartz, *Threats and Responses: Investigations; Some Companies Will Release Customer Records on Request*, N.Y. TIMES, Dec. 18, 2002, at A16 (describing a recent survey showing that forty-one percent of corporations asked would voluntarily disclose client records to the government if the reason proffered was a national-security investigation).

67. *See, e.g.*, 50 U.S.C. § 1801(h) ("Minimization procedures . . . means . . . specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information."); *In re Sealed Case*, 310 F.3d 717, 731 (FISA Ct. Rev. 2002) (describing statutory-mandated minimization procedures as "designed to protect, as far as reasonable, against the acquisition, retention, and dissemination of nonpublic information which is not foreign intelligence information").

68. *See infra* note 94.

69. Josh Meyer & Greg Miller, *U.S. Secretly Tracks Global Bank Data*, L.A. TIMES, June 23, 2006, at A1.

70. *Id.*; *see* Barton Gellman et al., *Bank Records Secretly Tapped*, WASH. POST, June 23, 2006, at A1; *see also* Eric Lichtblau & James Risen, *Bank Data Sifted in Secret by U.S. To Block*

leading American officials to call SWIFT's databases a "unique and powerful window into the operations of terrorist networks."[71]

SWIFT executives insist that their organization's participation has not been voluntary, but instead has turned on the U.S. government's production of National Security Letters (NSLs), a type of compulsory administrative subpoena.[72] Proceeding via NSLs appears to meet the relevant American legal standards.[73] Nevertheless, SWIFT's willing cooperation represents "a significant departure from typical practice."[74] Member institutions, fearful of alienating influential segments of the financial community that zealously guard their anonymity, have long opposed law enforcement "intrusions into the confidentiality of their communications";[75] equally significant, cooperation with the United States might well have violated European Union privacy laws.[76]

F. Data Brokers ("Fourth Parties")

Thus far, my primary focus has been on corporations that collect or have access to stores of customer data as a byproduct of their providing those customers with goods or services.[77] Following convention, I call such actors "third parties," as they are directly entrusted with personal or business

---

Terror, N.Y. TIMES, June 23, 2006, at A1.

71. Lichtblau & Risen, *supra* note 70.

72. *See id.*; Gellman et al., *supra* note 70 (quoting a SWIFT statement that the consortium "responded to compulsory subpoenas for limited sets of data" and remains committed to "preserv[ing] the confidentiality of our users' data while complying with the lawful obligations in countries where we operate"). *See generally infra* note 86.

73. *See* Eric Lichtblau, *Europe Panel Faults Sifting of Bank Data*, N.Y. TIMES, Sept. 26, 2006, at A1; *but see* OFFICE OF THE INSPECTOR GEN., U.S. DEP'T OF JUSTICE, A REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION'S USE OF NATIONAL SECURITY LETTERS (2007), *available at* http://www.usdoj.gov/oig/special/s0703b/final.pdf (detailing similar irregularities vis-à-vis the FBI's issuance of NSLs) [hereinafter 2007 OIG REPORT ON NSL AUTHORITY].

74. Lichtblau & Risen, *supra* note 70; *see also* Gellman et al., *supra* note 70 (noting SWIFT's refusal to cooperate on a voluntary basis in the 1990s).

Observers have speculated that but for extensive, post-September 11 pressure by then-Federal Reserve Chairman Alan Greenspan and FBI Director Robert Mueller, SWIFT would likely have fought harder to protect the privacy of its clients. *See* Lichtblau & Risen, *supra* note 70 (describing pressure placed on SWIFT by the Bush Administration, coupled with the general sentiment within the financial community to support counterterrorism measures); Meyer & Miller, *supra* note 67 (emphasizing how "SWIFT promotes its services largely by touting the network's security"); Karen DeYoung, *Officials Defend Financial Searches*, WASH. POST, June 24, 2006, at A1 (noting that SWIFT has sought an outside auditor to monitor the scope of administrative subpoenas). *See also* JOHN F. HARRIS, THE SURVIVOR: BILL CLINTON IN THE WHITE HOUSE 407 (2005) (describing then-Treasury Secretary Robert Rubin's opposition to the government monitoring international financial transactions, even after monitoring was recommended by then-counterterrorism chief Richard Clarke).

75. Meyer & Miller, *supra* note 67 (indicating that obtaining data via administrative subpoenas represents a "striking leap in cooperation from international bankers").

76. *See* Dan Bilefsky, *Europeans Berate Bank Group and Overseer for U.S. Access to Data*, N.Y. TIMES, Oct. 5, 2006, at A15.

77. *See supra* note 24.

information as a means of furthering their customers' transactions.[78] For another set of corporate players, however, the collection and sale of personal information is their business, not just a byproduct of the exchange of goods and services. Among these "commercial data brokers," companies such as ChoicePoint, Acxiom, and LexisNexis have wide-ranging and lucrative contracts with thousands of law-enforcement agencies, at the local, state, and federal level.[79]

Despite lacking the in-house access to the information that, say, BellSouth, AOL, or United Airlines has by virtue of handling customers' affairs, these "fourth parties" are quite important to the government. They collect information from a range of private (third-party) sources, thus providing one-stop shopping for the intelligence agencies.[80] Additionally, they can serve as convenient intermediaries between the government and third-party companies, which sometimes cannot, because of certain asymmetries in federal privacy laws, voluntarily transfer information directly to the government as easily as they can to other private entities.[81] For instance, the Stored Communications Act prohibits certain telecommunications providers from voluntarily giving information to the government, but allows them to transfer the same information to other private entities. Those entities, in turn, can readily sell or give the information to the government.[82]

In addition to providing raw information, some of these firms also offer their own data-mining services and thus are capable of running their own pattern-based searches of massive stores of data in an attempt to, among other things, locate terrorists.[83] These services are an added bonus to the intelligence community especially when government agencies have come under sharp criticism from Congress and the public for conducting their own internal data-mining projects[84] and have, in certain instances, been forced to operate under greater regulatory restrictions than those placed on private data-mining

78. *Cf.* Smith v. Maryland, 442 U.S. 735 (1979) (determining that personal call-data information held by telephone companies in the course of their providing services to their customers was not constitutionally protected information, notwithstanding the constitutional protections accorded to the content of such calls).

79. *See* Kreimer, *supra* note 1, at 157-59; Solove & Hoofnagle, *supra* note 4, at 362-63.

80. *See* Dempsey & Flint, *Commercial Data*, *supra* note 4, at 1472 n.41.

81. *See* DEMPSEY & FLINT, PRIVACY'S GAP, *supra* note 23.

82. *See* 18 U.S.C. § 2702(c)(6); *see also supra* note 23; *infra* note 271.

83. *See* Dempsey & Flint, *Commercial Data*, *supra* note 4, at 1468-69.

84. *See* Martha Minow, *Outsourcing Power: How Privatizing Military Efforts Challenges Accountability, Professionalism, and Democracy*, 46 B.C. L. REV. 989, 991-92 (2005) [hereinafter Minow, *Outsourcing Power*]; Solove & Hoofnagle, *supra* note 4, at 364; *see also* Pub. L. No. 108-87, § 8131 (2003) (de-funding the Terrorism Information Awareness data-mining project); Michael J. Sniffen, *DHS Ends Criticized Data-Mining Project*, WASHINGTONPOST.COM, Sept. 5, 2007, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2007/09/05/AR2007090500795.html (terminating a Homeland Security data-mining project due to inadequate attention to privacy protocols).

projects.[85]

II
THE INCENTIVE STRUCTURE OF THE HANDSHAKE INTELLIGENCE PARTNERSHIP

Having described the Executive's dependence on private intelligence gathering and having surveyed a variety of private-public arrangements established to further national-security investigations, I turn in this Part to examine how these relationships are structured. First, I will explain why the Executive may view "handshake" partnerships as particularly advantageous vehicles through which its intelligence agents can hunt for terrorists without the hassles of inter-branch oversight. Second, I will discuss how the corporations' attachments to informality are, or at least ought to be, considerably weaker than the Executive's and thus more easily severed. Appreciating the differing levels of commitment to informality between private and public actors (and their differing ability to fend off would-be government regulators) will be essential when it comes time, in Part IV, to re-conceptualize the problem of compliance and to consider leveraging the Executive's dependence on private actors in order to enhance accountability.[86]

---

85. *See, e.g.*, Consolidated Appropriations Resolution, 2003, Pub. L. No. 108-7, div. M, § 111(b), 117 Stat. 11, 535 (codified at 10 U.S.C. § 2241 note (2003)) (prohibiting the expenditure of funds on Total Information Awareness data mining unless the Attorney General, the Director of the CIA, and the Secretary of Defense file reports regarding the value of data mining and its effect on civil liberties); S. 236, 110th Cong. (2007) (requiring congressional notification of data-mining projects); *see also* DEMPSEY & FLINT, PRIVACY'S GAP, *supra* note 23.

86. Before examining the Executive's preference for informality in intelligence collaborations, a brief description of "formality" is in order. An exhaustive discussion of the formal state of foreign-intelligence law is beyond the scope of this Article and has, in any event, been ably discussed elsewhere. *See, e.g.*, Schulhofer, *supra* note 35; Paul M. Schwartz, *Reviving Telecommunications Surveillance Law*, 75 U. CHI. L. REV. 287 (2008) [hereinafter Schwartz, *Reviving*]. Instead, I offer a basic overview.

Electronic Surveillance. When a significant purpose of an investigation is the gathering of foreign-intelligence information and when a U.S. person is being targeted as part of the investigation, FISA governs telephonic eavesdropping and accessing the content of data transmissions, notably email communications. *See* 50 U.S.C. §§ 1801-1811. (If the surveillance operation lacks a significant connection to foreign intelligence, it is regulated under the Wiretap Act, 18 U.S.C. § 2511, which imposes different and, in some respects, more stringent showings by the government agents seeking judicial authorization. *See* Schwartz, *Reviving*, *supra* (comparing national-security wiretapping's comparatively lower authorization hurdles to the "super search warrant" requirements that attach when seeking wiretap authority for ordinary law-enforcement purposes).)

To obtain authorization to conduct electronic surveillance for foreign-intelligence purposes, the Department of Justice submits an ex parte application to the Foreign Intelligence Surveillance Court (FISC), on which eleven federal district court judges sit. The FISA application must be signed by the Attorney General, who certifies that a significant purpose of the investigation is to obtain foreign-intelligence information and that the information sought "cannot reasonably be obtained by normal investigative techniques." 50 U.S.C. § 1804. Provided that the judge finds that on the basis of the facts submitted that there is probable cause to believe that (1) the target of the electronic surveillance is a foreign power or an agent of a foreign power and (2) each of the facilities or places at which electronic surveillance is directed is being used, or is about to be used,

by a foreign power, an agent of a foreign power, or a so-called "lone wolf" (i.e., an unaffiliated foreign individual posing a threat), a court order is issued authorizing the government to proceed, either directly or by compelling the assistance of third parties to facilitate in the surveillance. *Id.* § 1805. Depending on the target, orders typically remain valid for 90 days, 120 days, or 1 year, *id.* § 1805(e)(1), and then are subject to reauthorization pursuant to the same standards required for initial authorization, *id.* § 1805(e)(2).

FISA also authorizes the Executive to undertake certain surveillance activities *without* first obtaining a court order. Two situations are worthy of attention. First, in instances where the Attorney General can certify that there is no substantial likelihood of acquiring the contents of a U.S. person's communications and that the electronic surveillance is transmitted by means of communication used exclusively between or among foreign powers, she can unilaterally authorize an electronic-surveillance operation. *Id.* U.S.C. § 1802(a). Second, even in foreign-intelligence situations that *are* likely to include the contents of U.S. persons' communications, FISA permits the Attorney General to authorize electronic surveillance based both on her own certification that the conditions required to satisfy a FISA-court-order application are met and on her reasonable belief that a state of emergency exists and must be addressed before a court order could reasonably be obtained. In this scenario, the Attorney General must inform the FISC at the time of the emergency authorization and then send a formal application for a court order within seventy-two hours. *Id.* U.S.C. § 1805(f). Notably, based on the reported description of warrantless eavesdropping, *see supra* notes 25-42 and accompanying text, it does not appear that the TSP fell within the statute's warrant exemptions.

Immunity from civil liability attaches when parties directed to comply do so in accordance with the terms specified. *See id.* § 1805(i) ("No cause of action shall lie in any court against any provider of a wire or electronic communication service, landlord, custodian, or other person . . . that furnishes any information, facilities, or technical assistance in accordance with a [FISA] court order or request for emergency assistance . . . for electronic surveillance."); *see also* 18 U.S.C. § 2511(2)(a)(ii).

In response to claims by the Bush Administration that FISA placed excessive burdens on counterterrorism agents, hindering their ability to use electronic surveillance to gather foreign intelligence, Congress passed the Protect America Act (PAA) in August 2007. *See* Pub. L. No. 110-55, 121 Stat. 552. The PAA specifically carved out of FISA a subset of electronic surveillance operations, namely those directed at persons reasonably believed to be located outside of the United States—even if the foreign targets communicated with persons in the United States—and exempted them from FISA's judicial-authorization requirement. Instead, the Attorney General and the Director of National Intelligence could, on their own joint authority, order the surveillance.

The PAA contained a six-month sunset provision, and, in February 2008, the statute lapsed. Having each passed its own version of a successor bill, see FISA Amendment Acts of 2007, S. 2248, 110th Cong. (2007); FISA Amendments Act of 2008, H.R. 3773, 110th Cong. (2008), the House and Senate remained at a standstill throughout the spring of 2008. They disagreed on, among other things, the questions whether to grant the telecommunications firms retroactive legal immunity for their role in the warrantless-eavesdropping program and how much judicial overview and congressional oversight should be required. *See supra* note 42 and accompanying text; *see infra* notes 115 and 198 and accompanying text.

At the time of this writing, the House appears to have blinked first. In passing the FISA Amendments Act of 2008, H.R 6304 110th Cong. (2008) in June 2008, the House subsequently opened the door to retroactive immunity for telecommunications firms involved in the TSP, authorizing courts to "promptly dismiss[]" suits upon, among other things, a showing that the President instructed them to cooperate, *id.* at § 802, regardless whether the surveillance was, in fact, legal. The Senate swiftly passed a new version of S. 2248, with minimal concessions to the House's earlier provisions from H.R. 3773, and the president signed this bill into law in July 2008. The Foreign Surveillance Act of 1978 Amendments Act of 2008, Pub. L. No. 110-261, 122. Stat. 2436.

Physical searches. When a significant purpose of physical searches is to gather foreign-intelligence information, they too are governed by FISA. Since 1994, the procedures and

standards for obtaining authorization are substantially the same as those that apply in the electronic-surveillance context. *See* 50 U.S.C. §§ 1821-1824. Outside of the national-security context, the Fourth Amendment's reasonableness-test applies.

Through 2005, there have been 20,844 FISA applications approved and only four rejected. For a compilation of FISA application statistics, see Electronic Privacy Information Center, Foreign Intelligence Surveillance Act Orders 1979-2006, http://www.epic.org/privacy/wiretap/stats/fisa_stats.html (last visited Feb. 19, 2008). Under FISA, the Justice Department provides Congress an annual report listing the number of court orders requested and granted. Few meaningful details, regarding, for example, what those applications were for, how successful the authorized programs have been, etc., are included in the reports. *See* 50 U.S.C. § 1807 (2000). The FISA filings thus stand in stark contrast to the more robust reports made and published in the case of *non*-foreign-intelligence surveillance operations under the Wiretap Act. *See* 18 U.S.C. § 2519 (2000). For a compilation of the annual FISA reports to Congress, see Federation of American Scientists, Foreign Intelligence Surveillance Act, http://www.fas.org/irp/agency/doj/fisa/#rept (last visited Feb. 17, 2008). For reports of the annual non-foreign-intelligence wiretaps, see U.S. Courts, Wiretap Reports, http://www.uscourts.gov/library/wiretap.html (last visited Feb. 17, 2008).

Pen Registers and Trap-and-Trace Devices. Real-time gathering of telephonic and email "envelope" information for foreign-intelligence purposes is also regulated by FISA. Under FISA, authorization to use trap-and-trace devices (showing incoming telephone numbers or incoming email addresses) and pen registers (showing outgoing numbers or addresses) in the course of foreign-intelligence operations does not require independent judicial authorization. If the Attorney General (1) certifies that the foreign-intelligence information at issue does not concern a U.S. person or that it is sought to protect against international terrorism or clandestine-intelligence activities, and (2) presents an application to a U.S. Magistrate Judge, that magistrate is required to authorize the operation. 50 U.S.C. §§ 1842-43. Where there is no national-security connection, government officials have to follow the ordinary criminal-law procedures set forth in 18 U.S.C. §§ 3121-3127.

National Security Letters (NSLs). NSLs permit the government to obtain customer and consumer transaction information in national-security investigations from, principally, communications providers, financial institutions (defined very broadly), and credit agencies. Acting on their own authority, high-ranking law-enforcement and intelligence agents can serve NSLs on third parties. They need not first secure court authorization, nor must they even certify that there is a *need* for such information. *See* 12 U.S.C. § 3414, 15 U.S.C. §§ 1681u, 1681v, 18 U.S.C. § 2709, 50 U.S.C. § 436. As relevant to this inquiry, the information that can be obtained through NSLs includes (1) telephone and email records (e.g., when telephone calls or emails were sent or received, and identifying information about the other correspondent), 18 U.S.C. § 2709; (2) financial records (e.g., open and closed checking and savings accounts, transaction records from banks, private bankers, credit unions, thrift institutions, brokers and dealers, investment companies, credit card companies, insurance companies, travel agencies, casinos, and others), 12 U.S.C. § 3414; 31 U.S.C. § 5312(a)(2); and, (3) credit information (e.g., credit reports, names and addresses of all financial institutions at which the consumer has maintained an account, and identifying information of a consumer), 15 U.S.C. §§ 1861u, 1861v. *See also* 50 U.S.C. § 1861 (authorizing the government to obtain tangible objects, such as books, records, and documents, from third parties).

In certain circumstances, classes of private possessors of this consumer information are prohibited from giving the information to the government absent legal compulsion. *See, e.g.*, 18 U.S.C. § 2702 (2006). But the disclosure rules are relaxed when the information held by the third parties is passed to non-governmental entities instead of intelligence agencies, *id.* § 2702(c)(6), or when exigent circumstances exist, *id.* § 2702(c)(4).

From this quick treatment of the substance of the foreign-intelligence laws it is worth bearing in mind the following: first, this foreign-intelligence regulatory regime does not necessarily cover the range of all foreign-intelligence operations, and thus inevitably there are investigations that can be lawfully conducted in the interstices. Second, even when an operation squarely falls within a regulated domain, the requirements for securing authorization tend to be relatively easily met.

A. Executive's Perspective

Singularly tasked with protecting American lives and interests, the Executive is institutionally committed to facilitating the activities of its national-security and intelligence agencies.[87] This is not to say that officials within the Executive Branch do not take oversight by the congressional and judicial branches seriously.[88] But given the ever-present threat of terrorist attacks, the intelligence community's history of conducting extra-legal covert operations,[89] the Bush Administration's assertion that the President's Article II constitutional authority and Congress's 2001 Authorization for Use of Military Force[90] endow the Executive with sweeping national-security powers,[91] and the real-world examples discussed in this Article, there is not strong support for the more neutral premise that the Executive, irrespective of who is President, is particularly adept at balancing strategic needs with legal imperatives.[92]

Beyond the functional explanation that some of today's intelligence operations simply do not fall within already regulated categories (and thus cannot proceed any other way but, for lack of a better term, *informally*),[93] there

---

Either the representation of the intelligence agency suffices or the government must petition an independent court that has granted its electronic surveillance and requests in 99.9% of the cases. *See, e.g.*, Foreign Intelligence Surveillance Act Orders 1979-2006, *supra*. Third (and again even within regulated domains), Congress has not reserved for itself nor has it carved out for the courts a meaningful role in reviewing, monitoring, or auditing ongoing operations. *See, e.g.*, 2007 OIG REPORT ON NSL AUTHORITY, *supra* note 73.

87. *See, e.g.*, HEYMANN, *supra* note 1, at 159 (suggesting that the intelligence community does not adequately weigh democratic values and civil liberties in its efforts to "beat and stop terrorism"); *id.* at 160 (noting that accompanying the Administration's counterterrorism objectives has "been a strategy of preventing, after the fact, the operation of the separation of powers"); Robert M. Chesney, *The Sleeper Scenario: Terrorism-Support Laws and the Demands of Prevention*, 42 HARV. J. ON LEGIS. 1, 21, 26-27 (2005) (noting that the Department of Justice's primary focus is on thwarting terrorism); Golove & Holmes, *supra* note 5, at 2-3 (referencing the Bush Administration's "compulsive desire to avoid oversight by, or accountability to, any body outside the executive branch"); Solove, *Digital Dossiers*, *supra* note 19, at 1106-07 (noting pressures on the law-enforcement community to produce results).

88. *See, e.g.*, Katyal, *supra* note 5. *See generally infra* Part IV.B.2.

89. *See Church Committee*, *supra* note 38; MORTON H. HALPERIN ET AL., THE LAWLESS STATE: THE CRIMES OF THE U.S. INTELLIGENCE AGENCIES 58, 93 (1976); Swire, *System*, *supra* note 3, at 1317-18; Kreimer, *supra* note 1, at 138-41 (recounting domestic-intelligence operations from the Civil War onward).

90. Pub. L. No. 107-40, 115 Stat. 224 (2001).

91. *See, e.g.*, Brief for the Respondents, Boumediene v. Bush, No. 06-1195 (U.S. Oct. 9, 2007), *available at* http://www.abanet.org/publiced/preview/briefs/pdfs/07-08/06-1195_Respondent.pdf; Brief for Respondents, Hamdan v. Rumsfeld, 126 S. Ct. 2749 (2006) (No. 05-184), *available at* http://www.usdoj.gov/osg/briefs/2005/3mer/2mer/2005-0184.mer.aa.pdf; Brief for the Respondents, Hamdi v. Rumsfeld, 542 U.S. 507 (2004) (No. 03-6696), *available at* http://www.usdoj.gov/osg/briefs/2003/3mer/2mer/2003-6996.mer.aa.pdf.

92. *See* HEYMANN, *supra* note 1, at 160 ("[The Bush Administration has] a strategy of preventing, after the fact, the operation of the separation of powers (denying the need for legislative oversight and the right of judicial review). The costs of not trusting the Congress and the courts are grave and unjustified.").

93. *See* Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 637 (1952) (Jackson, J.,

are a range of benefits that the Executive may want to capture by choosing to proceed informally, even when that means bypassing the prescribed regulatory procedures. First, informality increases operational flexibility and thus gives the intelligence agencies greater discretion to counteract would-be terrorist threats. A legalistic, transactional relationship with a corporation, in which the firm cooperates only to the extent a court order or subpoena specifies, is likely to inhibit the type of open-ended, fast-moving collaboration that the intelligence agencies prefer. That is, the more arm's-length "law" that exists between the private and public partners, the less likely it is that the corporations will support sudden decisions by the Executive to broaden a given operation, or to countenance "mission creep," such as when an operation drifts, expands, or devolves from investigating only pressing questions of national security to probing ordinary criminal activity.[94]

Second, informality and consensual cooperation enable intelligence agents to avoid having to secure authorization from the FISA Court or from a ranking agency head. More than just a time- and labor-saving hurdle,[95] the agents might also be seeking what then-Deputy National Intelligence Director Michael Hayden called "a subtly softer trigger" than the laws actually permit,[96]—that is, greater discretion to act quickly, over a broader range of targets, and on the basis of "thinner evidence."[97] Or, they might be trying to evade the various minimization requirements included in many of the foreign-intelligence search and surveillance statutes.[98]

Third, under an informal scheme, secrecy is at its apex: technically, no one outside of the bilateral relationship needs to be told about the arrangement.

---

concurring) ("[C]ongressional inertia, indifference or quiescence may sometimes, at least as a practical matter, enable, if not invite, measures on independent presidential responsibility. In this area, any actual test of power is likely to depend on the imperatives of events and contemporary imponderables rather than on abstract theories of law."); *see also infra* note 187.

94. *See* Balkin & Levinson, *supra* note 1, at 522-23 (describing uses of data collected for intelligence purposes in other, unrelated areas such as tracking down perpetrators of child-care, tax, and health-care frauds). As described above, an informal relationship may be particularly susceptible to such expansions. *See supra* notes 65-68 and accompanying text. In that reported instance, FedEx was assisting the government ostensibly to track down terrorists and ended up discovering a handful of packages containing bootlegged CDs, unrelated to the national-security concern. FedEx nevertheless turned the contraband over to the government, which brought criminal charges against the bootleggers. Block, *Private Eyes*, *supra* note 52. *Cf. infra* notes 149-153 and accompanying text.

95. National Intelligence Director Mike McConnell recently stated that securing a FISA court order requires 200 hours of labor. *See* Chris Roberts, *Transcript: Debate on the Foreign Intelligence Surveillance Act*, ELPASOTIMES.COM, Aug. 22, 2007, *available at* http://www.elpasotimes.com/news/ci_6685679 [hereinafter *McConnell Interview*] (transcript of interview with Director McConnell).

96. Press Briefing by Attorney General Alberto Gonzales and General Michael Hayden, Principal Deputy Director for National Intelligence, in Washington, D.C. (Dec. 19, 2005), *available at* http://www.whitehouse.gov/news/releases/2005/12/print/20051219-1.html.

97. *See* SCHWARZ & HUQ, *supra* note 35, at 132.

98. *See supra* note 67 and accompanying text.

This secrecy is very important to the intelligence agencies, which often claim that even modest policy discussions by Congress could compromise operations and endanger American lives.[99] As such, endeavoring to minimize the chance of leaks, the Executive might conclude that, independent of any operational advantage, informal collaboration with minimal-to-no reporting to Congress or the courts is the better option.[100]

Fourth, oversight is at its nadir. Congress cannot effectively monitor—let alone interfere with—that which is not disclosed to it.[101] When intelligence relationships are established informally, Congress is not well-positioned to investigate intelligence operations, interrogate corporate executives about their involvement in the partnerships, demand some showing of success, withhold funding, or insist that the parties take specific measures to safeguard against, among other things, unnecessary or excessive privacy intrusions.[102] Although

99. *See McConnell Interview*, *supra* note 95 (stating that public debates in Congress about intelligence policy or on-the-record interviews may "mean[] that some Americans are going to die"); Golove & Holmes, *supra* note 5, at 3-4 (asserting that the Executive considers it impossible and imprudent to allow congressional involvement in national-security policy matters); Mark Fenster, *The Opacity of Transparency*, 91 IOWA L. REV. 885, 892 (2006) (describing the national security agencies' position that openness is a threat to their work); Laura A. White, Note, *The Need for Governmental Secrecy: Why the U.S. Government Must Be Able To Withhold Information in the Interest of National Security*, 43 VA. J. INT'L L. 1071 (2003).

100. *See, e.g.*, *Wartime Executive Power and the National Security Agency's Surveillance Authority: Hearings Before the S. Judiciary Comm.*, 109th Cong. 73 (2006) (statement of Alberto Gonzales, Att'y Gen. of the United States), *available at* http://www.fas.org/irp/congress/2006_hr/nsasurv.html. *Cf.* GOLDSMITH, *supra* note 7, at 167 (suggesting that the Justice Department's practice of not sharing legal opinions with the State Department was "ostensibly . . . to prevent leaks," but more likely "to control outcomes in the opinions and minimize resistance to them").

101. *See* BRUCE ACKERMAN, BEFORE THE NEXT ATTACK: PRESERVING CIVIL LIBERTIES IN AN AGE OF TERRORISM 85 (2006) ("The legislature cannot act effectively if it is at the mercy of the executive for information."); Charles Babington & Dafna Linzer, *Senator Sounded Alarm in 03; Rockefeller Wrote Cheney To Voice Concerns on Spying*, WASH. POST, Dec. 20, 2005, at A10 (quoting then-Ranking Senate Intelligence Committee member Jay Rockefeller as expressing frustration over the lack of information provided by the White House about the TSP, "'Without more information . . . I simply cannot satisfy lingering concerns raised by the briefing we received.'"); *see also* KEEFE, *supra* note 1, at 222 (noting that "because the world of signals intelligence is so closed no outside authority is ever able to actually weigh the merits and effectiveness of listening in"); Kitrosser, *supra* note 11, at 1204 ("[O]n a practical level, it is impossible to have effective congressional oversight when information is conveyed only to a handful of congresspersons on the condition that they not repeat it.").

102. *See* Golove & Holmes, *supra* note 5, at 2 ("Serious involvement of actors outside the U.S. executive branch is undesirable [to the administration] not only because it would limit the administration's flexibility but also because it would require the administration to provide persuasive justifications for its actions."); Congress as a Consumer of Intelligence Information, Memorandum from Alfred Cumming, Specialist in Intelligence & Nat'l Sec., Foreign Affairs, Def. & Trade Div., Cong. Research Serv., to Sen. Dianne Feinstein (Dec. 14, 2005) (noting Congress's comparatively inferior position, because of the limited information it is given, to assess the quality of intelligence and the operations themselves); *see also* GOLDSMITH, *supra* note 7, at 124 (referencing White House lawyer David Addington's overarching concern that "Congress [might] limit our operations in ways that jeopardize American lives"); Kreimer, supra note 1, at 154 (noting that the possibility of future congressional oversight "has etched in the

the current "formal" legal regime does not require that the intelligence agencies submit reports of any great substance to Congress,[103] the Executive still seems committed to avoiding oversight. Indeed, when Congress has succeeded even modestly in bolstering oversight mechanisms, the Executive has taken pains to maneuver around them.[104]

Finally, perhaps it is the absence of credible sanctions, as much as any affirmative benefit, that explains why the balance tips in favor of expedient informality in national-security intelligence operations. In ordinary criminal investigations, credible sanctions do exist. There, the ready availability of suppression remedies at trial[105] and those remedies' negative effect on obtaining convictions[106] strongly deter law-enforcement officials from employing unreasonable investigatory techniques.[107] But in the counterterrorism context, where criminal prosecutions are rare and generally take a back seat to national-security investigations and military detentions (and where suppression may not be an available remedy even if an investigation does lead to a criminal trial),[108] there is no comparable built-in mechanism for

---

organizational culture of a number of [intelligence] agencies the impropriety of abusing security intelligence").

103. *See supra* note 86 (describing the minimal oversight of intelligence agencies conducting foreign-intelligence operations). *Compare* 50 U.S.C. § 1807 (2000) (prescribing relatively less substantial foreign-intelligence surveillance disclosure requirements), *with* 18 U.S.C. § 2519 (2000) (prescribing relatively more substantial domestic, non-foreign-intelligence surveillance disclosure requirements).

104. *See* Dempsey & Flint, *Commercial Data*, *supra* note 4, at 1500 (describing how the White House circumvented the congressionally created Privacy/Civil Rights Office in the newly established Department of Homeland Security by creating a "Terrorist Threat Integration Center" and placing it "under the Director of Central Intelligence [and] outside of the oversight mechanisms that Congress specifically created at DHS"); *see also* Hope Yen, *Privacy Board Clears U.S. Spy Programs*, USATODAY.COM, Mar. 5, 2007, *available at* http://www.usatoday.com/news/washington/2007-03-05-1213535875_x.htm (noting the heavily partisan makeup of the White House's oversight board that endorsed the conclusion that the TSP did not require FISA Court authorization).

105. *See* Weeks v. United States, 232 U.S. 383, 398 (1914); Daniel J. Solove, *Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 74 FORDHAM L. REV. 747, 749 (2005) [hereinafter Solove, *Fourth Amendment*] ("[T]he principal remedy for a Fourth Amendment violation [at a criminal trial] is the exclusionary rule.").

106. *See* Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 758 (1994); Richard A. Posner, *Rethinking the Fourth Amendment*, 1981 SUP. CT. REV. 49, 54-56.

107. *See, e.g.*, Pa. Bd. of Prob. & Parole v. Scott, 524 U.S. 357, 370-77 (1998) (Souter, J., dissenting) (explaining that because it is important to deter improper government conduct in the parole-revocation context, just as it is in the criminal-prosecution context, the exclusionary rule should apply in both settings); Warren E. Burger, *Who Will Watch the Watchman?*, 14 AM. U. L. REV. 1, 12 (1964); Orin S. Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law*, 54 HASTINGS L.J. 805, 810-11 (2003) [hereinafter Kerr, *Lifting*]; Daniel J. Meltzer, *Deterring Constitutional Violations by Law Enforcement Officials: Plaintiffs and Defendants as Private Attorneys General*, 88 COLUM. L. REV. 247, 271-74 (1988).

108. *See* Swire, *System*, *supra* note 3, at 1340; *see also* William C. Banks & M.E. Bowman, *Executive Authority for National Security Surveillance*, 50 AM. U. L. REV. 1, 3-4 (2000). Professors Balkin and Levinson speculate that because the evidence obtained on alleged

deterring officials from engaging in unreasonable practices.[109] Indeed, absent the credible threat that an investigation will be for naught if it is shown to have been conducted in an extra-legal fashion,[110] officials may well be emboldened to act with less regard for legal formalities.[111]

B. Corporation's Perspective

Because a corporation has less to gain and far more to lose than the Executive does, a corporation's incentives to enter into an informal arrangement with the government are less clear. A firm is rewarded in full for its commercial success in the marketplace, but will receive only a small share of the benefit for any counterterrorism victory it helps to secure for the nation, especially if its involvement remains a state secret. Moreover, all of its handshake collaborations, and not just the patently illegal ones, leave the firm particularly vulnerable to shareholder and consumer lawsuits.[112] Yet, for a variety of (possibly misguided) reasons, corporations may nevertheless go along with the intelligence agencies' preference for informal intelligence-gathering partnerships.

From a rational economic actor's perspective, in order to prefer informality, the corporation would have to value the anticipated compensatory gains it would receive from agreeing to an ad-hoc or illegal collaboration over the benefits of either a formal, legalistic arrangement or no arrangement at all.[113] Presumably, corporations would define gains to include whatever "soft"

---

terrorists is often too tainted to be admissible in regular courts, the Bush Administration has not pursued those prosecutions. *See* Balkin & Levinson, *supra* note 1, at 524-25.

109. Moreover, even if there were an occasion to challenge, say, an incident of warrantless eavesdropping outside of the criminal-defense context—perhaps in the form of a *Bivens* action—a range of obstacles, including claims of executive privilege and the invocation of the state secrets doctrine, would make it more difficult to prevail than would be the case were a similar claim made in response to an ordinary (non-national-security) investigation. *Cf.* Banks & Bowman, *supra* note 108, at 87 ("The secrecy that attends [FISA Court] proceedings, and the limitations imposed on judicial review of FISA surveillance, may insulate unconstitutional surveillance from any effective sanction."); Oren Gross, *Chaos and Rules: Should Responses to Violent Crises Always Be Constitutional?*, 112 YALE L.J. 1011 (2003) (suggesting the possibility that in matters of national security even illegal acts would be ratified ex post, or at least not prosecuted); Editorial, *Wiretap Surrender*, WASH. POST, July 15, 2006, at A20.

110. This is not to say I am advocating the extension of the exclusionary rule to national-security investigations, the costs of which might well be too high for society to bear. *Cf.* Daryl J. Levinson, *Rights Essentialism and Remedial Equilibration*, 99 COLUM. L. REV. 857, 884-85 (1999) (discussing the concept of remedial deterrence and noting that in some instances "the threat of undesirable remedial consequences motivate[s] courts to construct . . . right[s] in such a way as to avoid those consequences").

111. *See Scott*, 524 U.S. at 378 (Souter, J., dissenting) ("Fourth Amendment standards will have very little deterrent sanction unless evidence offered for parole revocation is subject to suppression for unconstitutional conduct.").

112. *See, e.g.*, Hepting v. AT&T Corp., 439 F. Supp. 2d 974 (N.D. Cal. 2006); *see also* John D. Rockefeller IV, Editorial, *Partners in the War on Terror*, WASH. POST., Oct. 31, 2007, at A19 (suggesting harm that could come to collaborating corporations absent a grant of immunity).

113. Needless to add, when a corporation is asked to defy existing laws, its decision is

payments they receive in terms of favorable treatment in related regulatory and procurement contexts[114] and whatever positive media coverage would follow if it were ever made public that the companies provided crucial assistance to thwart an attack. Against this, corporations would have to calculate the possible losses they might incur in the form of diminished consumer confidence, debarment from government contracting, and possible lawsuits, were the secret, informal relationships exposed. The likelihood of lawsuits, customer revolts, or regulatory troubles might not have figured into the firms' calculations in, say, the immediate aftermath of the September-11 attacks, but it arguably ought to be part of their long-term thinking. No matter how much legal protection the Executive may promise to corporations during a terrorism crisis, if the tides change in Washington,[115] the corporations may find themselves in a precarious situation with little political or legal cover for their informal collaborations.[116]

There are at least two other explanations why a firm may agree to an informal relationship rather than insist on legal compulsion or simply decline to collaborate. Both explanations suggest structural flaws in corporate decision making that leave the firm potentially vulnerable to damaging lawsuits. The first turns on the principal-agent problem: corporations are run by individuals whose business judgment can be clouded. As Ron Suskind showed in describing how George Tenet wooed Western Union officials,[117] the

---

more complicated than when the government asks it to cooperate informally (but not illegally) in an unregulated intelligence domain.

114. *See supra* notes 46-47.

115. *See, e.g.*, FISA Amendments Act of 2008, H.R. 3773, 110th Cong. (2008) (omitting a retroactive-immunity provision for telecommunications firms that participated in the TSP); Jonathan Weisman, *House Passes a Surveillance Bill Not to Bush's Liking*, WASH. POST, Mar. 15, 2008, at A2 ("[The] House approved its latest version of terrorist surveillance legislation yesterday, rebuffing President Bush's demand for a bill that would grant telecommunications firms retroactive immunity for their cooperation in past warrantless wiretapping . . . ."). The House bill not only fails to provide immunity, it also makes it arguably easier to carry out private suits against the providers. By authorizing federal judges to review classified information *in camera* and ex parte, thus limiting the Executive's ability to invoke the state secrets doctrine (and, effectively, the Executive's ability to have the suit quashed), and by requiring the Attorney General to disclose any information that the courts may seek, the House measure would substantially increase the likelihood that the courts would reach the merits in civil cases. *But see* H.R. 6304 110th Cong. (2008) (providing retroactive immunity for telecommunications firms invested in the TSP after H.R. 3773 was opposed by the Senate and White House).

116. *See supra* note 112 and accompanying text; *see also* Scott Shane, *In Legal Cases, C.I.A. Officers Turn to Insurer*, N.Y. TIMES, Jan. 20, 2008, at A31 (describing CIA officers, concerned that the government might not provide them with legal protections for their actions in prosecuting the War on Terror, as purchasing private legal insurance to pay attorneys' fees); R. Jeffrey Smith, *Worried CIA Officers Buy Legal Insurance*, WASH. POST, Sept. 11, 2006, at A1 ("The new enrollments [in legal insurance plans] reflect heightened anxiety at the CIA that officers may be vulnerable to accusations they were involved in abuse, torture, human rights violations, and other misconduct, including wrongdoing related to the Sept. 11, 2001, attacks. They worry that they will not have Justice Department representation in court or congressional inquiries . . . ."). If core governmental actors feel this way, one can only assume that private agents would (or should) feel even more vulnerable.

117. *See supra* notes 52-56 and accompanying text.

intelligence agencies may make appeals to CEOs' personal vanities, friendship, or sense of patriotism to get them to expend corporate resources in a way that might not be consistent with their primary responsibility to their customers and shareholders.[118]

Second, corporations are not equal bargaining partners.[119] In many instances, the corporations do not have the same information the Executive has, and it might simply be convenient to place their trust in the government's representations. Thus, corporations may be misled into entering into what they do not realize are informal, quasi-consensual (rather than legally compelled) collaborations. One striking example of this information asymmetry involved military intelligence agencies misrepresenting their authority and leading corporate actors to believe that they were actually being legally coerced into complying, when, in fact, the agencies had no such power of compulsion.[120] Another instance occurred when several major airlines seemingly innocently turned over extensive amounts of passenger data to government contractors, evidently because they thought they were obligated to do so.[121] Moreover, because of good-faith provisos immunizing corporations from civil liability so long as they have reason to believe they are complying with the law,[122] firms do not always have sufficiently strong incentives to ask a whole lot of questions or necessarily to conduct their own legal research.

Thus, the failure to consider the long-term business consequences of informality, the inability to correct for principal-agent asymmetries, and the inadequacy of incentives to challenge intelligence agents' ad-hoc requests are all factors that make corporations more likely to agree to informal relationships.

III

THE INSCRUTABILITY AND ATTENDANT HARMS OF INFORMAL PRIVATE-PUBLIC

118. *See* Henry Hansmann & Reinier Kraakman, *The End of History for Corporate Law*, 89 GEO. L.J. 439, 439 (2001) ("There is no longer any serious competitor to the view that corporate law should principally strive to increase long-term shareholder value."); *see also* Schwartz, *supra* note 66.

119. *See, e.g.*, Joseph William Singer, *Real Conflicts*, 69 B.U. L. REV. 1, 43 (1989) (describing unequal bargaining power); *but see* Nicholas Parrillo, *"The Government at the Mercy of Its Contractors": How the New Deal Lawyers Reshaped the Common Law To Challenge the Defense Industry in World War II*, 57 HASTINGS L.J. 93 (2005).

120. *See* Eric Lichtblau & Mark Mazzetti, *Military Expands Intelligence Role in U.S.*, N.Y. TIMES, Jan. 14, 2007, at A1 (describing how military intelligence officers served corporations with NSLs that had no force of law); *see also* 2007 OIG REPORT ON NSL AUTHORITY, *supra* note 73 (detailing legal irregularities vis-à-vis the FBI's issuance of NSLs).

121. *See* Mark Glassman, *4 More Airlines Named in Release of Data*, N.Y. TIMES, June 24, 2004, at A17; *see also* Philip Shenon, *Airline Gave Defense Firm Passenger Files*, N.Y. TIMES, Sept. 20, 2003, at A1 (describing airline executives who turned over passenger information based on an "exceptional request" by the Pentagon).

122. *See, e.g.*, 18 U.S.C. § 2707(e) (2002) (granting good-faith civil immunity under the Electronic Communications Privacy Act for firms that rely on government representations of legal process); 50 U.S.C. § 1861(e) (providing good-faith civil immunity under the Business Records Provision of the USA PATRIOT Act).

PARTNERSHIPS

Having explored some of the central reasons why the Executive prefers informality in intelligence operations, I will now discuss some of the harms that handshake agreements may engender. As evidenced by the case studies discussed in Part I, the scope and intensity of the harms vary considerably among types of counterterrorism operations, reflecting the diversity of collaborative objectives and partnership arrangements. In what follows, I examine four sets of harms: legal, structural, market and societal, and strategic.

A. Legal Harms

Some informal relationships may violate constitutional and statutory law. The TSP represented a prominent example of an informal, electronic-surveillance arrangement that for years appeared to violate FISA's unambiguous "warrant" requirement, and quite possibly the Constitution as well.[123] This was the case until the Bush Administration decided in January 2007 to seek ex ante approval from the FISA Court for its eavesdropping operations[124] and subsequently sought legislative authorization for enhanced electronic surveillance powers.[125]

In addition, with respect to intelligence gathering and physical searches, the Executive's relationship with FedEx—specifically FedEx's willingness to open suspicious packages upon being orally asked to do so—may provide government officials with a convenient opportunity to bypass statutory (and possibly constitutional) laws.[126] That is, when a private company (and not the government) opens a package, otherwise applicable warrant requirements may not attach.[127] To date, too little information is publicly available about the

123. *See, e.g.*, ACLU v. NSA, 438 F. Supp. 2d 754 (E.D. Mich. 2006), *vacated on standing grounds*, 493 F.3d 644 (6th Cir. 2007); *see also* Daniel J. Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U. L. REV. 112 (2007) [hereinafter Solove, *First Amendment*]. For a description of the legal standoff over the TSP, see Dan Eggen & Paul Kane, *Gonzales Hospital Episode Detailed*, WASH. POST, May 16, 2007, at A1. *See also Preserving Prosecutorial Independence: Is the Department of Justice Politicizing the Hiring and Firings of U.S. Attorneys? – Part IV: Hearing Before the S. Judiciary Comm.*, 110th Cong. (2007) (statement of James B. Comey, Former Deputy Att'y Gen.), *available at* http://gulcfac.typepad.com/georgetown_university_law/files/comey.transcript.pdf.

124. *See* Lichtblau & Johnston, *supra* note 30.

125. *See* Protect America Act of 2007, Pub. L. No. 110-55, 121 Stat. 552; *see supra* note 86 (describing the Protect America Act, noting that it expired in February 2008, and discussing subsequent legislative activity).

126. *See supra* note 58 and accompanying text.

127. *See* United States v. Jacobsen, 466 U.S. 109 (1984); *but see* United States v. Robinson, 390 F.3d 853, 872 (6th Cir. 2004) ("[T]o trigger Fourth Amendment protection under an agency theory, 'the police must have instigated, encouraged, or participated in the search,' and 'the individual must have engaged in the search with the intent of assisting the police in their investigative efforts.'") (quoting United States v. Lambert, 771 F.2d 83, 89 (6th Cir. 1985)); United States v. Smith, 383 F.3d 700, 705 (8th Cir. 2004) ("We look to several factors in determining whether a private citizen was acting as an agent of the government. Chief among

FedEx-government partnership and whether the examples discussed in Part I.D. are representative of a larger pattern of practice. The threshold for warrants attaching may be met if the government's requests concern packages of a specific type, or sent from a specific set of names or neighborhoods, or if the requestor is a sufficiently senior government official. But if we imagine a tacit understanding of ongoing assistance, which would require the cooperating corporation to develop its own protocols to guide its employees with respect to how and when to respond to government inquiries, this de facto yet highly institutionalized collaboration might fall outside the scope of state action.

The use of "fourth parties" may provide another opportunity for the Executive to evade legal requirements. For example, we can conceive of a situation in which an Internet Service Provider, prohibited under the Stored Communications Act from turning over certain information to the government, but not forbidden from passing it to another private entity,[128] gives or sells customer data to a fourth party like ChoicePoint or LexisNexis. The fourth party can then give or sell the information to intelligence or law-enforcement agencies. In such a scenario, though no law may actually be violated (because the information was first transferred to another private party),[129] the government would nevertheless be engaging in data laundering of a sort that is uniquely entangled with privatization.

Less apparent from the case studies, but no less disconcerting, is another kind of laundering: the cleansing or leveraging of ill-begotten evidence. Government agents who receive intelligence through, for example, warrantless eavesdropping, have reportedly funneled that information back through the proper, formal channels. These agents may have reused the evidence to obtain faster FISA authorization for additional investigations, particularly in instances when the still-sought-after information is possessed by an entity that will not go along with informality;[130] or, the laundering may be done to re-run the same search, this time with the requisite court order in place, on those occasions when a criminal prosecution is in the offing, and the government needs to remove any potential taint of illegality from the evidence.[131]

---

these are whether the government had knowledge of and acquiesced in the intrusive conduct; whether the citizen intended to assist law enforcement agents or instead acted to further his own purposes; and whether the citizen acted at the government's request.").

128. *See supra* note 82 and accompanying text; *infra* note 271 and accompanying text.

129. *See supra* note 82 and accompanying text; *infra* note 271 and accompanying text.

130. *See* Carol D. Leonnig, *Secret Court's Judges Were Warned About NSA Spy Data*, WASH. POST, Feb. 9, 2006, at A1 (noting that illegally obtained evidence may have been used to secure legitimate court orders).

131. *See* SCHWARZ & HUQ, *supra* note 35, at 130-31 ("[E]vidence obtained illegally by the NSA was 'laundered' through the FISA process for potential use in a criminal trial."); *see also* OFFICE OF THE INSPECTOR GEN., U.S. DEP'T OF JUSTICE, A REVIEW OF THE FBI'S USE OF NATIONAL SECURITY LETTERS: ASSESSMENT OF CORRECTIVE ACTIONS AND EXAMINATION OF NSL USAGE IN 2006, at 131 (2008), *available at* http://www.usdoj.gov/oig/special/s0803b/final.pdf ("We . . . found that the FBI issued 11 'blanket' NSLs in 2006 that sought

These rule-of-law violations are no less troubling simply because the President likely could have obtained the necessary authorization from Congress, had he sought it. There is always the chance that Congress would refuse to go along with the most sweeping aspects of programs proposed; and, in any event, even if Congress agreed to authorize the programs in toto, it might nevertheless have insisted on at least some additional oversight measures.[132] But, even assuming Congress would have written the Executive a blank check, the institutional harms from bypassing Congress are no less significant.

In fact, the eschewal of otherwise obtainable legislative support may only exacerbate institutional harms. As Jack Goldsmith has written, the refusal to seek congressional authorization in due course was part of a strategy by President Bush and Vice President Cheney to strengthen executive power, "to leave the presidency stronger than they found it."[133] He concluded, however, that "[i]n fact they seemed to have achieved the opposite. They borrowed against the power of future presidencies—presidencies that . . . will be viewed by Congress and the courts . . . with a harmful suspicion and mistrust because of the unnecessary unilateralism of the Bush years."[134] Indeed, Goldsmith points to *Hamdan v. Rumsfeld* as a telling indication of the type of backlash against executive power, one far more forceful, and difficult to scale back than what would have been the case had the Bush Administration first asked Congress to authorize military commissions.[135] He also notes previous instances in which the Executive, seen as overreaching in terms of its unilateral exercise of intelligence-gathering policy in the 1960s and 1970s, was subsequently hamstrung by Congress, which responded in the late 1970s and 1980s in a severe (and perhaps security-jeopardizing) way.[136]

---

retroactively to justify the FBI's acquisition of data through the exigent letters *or other informal requests*.") (emphases added) [hereinafter 2008 OIG REPORT ON NSL AUTHORITY]. *Cf.* Adam Liptak, *Spying Program May Be Tested by Terror Case,* N.Y. TIMES, Aug. 26, 2007, at A1 (describing a criminal appeal of a U.S. person convicted of supporting terrorist activity, allegedly on evidence obtained through the TSP, as raising the illegality of the TSP as a basis for overturning the conviction).

132. *See, e.g.*, FISA Amendments Act of 2008, H.R. 3773, 110th Cong. (2008). As described by the *Washington Post*, H.R. 3773 "would challenge the Bush administration on a number of fronts, by requiring upfront court approval of most wiretaps, authorizing federal inspectors general to investigate the administration's warrantless surveillance efforts, and establishing a bipartisan commission to examine the activities of intelligence agencies in the wake of the Sept. 11, 2001, attacks." Weisman, *supra* note 115.

133. GOLDSMITH, *supra* note 7, at 140.

134. *Id.*

135. *Id.* at 139 ("If it had earlier established a legislative regime of legal rights on Guantanamo Bay, it never would have had to live with the Court's Common Article 3 holding, or with the War Crimes Act. If the administration had simply followed the Geneva requirement . . . or had gone to Congress for support of their detention program in the summer of 2004, it probably would have avoided the more burdensome procedural and judicial requirements that became practically necessary under the pressure of subsequent judicial review.").

136. *Id.* at 163 (highlighting the state of affairs when the discretion-versus-restraint pendulum swung too wildly during the 1960s, 1970s, and 1980s between executive and

Besides the legislative and judicial backlash, flagrant violations of the rule of law run the risk of further contributing to the erosion of America's moral authority internationally. Fair or not, the international community can point to the TSP or extraordinary rendition or the abuses at Abu Ghraib[137] and take easy shots at the United States. In so doing, they can effectively discredit our normative and legal pleas for other nations and peoples to respect the rule of law.[138]

B. Structural Harms

Informal intelligence-gathering arrangements may produce at least three sets of structural or institutional harms as well. One of these harms is the creation of an accountability gap, as informal collaborations are masked from Congress and the courts. The second results from privatizing sensitive responsibilities in a way that provides private actors with considerable power over personal information (far more than what they have when they possess the information outside of the intelligence-partnership context). A third is that informality may generate a ripple effect of questionable practices that reverberates throughout the federal government's regulatory and procurement realms.

1. Accountability

Because ad-hoc intelligence partnerships are essentially inscrutable, meaningful oversight is next to impossible. To be sure, the existing legal framework, even when followed, is no model of successful regulation, as both the ex ante authorization hurdles and the provisions for ongoing congressional or judicial monitoring are minimal.[139] Nonetheless, informal partnerships that

---

congressional dominance).

137. *See* Jeffrey K. Cassin, Note, *United States' Moral Authority Undermined: The Foreign Affairs Costs of Abusive Detentions*, 4 CARDOZO PUB. L. POL'Y & ETHICS J. 421 (2006). Note that, as in the case of the warrantless eavesdropping program, questions over America's use of extraordinary rendition, whereby detainees are transferred to third-party countries, and over its treatment of detainees at the Abu Ghraib facility in Iraq included the voicing of concerns over the role private agents played in these activities. *See* Jane Mayer, *The C.I.A.'s Travel Agent*, NEW YORKER, Oct. 30, 2006, at 34 ("Most of the planes used in rendition flights are owned and operated by tiny charter airlines that function as C.I.A. front companies, but it is not widely known that the agency has turned to a division of Boeing, the publicly traded blue-chip behemoth, to handle many of the logistical and navigational details for these trips, including flight plans, clearance to fly over other countries, hotel reservations, and ground-crew arrangements."); Michaels, *Beyond Accountability*, *supra* note 7, at 1033-34, 1067, 1072 (describing the role of private contractors in Abu Ghraib interrogations).

138. A comparison can be drawn to Cold War politics, when the Soviet Union pointed to America's dismal civil rights record as evidence that its moral claims could not be taken seriously. *See, e.g.*, MARY L. DUDZIAK, COLD WAR CIVIL RIGHTS: RACE AND THE IMAGE OF AMERICAN DEMOCRACY (2000); PHILIP A. KLINKNER WITH ROGERS M. SMITH, THE UNSTEADY MARCH: THE RISE AND DECLINE OF RACIAL EQUALITY IN AMERICA (1999).

139. *See supra* note 86.

operate outside of *any* positive-law framework (however weak), and quite possibly also ignore or shortchange the current congressional-disclosure requirements,[140] pose disproportionately serious structural concerns.

First, when not providing a formal accounting of their collaborative programs, the intelligence agencies are freed from a critical check on their powers. The very process of having to describe a program to Congress, to the courts, or simply to the head of their own agency, would lead officials to put forward more careful and well-thought-out proposals.[141] As Golove and Holmes note,

> The point is that accountability mechanisms are designed not to block the executive from achieving important policy goals supported by the public, but rather to enhance the effectiveness of executive decision-making by forcing executive officials to offer public justifications for their policy choices and thereby compelling them to act with more consistency. . . . Requiring the executive to submit to congressional or even bureaucratic oversight . . . [is one of] the best mechanisms we have for ensuring that executive policy does not veer off on ill-considered tangents, imperiling the very national interests that it claims to be advancing.[142]

As a corollary, oversight forces officials to think twice before authorizing excessive or overreaching practices.[143] With an eye to a tough Senate hearing (or, even to her next job), a responsible officer might be more likely to seek to moderate a particularly rights-depriving program of the sort that has discredited more than a few of her predecessors over the years.[144]

---

140. *See, e.g.*, 50 U.S.C. § 413(a) (2004) (requiring intelligence officials to "ensure that the congressional intelligence committees are kept fully and currently informed of the intelligence activities," including "significant anticipated intelligence activity"); ALFRED CUMMING, CONG. RESEARCH SERV., STATUTORY PROCEDURES UNDER WHICH CONGRESS IS TO BE INFORMED OF U.S. INTELLIGENCE ACTIVITIES, INCLUDING COVERT ACTIONS 2 (2006) (noting that the President must keep the congressional intelligence committees "fully and currently informed" of U.S. intelligence operations, including any "significant anticipated intelligence activity").

141. While it is not apparent what, if any, notification has been given to Congress in any given operation, *see supra* note 101 and accompanying text, what is clear is that oversight agents are almost entirely dependent on Executive reporting in instances involving intelligence operations that, for good reason, are not publicly observable.

142. Golove & Holmes, *supra* note 5, at 6.

143. *See* RISEN, *supra* note 27, at 59 (noting that the more the intelligence agencies act without oversight or accounting, the more likely it will be the case that such overreaching operations will become part of a permanent state of affairs); Martha Minow, *The Constitution as Black Box During National Emergencies: Comment on Bruce Ackerman's* Before the Next Attack: Preserving Civil Liberties in an Age of Terrorism, 75 FORDHAM L. REV. 593, 604 (2006) [hereinafter Minow, *Constitution*] (suggesting the importance of having historical records both of national-security programs and of the decisions to initiate those programs); National Security Letter Matters, Memorandum from Gen. Counsel, Nat'l Sec. Law Unit, Fed. Bureau of Investigation 3 (Nov. 28, 2001), *available at* http://www.aclu.org/patriot_foia/FOIA/Nov2001FBImemo.pdf (warning agents to be circumspect regarding the issuance of NSLs because Congress might question how the powers are being exercised).

144. *See, e.g.*, Maria L. La Ganga, *Scholar Calmly Takes Heat for His Memos on Torture*,

Second, without effective monitoring of the totality of the intelligence agencies' surveillance activities, Congress is ill-equipped to grasp the full scope of U.S. counterterrorism policies and commitments.[145] Because it does not know the range of the Administration's projects, the success of those operations, or the actual social, legal, and financial costs incurred,[146] Congress is not in a position to make informed legislative or appropriations decisions.[147] Moreover, what programmatic information Congress does possess is likely skewed to include only what the Executive wants to disclose through voluntary reports and selective compliance with mandatory requirements. Thus, Congress may be systematically misled into thinking that the Executive's operations are, on the whole, more successful and less intrusive than is actually the case. Over time, this misinformation may exacerbate the difficulties Congress faces in trying to flesh out the legal landscape regulating domestic intelligence operations.

Third, without effective oversight, an informal partnership is far more likely to experience mission creep of the sort suggested in Part II.A.[148] Undirected bureaucratic expansion is, of course, a classic concern with respect to any organizational structure.[149] This age-old problem is compounded here as

---

L.A. TIMES, May 16, 2005, at A1; Raymond Hernandez, *Bush Nominee Tries To Calm Torture Furor*, N.Y. TIMES, July 12, 2006, at A20; Paul D. Thacker, *Appointment Roils a Law School*, INSIDE HIGHER ED, Nov. 29. 2006, *available at* http://www.insidehighered.com/news/2006/11/29/delahunty. *Cf.* SCHWARZ & HUQ, *supra* note 35, at 56-58 (emphasizing the importance of a post-Iran Contra congressional amendment requiring Presidents to personally find that covert actions were necessary and important before commencing operations). For a further discussion regarding why mandatory disclosure to oversight agents might well lead intelligence officials to design more careful programs, see *infra* notes 263-264 and accompanying text.

145. *Cf.* PAUL R. VERKUIL, OUTSOURCING SOVEREIGNTY: WHY PRIVATIZATION OF GOVERNMENT FUNCTION THREATENS DEMOCRACY AND WHAT WE CAN DO ABOUT IT 113 (2007) (suggesting that improperly privatized executive activities and operations subvert Congress's "constitutionally designed accountability mechanism[s]").

146. *See* Kreimer, *supra* note 1, at 149 ("In any bureaucracy, you manage what you measure.") (internal citation omitted).

147. *See* Geoffrey Corn & Eric Talbot Jensen, *The Political Balance of Power over the Military: Rethinking the Relationship Between the Armed Forces, the President, and Congress*, 44 HOUS. L. REV. 553, 572-76 (2007) (emphasizing Congress's constitutional need to have access to national security and military information in order to make informed appropriations and legislative decisions); William P. Marshall, *The Limits on Congress's Authority To Investigate the President*, 2004 U. ILL. L. REV. 781, 799 ("[L]egislative judgment is impossible without access to information. Legislative bodies would be unable to effectively evaluate policy alternatives and weigh competing priorities if they could not call witnesses and otherwise inquire into complex issues. Indeed, it is often through congressional hearings and investigations that foundational ideas and insights of how to address social ills are generated.").

148. *See supra* note 94 and accompanying text.

149. *See* DANIEL PATRICK MOYNIHAN, SECRECY: THE AMERICAN EXPERIENCE 214 (1998) (noting that government intelligence agencies will expand their agendas and, essentially, reinvent themselves in order to stay relevant); J.R. DeShazo & Jody Freeman, *The Congressional Competition To Control Delegated Power*, 81 TEX. L. REV. 1443, 1454 (2003) (suggesting that agencies may exploit discretion and may seek to "expand their authority, enlarge their budgets, ensure their survival, . . . or otherwise pursue interests that may not coincide with those of

outside observers, either among the broad public or within the government, lack real opportunities to monitor subtle shifts in the partnership's agenda.[150] As they have in the past,[151] and as seems true today,[152] intelligence partnerships that lack clear, auditable guidelines (or minimization protocols) might well drift into unrelated law-enforcement domains.[153] One could imagine mission creep occurring in the context of a collaboration such as the government's reported relationship with Western Union. Without clear guidelines in terms of what information ought to be transmitted, and for what *limited* (i.e., national security) purposes, intelligence agents may, in the course of their work, encounter evidence of tax fraud, money laundering, immigration irregularities, or even indications of child-support evasions and may be prompted to initiate investigations completely unrelated to the War on Terror.

2. Outsourcing Sensitive Responsibilities

Another set of structural harms results from having private actors intimately involved in the collection of information for intelligence purposes. Although the corporations are the ones that possess the data in the first place, the fact that the firms are now in a position to shape the way the intelligence

---

Congress"); Daryl J. Levinson, *Empire-Building Government in Constitutional Law*, 118 HARV. L. REV. 915, 932-33 (2005).

150. *See* SCHWARZ & HUQ, *supra* note 35, at 133 (noting that the lack of clear guidelines and the absence of meaningful checks are "a recipe for mission creep"); *cf.* Mathew D. McCubbins et al., *Administrative Procedures as Instruments of Political Control*, 3 J.L. ECON. & ORG. 243 (1987) (suggesting that, absent oversight, bureaucrats are particularly likely to make decisions promoting personal preferences and career objectives).

151. *See, e.g.*, *Church Committee*, *supra* note 38.

152. *See supra* notes 57-68 and accompanying text.

153. Jack Balkin has noted the possibility that the Executive will use its ostensible war powers to displace investigations normally conducted within the bounds of the "criminal justice system . . . [that] come[s] with a series of traditional civil liberties protections that constrain and check the Executive." Balkin adds that if "the government can create a parallel law enforcement structure that routes around the traditional criminal justice system, and which is not subject to the oversight and restrictions of the criminal justice system, it may be increasingly tempted to make use of that parallel system for more and more things." Posting of Jack Balkin, The Twin Dangers of the National Surveillance State, to Balkinization, http://balkin.blogspot.com/2006/05/twin-dangers-of-national-surveillance.html (May 17, 2006, 09:04 EST).

This conflation of domestic and foreign tools and objectives is not new. Indeed, it may well have also happened a generation ago when intelligence operations were turned inward to spy on domestic "dissenters," namely those involved in the Civil Rights Movement and in anti-(Vietnam) war protests. *See* STAFF OF S. SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, 94TH CONG., FINAL REPORT ON INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, BOOK II, at 69-70 (Comm. Print 1976); Kitrosser, *supra* note 11, at 1181-95; Banks, *supra* note 3, at 1153. As a practical matter, the decision to use foreign-intelligence tools and procedures, *see, e.g.*, Robert Block, *U.S. To Expand Domestic Use of Spy Satellites*, WALL ST. J., Aug. 15, 2007, at A1, to investigate ordinary criminal activity raises two sets of concerns. First, law enforcement will have greater powers and fewer restrictions in its efforts to pursue suspects (than it should have under ordinary conditions). Second, a disproportionate number of Arabs and Muslims, i.e., the main targets of national-security investigations, will likely be ensnared.

agencies collect and process this information provides them with unique opportunities to affect public policy, possibly in abusive ways. In turn, corporations may also use what they learn from the government to re-examine their own data and how they treat those customers perceived to be under government investigation.

For example, poor data management by private businesses acting on their own may mean that the wrong customers are invited to a special sale or are shown pop-up online advertisements that do not correspond with their buying interests. On the other hand, false positives in the national-security context, which could come about through the government's reliance on faulty information obtained from the private sector, may result in the wrong person being placed on a no-fly list, or perhaps detained. One could also easily imagine instances where individuals tagged for surveillance by the government, possibly without any showing of heightened suspicion, are then treated differently by the collaborating corporation. For example, notwithstanding, say, a bank lacking any independent basis for having doubts about a particular customer (or even knowing why the government wants her records), the very fact that the government may be investigating that person may lead the bank to refuse to extend her a loan.

Of course, concerns with giving private actors day-to-day discretion over sensitive governmental functions are not new.[154] My point here simply is to note that the informality of these relationships, undefined and unmonitored, only exacerbates the potential dangers of private abuse or mismanagement.[155]

3. Contracting and Regulatory Corruption

Another structural harm is the ripple effect that may be generated by informal bargaining with the private sector. "Soft" payments, in the form of preferred treatment with respect to the private partners' other dealings with the federal government, may lead to distortions in what would otherwise be competitive procurement contests, impartial licensing adjudications, or regulatory-compliance evaluations.[156] To the extent these processes are corrupted because of promises made in the intelligence-gathering arena (recall

154. *See* COMMERCIAL ACTIVITIES PANEL, U.S. GOV'T ACCOUNTABILITY OFFICE, IMPROVING THE SOURCING DECISIONS OF THE GOVERNMENT: FINAL REPORT (2002); VERKUIL, *supra* note 145, at 23-46; Michaels, *Beyond Accountability*, *supra* note 7, at 1019-23; Minow, *Outsourcing Power*, *supra* note 84, at 1014-16; Schooner, *supra* note 15, at 553-56.

155. One safeguard often emphasized in discussions of government data-mining operations is the implementation of a strong auditing regime to ensure proper care is given to protect private information and to determine the bases for misuse of information as well as computer-generated false-positive identifications. *See, e.g.*, TECH. & PRIVACY ADVISORY COMM., U.S. DEP'T OF DEF., SAFEGUARDING PRIVACY IN THE FIGHT AGAINST TERRORISM 40-42 (2004), *available at* http://www.cdt.org/security/usapatriot/20040300tapac.pdf. With a purposely informal system, the implementation of a comprehensive auditing regime may be more unlikely.

156. *See supra* notes 46, 63-64 and accompanying text.

the NSA's alleged contracting relationship with Qwest[157] and consider also the possibility of favoritism, as evidenced by the various perquisites bestowed on the helpful FedEx, in contrast, we might suppose, to the less cooperative UPS[158]), palpable distortions could reverberate throughout the administrative state. The combined effect of these distortions and corruptions may ultimately deter Congress from delegating the optimal level of discretion to the Executive; instead, a frustrated legislature distrustful of the integrity of agency decision making may find itself forced to govern through more inefficient and cumbersome statutory mandates.[159] These would be yet additional instances of a backlash effect, that is, an arguably overblown—but understandable—response to counter unrestrained Executive unilateralism.[160]

C. Market and Societal Harms

Even if a given informal partnership is not aimed at defying governing legal requirements, a range of harms may still follow from the ostensibly lawful decision to proceed by handshake. For instance, left to their own devices, both corporations and intelligence agencies may systematically undervalue the social costs associated with the commodity being traded (i.e., private information)—and thus traffic in an inordinately high amount of citizens' personal information.[161] As in the case of industrial regulation of pollution, the possibility of exposing or misusing individuals' personal data is not fully internalized by the parties to the given transaction. Therefore, irrespective of what value society as a whole would assign to the personal information in question,[162] the parties to the transaction peg it comparatively lower.[163] In other words, without the government having to resort to legal process (e.g., by obtaining ex ante authorization and compelling corporate cooperation,[164]), the

157. *See supra* notes 46-47.

158. *See supra* note 60.

159. I thank David Super for helping me to develop this point.

160. *See supra* notes 133-136 and accompanying text.

161. *See* James P. Nehf, *Recognizing the Societal Value in Information Privacy*, 78 WASH. L. REV. 1, 11-13 (2003); Solove & Hoofnagle, *supra* note 4, at 382 (suggesting that "the business community has been loathe to recognize the costs of a lack of privacy to individuals"); Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1303 (2000) (noting that the market for private information "encourages transactions in data that most of us would prefer be discouraged"); Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2079 (2004) [hereinafter Schwartz, *Property*] (suggesting that corporations may buy and sell personal information at "below-market costs"); *cf.* Nicholas Bagley, *Benchmarking, Critical Infrastructure Security, and the Regulatory War on Terror*, 43 HARV. J. ON LEGIS. 47, 55 (2006) (describing how private companies undervalue risk-prevention investments).

162. Assuming, that is, that even in times of war the value of privacy is greater than zero.

163. *See generally* 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 (2007).

164. I assume that mechanisms such as reasonableness-of-search determinations, made by judges and pegged either to constitutional or statutory guideposts, help regulate the societal value of privacy rights.

"informal market" may transfer more information with fewer safeguards than is socially optimal, or even necessary.[165] If, on the other hand, the Executive and the corporations were required to internalize these social costs (say, if a robust oversight regime existed or if private rights of action were readily enforceable),[166] it is likely that the parties would have a greater incentive to reduce instances of over-trafficking in the information and thus better abide by whatever agreed-upon privacy protections were in place. This result would be similar to how corporations respond when forced by outside interests to come to terms with an environmental externality.[167]

Second, under any of the possible arrangements agreed to voluntarily or via legal compulsion, if word gets out that such partnerships exist for the purpose of domestic-intelligence gathering, there could be a chilling effect. Some individuals would be less candid on the telephone and over email (especially when voicing political dissent), and expressive activities would

165. Consumer-disclaimer provisions, which indicate that the consumer is agreeing to a company's use or disclosure of the information she provides to that company, have been viewed as having only modest effects on influencing consumer behavior. *See infra* note 178 and accompanying text. Presumably, restrictions on government access to that information, such as those prescribed in the Stored Communications Act, *see infra* note 271, reflect Congress's appreciation that consumers cannot adequately protect their privacy interests through contractual agreements with, among others, telecommunications companies.

166. *See* Kreimer, *supra* note 1, at 178-79 (positing ways to have intelligence agents work within hypothetical budgets of privacy costs); Schwartz, *Property*, *supra* note 161, at 2087-89 (referring to privacy as a public good and noting the applicability of the *Tragedy of the Commons* theory to the market for private information).

167. Notwithstanding the old bromide that only the guilty, or the paranoid, have anything to fear from privacy invasions, a significant number of individuals and groups of innocents—even those whose viewpoints and lifestyles are so-called mainstream—may well feel the legal, economic, social, and psychic effects of being the intended or inadvertent targets of an intelligence-gathering sweep. *See, e.g.*, Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1426 (2000); Nehf, *supra* note 161, at 11-13; Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1656 (1999); Daniel J. Solove, *"I've Got Nothing To Hide," and Other Misunderstandings of Privacy*, 44 SAN DIEGO L. REV. 745, 764-72 (2007) [hereinafter Solove, *"Nothing To Hide"*]. Currently, there may be inadequate safeguards to remedy situations when innocents become the victim of (1) misidentification, when someone is mistaken for someone else who has done something truly bad; *see* Eric Lichtblau, *Papers Show Confusion as Watchlist Grew Quickly*, N.Y. TIMES, Oct. 9, 2004, at A9; David Stout, *Inquiry Says F.B.I. Erred in Implicating Man in Attack*, N.Y. TIMES, Jan. 7, 2006, at A8; (2) misappropriation, when information ostensibly collected for national-security purposes is used to conduct unrelated investigations; *see* SOLOVE, DIGITAL PERSON, *supra* note 4, at 184 (noting that information compiled for purposes of constructing a suspected terrorist profile may be used to pursue a non-terrorist for illegally downloading music); *see supra* note 94; (3) dissemination, whereby personal information (however innocuous and uninteresting to busy, professional intelligence analysts) is released to a less discreet audience; *see* Steve Lohr, *Surging Losses, but Few Victims*, N.Y. TIMES, Sept. 27, 2006, at G1 (reporting that misplaced Department of Veterans Affairs data could expose many veterans to identity theft); and, (4) retaliation, when personal information is used to exact some form of blackmail; *see* Kreimer, *supra* note 1, at 149-51. Moreover, our own relationships may be impoverished by (5) chilling effects, whereby our associates may be less intimate and candid with us because they too are troubled by fears (1)–(4); SOLOVE, DIGITAL PERSON, *supra* note 4, at 176.

suffer.[168] Certainly, if such a chilling effect occurred, it would set in no matter what type of private-public intelligence-gathering partnership was reported by the press; but, if the arrangement were described as having been regulated pursuant to the dictates of the law, individuals could take some solace in the fact that the partnership's activities were accountable and being monitored for a requisite showing of cause.[169] They might also find some comfort in the fact that the firms were evidently protective of their customers, giving out information only upon pains of legal compulsion.

By contrast, when a legally informal relationship is exposed by the media, a consumer could reasonably fear that intelligence-gathering intrusions lack meaningful limits. Consider a counterfactual about New York's Container Inspection Program, which involves police officers conducting random searches of subway passengers in an effort to locate or deter concealed explosives.[170] While many passengers may find the random search itself to be bothersome and intrusive, they at least know that as a matter of unambiguous law the agents are forbidden from looking through reading materials or collecting personally identifying information about those searched.[171] If suddenly, however, it came to light that the police had mini-hand scanners and, notwithstanding the clear limitations on their discretion, were secretly cataloging personal information and triangulating it with time/location of people's travel and reading habits, it may well be the case that, on the margins, people may choose to take the bus (at least when they are carrying particularly personal materials). Thus, informality, and the corresponding uncertainty that

---

168. *See generally* Solove, *"Nothing To Hide," supra* note 167.

169. *See* Zeller, *supra* note 48 (describing the rise in Qwest's popularity after its refusal to cooperate in the NSA Call-Data Program was made public); *see also* Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264, 1270 (2004) [hereinafter Solove, *Reconstructing*]. Professor Solove also offers this particularly salient explanation:

> [A]ccording to the rationale behind the warrant requirement, it is the process of the government having to justify its searches before the judiciary that gives us the assurance that we can exercise our freedoms without the fear of improper government surveillance. Under our system of regulation of government searches, we cannot expect complete immunity from being subjected to a government search; but we can expect that we will not be searched contrary to established constitutional and legal procedures . . . [T]he very point of procedural regulation of government searches is to give people the assurance that they will not be searched without oversight and justification. It is the destruction of this assurance that constitutes the injury. There is a big difference between a system of highly regulated surveillance subject to oversight and limitation and a system of unregulated surveillance without oversight or limit beyond the whims of the executive branch. One might be significantly more chilled in speaking under the latter regime than under the former.

Posting of Daniel J. Solove, ACLU v. NSA, to Concurring Opinions, http://www.concurringopinions.com/archives/2007/07/aclu_v_nsa.html (July 7, 2007, 18:34 EST).

170. *See generally* MacWade v. Kelly, 460 F.3d 260 (2d Cir. 2006) (upholding the constitutionality of New York's Container Inspection Program).

171. *Id.* at 265 ("Officers may not attempt to read any written or printed material. Nor may they request or record a passenger's personal information, such as his name, address, or demographic data.").

attaches, may excessively chill expression or limit freedoms.[172]

Third, and building on the previous point, evidence that any private-public surveillance program operated without complying with the relevant regulatory requirements is likely to engender distrust of private industry writ large. Individuals confronted with the realities of legally informal relationships have no reason to believe that journalists or government watchdogs have smoked out all of the possible collaborations of that kind. Instead, people have cause for suspecting that if such partnerships exist in realms A and B, the government might just as likely be doing something improper in realms C and D, too.[173] These worries are only compounded when revelation of such partnerships, including the infamous NSA warrantless eavesdropping program, prompts an unrepentant President to insist that Congress grant retroactive legal immunity to the private parties involved.[174]

Fourth, companies within a market may be unable as a matter of law,[175] or simply unwilling, to signal that they are "pro-privacy" firms.[176] Corporations

---

172. For a discussion of the difficulties associated with gauging chilling effects, see Solove, *First Amendment*, *supra* note 127, at 154-58.

173. *See* Editorial, *More Domestic Spying*, WASH. POST, May 12, 2006, at A20 (asking "[w]hat else don't we know?"). Any expectation that the press will continue to root out and report on classified stories of this nature must be tempered by the realities that, for the first time ever, journalists are being seriously threatened with prosecution under the Espionage Act of 1917, *see* Walter Pincus, *Prosecution of Journalists Is Possible in NSA Leaks*, WASH. POST, May 22, 2006, at A4, and are being held in contempt of court for not disclosing their government sources, *see In re* Grand Jury Subpoena, Judith Miller, 438 F.3d 1141 (D.C. Cir. 2006); *Hatfill v. Mukasey*, No. 03-1793 (RBW), 2008 WL 623586, (D.D.C. Mar. 7, 2008), *available at* https://ecf.dcd.uscourts.gov/cgi-bin/show_public_doc?2003cv1793-224 (holding *USA Today* reporter Toni Locy in contempt of court for refusing to reveal the identity of her source for a news story on the 2001 anthrax attack).

An analogy can be made to the federal government's reported anti-drug programs that rewarded television stations and magazines with public-broadcasting and lucrative advertising deals, respectively, for promoting anti-drug messages in their television shows and articles. *See, e.g.*, Gia B. Lee, *Persuasion, Transparency, and Government Speech*, 56 HASTINGS L.J. 983, 983 & n.1 (2005); Daniel Forbes, *The Drug War Gravy Train*, SALON.COM, Mar. 30, 2000, http://archive.salon.com/news/feature/2000/03/31/magazines/print.html. The concern in these instances was that the government was purchasing editorial content without taking public ownership of the message, thus further discrediting a private marketplace already believed to be compromised by the influence of private industry's advertising dollars. *See* Forbes, *supra* ("'It strikes me as highly dubious. Editors should edit and the sales side should sell. Sure, I'm concerned. The way you describe it, it seems the editorial function has been compromised.' He added, 'There shouldn't be arrangements that are hidden from readers.'") (quoting Tom Goldstein, then-Dean of the Columbia University School of Journalism); *id.* ("'Most consumer magazines a long time ago turned themselves into delivery systems for advertisers.'") (quoting Lewis Lapham, editor of *Harper's*).

174. *See, e.g.*, Jonathan Weisman & Ellen Nakashima, *Senate and Bush Agree on Terms of Spying Bill*, WASH. POST, Oct. 18, 2007, at A1 (describing the legislative effort to immunize the telecommunications firms against private liability for their participation in warrantless eavesdropping and noting "Bush had repeatedly threatened to veto any [foreign-intelligence] legislation that lacked [an immunity] provision.").

175. *See* 18 U.S.C. §§ 793, 798 (2000); 18 U.S.C. § 2511(2)(a)(ii) (2002).

176. Even if a whistleblower provision existed, the reporting of misdeeds would likely not

might fear alienating the segment of the customer base that would view them as soft on terror, or risk retaliation from the government, as Qwest allegedly experienced.[177] Moreover, notwithstanding customers' potential antipathy to intrusive surveillance, it is difficult even for those who especially prize privacy to understand privacy agreements in their contracts with telephone, Internet, or courier companies; and, even leaving aside the difficulties associated with parsing the fine print, consumers cannot necessarily be faulted for prioritizing cost or convenience over a slightly more protective privacy policy, which they may still value, just not as highly.[178] Indeed, a customer's decision to devalue a firm's privacy promises seems especially justified in light of the fact that companies can unilaterally change their privacy policies at the drop of a hat. This is exactly what AT&T did soon after the NSA call-data scandal came to light.[179] In the end, much like a food scare involving only a handful of producers can lead to consumer avoidance industry-wide,[180] it is not clear that individuals will, for instance, flock to Qwest, which refused to collaborate in the NSA Call-Data Program, so much as they will be circumspect on the telephone no matter who carries their calls.[181] Thus, because of legal limitations on discussing matters of national security, because of imperfect market conditions, and because of informational asymmetries, there may not be a strong basis for believing that competitive business decisions alone will ensure the existence of privacy-friendly commercial outlets.

D. Harms from Corporations Opting Out

Finally, there is a hidden strategic harm. For every private entity such as a Qwest or a UPS that refuses to enter into an ad-hoc partnership with the Executive, potentially valuable information may go unanalyzed (provided the intelligence agencies lack the legal means or will to obtain the data via

---

be a public disclosure—i.e., to the marketplace—but rather would be made to a confidential body, such as the congressional intelligence committees or an inspector general's office, that could hear the allegations *in camera*.

177. *See supra* note 47 and accompanying text.

178. *See* Swire, *System*, *supra* note 3, at 1350 (noting that consumers often value cost over privacy in the short term, yet still consider loss of privacy to be one of their biggest long-term fears); SOLOVE, DIGITAL PERSON, *supra* note 4, at 82 (questioning whether people are actually "able to bargain effectively over their contracts with their Internet Service Providers, cable providers, telephone companies, and the like").

179. *AT&T Revises Privacy Policy for Customer Data*, N.Y. TIMES, June 22, 2006, at C1 (reporting that AT&T unilaterally changed its privacy policy in the wake of the NSA Call-Data Program leak and now insists all customer call records are property of AT&T).

180. I thank Daniel Solove for the analogy.

181. *See supra* notes 45-48 and accompanying text. The Internet and telecommunications companies provide the biggest challenge, for even if one can exercise caution about choosing a market competitor that signals a pro-privacy position, one cannot control whether one's correspondents are equally discriminating in selecting their service provider, *see* Solove, *Reconstructing*, *supra* note 169, at 1270, or even whether one's carrier shares the network of other carriers, which may be far less concerned about customer privacy.

compulsion).[182] Whether the non-participants cloak themselves in the mantles of civil libertarianism and consumer rights, signal that they do not appreciate being pressured, or simply fear legal repercussions, in the end, their discomfort in working informally (again assuming that legal compulsion is either unavailable or simply not desired) may ultimately impede the Executive's effort to combat terrorism.[183]

IV
PRIVATIZATION AS A MECHANISM FOR ENGENDERING COMPLIANCE AND ENHANCING ACCOUNTABILITY

The most obvious solution to this problem of extra-legality and the concomitant accountability gap (that may contribute to a state of *under*regulation) is to insist on greater compliance with the extant legal regime.[184] This straightforward prescription has two problems. The first complication is that the current legal framework substantively covers only some subset of possible operations; and, even where collaborations fall squarely within well-regulated domains, the oversight mechanisms are quite weak.[185] Accordingly, any isolated attempt to strengthen compliance and enforcement obligations placed on intelligence agents, without also expanding

182. *See* SOLOVE, DIGITAL PERSON, *supra* note 4, at 170-71, 175 (noting that the government may not resort to subpoenas or court orders but rather may simply request—and receive—cooperation).

Note that the problems of informal cooperation are even greater for multinational corporations, which are regulated not only in the United States but also in other nations where they do business. They are thus more likely to be hesitant to engage in informal collaborations. *Cf.* Dan Bilefsky & Eric Lichtblau, *Swiss Official Says Banks Broke Law by Supplying Data to U.S.*, N.Y. TIMES, Oct. 14, 2006, at A7.

183. *See, e.g.*, Cauley, *supra* note 44; Zeller, *supra* note 48; *see also* William H. Jones, *AT&T Hits Wider Role in Wiretaps; Ma Bell Shuns Wider Wiretap Role*, WASH. POST, June 27, 1978, at E1 (indicating that after Watergate the telecommunications companies insisted on greater legal process rather than continue to cooperate informally with the intelligence agencies).

184. Again, my assumption is that there is a bona fide need for the sharing of private data with the government, but that those relationships are at times under-regulated. Absent a convincing explanation why modest compliance-enhancing requirements would undermine national security, *see, e.g.*, Daniel J. Solove, *Data Mining and the Security-Liberty Debate*, 75 U. CHI. L. REV. 343, 353 (2008) [hereinafter Solove, *Data Mining*] (suggesting that the government ought to demonstrate that data mining actually produces results), what I propose seeks to improve oversight in a way that still permits the Executive great discretion to access privately collected information. Clearly, when the Executive asks for greater authority, Congress is ready to accommodate, and does so in short order. *See infra* note 261 and accompanying text.

185. Surveillance and intelligence-gathering policy should, as a matter of law and policy, include mechanisms for meaningful oversight, remain tethered to the rule of law, and yet ensure what I presume is the continued strategic effectiveness of said operations. *See, e.g.*, Swire, *System*, *supra* note 3, at 1340 ("[T]he two principal goals of the [intelligence-surveillance] system are protecting national security and doing so in a manner consistent with the Constitution, the rule of law, and civil liberties."); HEYMANN, *supra* note 1, at 159 ("[T]he challenge is not to beat and stop terrorism. The trick is to do it in a way most consistent with the values of a democratic society.").

the regulatory terrain, would be a half-hearted gesture. The second complication involves the Executive's institutional predisposition to act informally. Attempting to increase the rigor and scope of the laws regulating intelligence operations, such that the framework would be more robust, is likely to drive an even greater percentage of operations underground, precisely because the benefits of skirting regulations would be that much greater for an Executive now required to comply with more demanding accountability standards.

The first complication has already been discussed above[186] and thus need not be belabored here. It suffices to say the legislation in place now covers some *but not all* intelligence operations. Further, it is not clear whether the scope of coverage corresponds to an optimal equilibrium or to an equilibrium that exists largely because Congress cannot effectively act when it is systematically deprived of information of the sort that it normally uses as a basis for making legislative and regulatory decisions.[187]

Because to date scholars and lawmakers have not focused on the centrality of private actors in American intelligence-gathering operations, they have failed to appreciate the second complication—that placing more legal requirements between the Executive and its intelligence aims will likely intensify the Executive's thirst for informality. Analogous processes can be seen in any number of other regulatory areas where demand is relatively inelastic and a black-market alternative exists. For example, the number of fake IDs rises with an increase in the legal drinking age, and bookies receive more business when the government tightens the reins on legalized sports gambling.[188] The same principle is likely at play here, so long as patriotic, greedy, gullible, or bullied corporations can be persuaded to assist the Executive informally.[189] But, again, because the connection between operational informality and dependency on privatization has not been

186. *See supra* Part III.C.1; *see also supra* note 11 and accompanying text.

187. There are, of course, loopholes even within ostensibly regulated domains. For discussions of loopholes in the federal surveillance and privacy laws, see Kerr, *Internet Surveillance*, *supra* note 4 at 632-33, Solove, *Reconstructing*, *supra* note 169, at 1293, 1298, and Solove, *Fourth Amendment*, *supra* note 105, at 767. As has been noted, collaboration with private actors, often placed under different and lesser restrictions vis-à-vis federal surveillance laws, has not yet been fully appreciated by Congress in ways that might compel it to smooth out status differentials and eliminate the Executive's ability to use these outside entities to skirt rules. *See supra* note 23 and accompanying text. *Cf.* John Warner National Defense Authorization Act for Fiscal Year 2007, § 552, Pub. L. No. 109-364, 120 Stat. 2083, 2217 (2006) (amending 10 U.S.C. § 802(a)(10)) (eliminating some legal-status differentials between U.S. soldiers and military contractors); Michaels, *Beyond Accountability*, *supra* note 7.

188. This is not to say that the government should never impose stricter standards, but rather to suggest that it has to appreciate the collateral effects that such a change might produce.

189. With the imposition of greater legal requirements, there is also the problem that some potentially useful intelligence-sharing partnerships will simply not come together. It is thus essential that in ratcheting up the requirements for oversight, substantive reforms do not swing too far in the direction of over-regulation.

extensively explored, little progress has been made in addressing this concern.

The purpose of this final Part is to take up in tandem the problems of weak regulatory structures and weak enforcement mechanisms, both of which, in practice, are intimately tied to the Executive's capacity to resist oversight and its reliance on corporations for assistance in intelligence gathering.

A. Shifting Accountability Responsibilities to the Executive's Corporate Partners

As stated above, the Executive's preference for operational flexibility, its preoccupation with secrecy, its reluctance to accept congressional limits on its broadly defined war-power authority, and its relative immunity from serious legal or political sanction cast great doubt on the adequacy of a reform solution dependent on securing compliance from the intelligence agencies themselves. Thus, rather than simply (and perhaps stubbornly) insist that the Executive eschew informality and adhere to what the law dictates, it behooves us to recognize the potential gains that could be achieved by going directly to the corporations and requiring them to demand greater legal formality in their dealings with the intelligence agencies. Also, rather than simply (and again perhaps stubbornly, not to mention imprudently) ratchet up the prescribed standards for obtaining ex ante authorization to conduct intelligence operations, we must seek to incorporate more flexible regulatory measures that respect both the agents' need for discretion in tracking terrorists and the regulators' need for information to monitor intelligence operations on an ongoing basis.

Ultimately, shifting the principal locus of compliance responsibility from the Executive to the private actors and rethinking how intelligence policy can be effectively monitored and evaluated will provide a foundation upon which a new private-public surveillance regime can be built. Although perhaps counterintuitive, this regime will be sturdier than any that could be constructed if the Executive were autarkic vis-à-vis information gathering. That is, the intelligence agencies' reliance on private parties to help collect and analyze data may actually prove to be a blessing in disguise.

1. Corporate Actors as Second-Best Agents of Accountability

a. Burdening the Corporations

Instead of accepting the status-quo situation in which corporate intermediaries enable the Executive to drive search and surveillance operations further underground,[190] an opportunity exists to flip these private-public

190. *See* Kerr, *Internet Surveillance*, *supra* note 4, at 622 (noting that when providers can be trusted to protect privacy information, the concerns about government overreaching via "indirect surveillance" may be lower than when the government conducts the intelligence-gathering operation itself).

collaborations on their heads, effectively converting the corporations into bulwarks of accountable intelligence policy. As discussed, unlike the Executive, the corporations lack the institutional motivation to insist on operating pursuant to legally informal arrangements; and, also unlike the Executive, the corporations lack the political and legal means to resist congressionally imposed oversight and enforcement efforts.[191]

That is, whereas the Executive is singularly responsible for protecting American lives (and views informality as a means of achieving the desired flexibility and autonomy to counteract any and all threats), the corporations are more institutionally detached from the commitment to informality. Indeed, notwithstanding the corporations' general regard for American safety and security, their fiduciary duties and obligations to customers may, at times, conflict with the Executive's intelligence objectives.[192]

Corporations are also much more susceptible than is the Executive to congressional and judicial pressure in the opposite direction, toward adherence to a legal system requiring greater disclosure and procedural regularity under threat of criminal, civil, or administrative sanction.[193] As such, if given the proper carrots and sticks,[194] corporations can be made to help usher in a new era where private parties have no choice but to resist Executive entreaties for informality and instead serve as agents of enhanced compliance and regulation.[195]

Once made aware of such new burdens, corporations will be in the initially awkward, but ultimately empowering position of insisting that the intelligence agencies compel their cooperation consistent with governing laws.

---

191. *See supra* Part II.B.

192. One arguably egregious illustration comes from a January 2008 Department of Justice Inspector General report that noted that the FBI's tardiness in paying for the cost of surveillance services

> ha[s] resulted in telecommunications carriers actually disconnecting phone lines established to deliver surveillance results to the FBI, resulting in lost evidence including an instance where delivery of intercept information required by a Foreign Intelligence Surveillance Act (FISA) order was halted due to untimely payment.

AUDIT DIV., OFFICE OF THE INSPECTOR GEN., U.S. DEP'T OF JUSTICE, AUDIT REPORT 08-03, SUMMARY OF FINDINGS: THE FEDERAL BUREAU OF INVESTIGATION'S MANAGEMENT OF CONFIDENTIAL CASE FUNDS AND TELECOMMUNICATION COSTS 4 (2008), *available at* http://www.usdoj.gov/oig/reports/FBI/a0803/final.pdf. In this instance, it seems as if the telecommunications firm, perhaps one of the ones that participated in the TSP or the Call-Data Program, was willing to cut an active foreign-intelligence wiretap not out of fear of legal reprisal, but presumably to save money (or punish a delinquent customer).

193. Executive branch immunities include sovereign immunity from private suit, absolute and qualified immunity for government officials, and executive privilege to refuse informational inquiries.

194. *See infra* Part IV.B.3.

195. *Cf.* Mashaw, *supra* note 10, at 130 ("From an institutional design perspective, a perceived weakness in one regime leading to irresponsible behavior is not necessarily a signal that that form of accountability should be *strengthened.* It may be more effective . . . to amplify the effects of a potentially reinforcing [regime].").

These burdens could in fact come to be seen as liberating, particularly for those corporations currently being sued for their informal collaborations. Thus, notwithstanding the likelihood of a less cozy relationship with the Executive (and fewer perks now that they would no longer be playing ball),[196] the corporations ought to embrace the legal certainty that comes with being a more responsible party and may well even support the passage of such initiatives.[197] To that effect, though the telecommunications companies are currently pressuring the White House to provide them with greater guarantees of legal immunity for their alleged participation in the TSP, thus seeking to have their cake and eat it too, they have further signaled that if those protections are not forthcoming, they will not "cooperat[e] further."[198] In other words, if the White House fails to secure sought-after immunities,[199] the firms may well condition

196. Such concerns could be raised in any context in which greater regulation has been superimposed on a bilateral relationship. Anti-discrimination, landlord-tenant, and occupational-safety laws may "alienate" the worker from those with whom she interacts; *see generally* Vicki Schultz, *The Sanitized Workplace*, 112 YALE L.J. 2061 (2003), but the added protections she receives are often well worth any loss in informality. *See, e.g.*, Patricia J. Williams, *Alchemical Notes: Reconstructing Ideals from Deconstructed Rights*, 22 HARV. C.R.-C.L. L. REV. 401, 406-08 (1987).

197. Indeed, it should be remembered that the telecommunications firms, craving statutory clarity in the aftermath of the Church Committee's revelations of informal corporate collaboration with the U.S. intelligence and law-enforcement agencies, supported the 1978 passage of FISA. *See* Jones, *supra* note 183. *See generally supra* note 183 and accompanying text.

For other instances of private industry ultimately welcoming greater regulation, see generally John W. Maxwell et al., *Self-Regulation and Social Welfare: The Political Economy of Corporate Environmentalism*, 43 J.L. & ECON. 583 (2000). *See also* Spencer E. Ante, *The Other U.S. Military*, BUS. WK., May 31, 2004, at 76; David J. Lynch, *Corporate America Warms to Fight Against Global Warming*, USA TODAY, June 1, 2006, at B1. *Cf.* THOMAS C. SCHELLING, MICROMOTIVES AND MACROBEHAVIOR (1978) (describing professional hockey players' desire for rules mandating the wearing of helmets because even though they all preferred the added protection they would not individually choose to wear them unless all agreed to wear them).

In light of the fact that businesses viewed the legal protections provided to corporations under the Protect America Act as inadequate, *see, e.g.*, Harold Furchtgott-Roth, Editorial, *New FISA Law Is Insufficient Protection for Businesses*, N.Y. SUN, Aug. 6, 2007, at 10, and that prospective immunity from civil suit might be difficult to secure, *see supra* note 115 and accompanying text, there might be reason to believe that, in the long term, corporations would prefer simply to get out of the practice of informally (and extra-legally) aiding the government.

198. James Risen, *Bush Signs Law To Widen Reach for Wiretapping*, N.Y. TIMES, Aug. 6, 2007, at A1; *see also* Eric Lichtblau, *Immunity Crucial in Talks on Eavesdropping Rules*, N.Y. TIMES, Oct. 10, 2007, at A20 (describing the telecommunication industry as "mount[ing] a vigorous campaign" to secure legal immunity for assisting the government's intelligence-gathering activities); Eric Lichtblau & Scott Shane, *Phone Companies Seeking Immunity Gave to Senator*, N.Y. TIMES, Oct. 23, 2007, at A22 ("AT&T and Verizon have been lobbying hard to insulate themselves from suits over their reported roles in the security agency program by gaining legal immunity from Congress."); Eric Lichtblau et al., *Wider Spying Fuels Aid Plan for Telecoms*, N.Y. TIMES, Dec. 17, 2007, at A1 ("At stake [in the debate over legal immunity] is the federal government's extensive but uneasy partnership with industry to conduct a wide range of secret surveillance operations in fighting terrorism and crime.").

199. *See supra* notes 86, 115 and accompanying text (describing H.R. 3773, the House bill that, contrary to the wishes of the President and a majority of the Senate, did not grant the telecommunications firms retroactive legal immunity).

future cooperation on the existence of arm's-length relationships, mediated by instruments of legal authorization.

b. Fiduciary Duties Serving the Public Interest

Typically, privatization raises a host of accountability concerns, including that the contractors will not work diligently or carefully enough, that they will aggregate too much discretionary authority,[200] or that their activities will not be effectively monitored. In short, the concern is that a contractor's private interests (such as profit maximization) will, when it matters, take precedence over those of the taxpaying public.

But scholars have posited that in certain instances the introduction of private actors can actually increase accountability.[201] In addition to the conventional pro-privatization claims that market competition is the best guarantor of accountability, it has been argued, for example, that contractors eligible for performance bonuses might skip their lunch hour to help additional welfare claimants find gainful employment;[202] and, that private prison guards, lacking the qualified immunity against tort actions that is accorded to their civil-servant counterparts, might better maintain highly professional and safe correctional facilities.[203]

All of this is to say that the private sector may contribute positively to the imperatives of accountability and good governance, particularly when the public sector is itself not performing adequately and there are insufficient public levers (e.g., salary flexibility; performance-based promotions and demotions; credible civil liability) available to create the necessary incentives to improve work quality within the bureaucracy.

In this particular instance, there is at least one other important reason to believe that the element of privatization in the intelligence-gathering context can be accountability enhancing. Consider Jody Freeman's thesis that some of the fears regarding privatization could be allayed if it were established that contractors could be better inculcated with public-sector norms, a process she

200. *See supra* Part III.C.2.

201. *See, e.g.*, E. S. SAVAS, PRIVATIZATION AND PUBLIC-PRIVATE PARTNERSHIPS 187-88 (2000); Jack M. Beermann, *Privatization and Political Accountability*, 28 FORDHAM URB. L.J. 1507, 1524-26 (2001); Jody Freeman, *Extending Public Law Norms Through Privatization*, 116 HARV. L. REV. 1285 (2002); Michele Estrin Gilman, *"Charitable Choice" and the Accountability Challenge: Reconciling the Need for Regulation with the First Amendment Religion Clauses*, 55 VAND. L. REV. 799, 801 (2002) ("Supporters argue that . . . religious organizations provide more effective social services than governments because of the spiritual and moral guidance the religious organizations provide."); Michaels, *Deforming Welfare*, *supra* note 15, at 642-43 (describing arguments made by proponents of privatization).

202. *See generally* Freeman, *supra* note 201, at 1287-88 (characterizing claims made by proponents of privatization that performance-based pay in the private sector may improve quality of services provided).

203. *See* Richardson v. McKnight, 521 U.S. 399, 409-10 (1997).

calls "publicization."[204] Here, it seems as if we have the converse situation to Freeman's, and it may work just as well. Precisely because the corporations in this context cannot ever truly identify with the Executive (because of the fundamentally divergent financial, legal, and institutional dynamics at play here, as opposed to when contractors actively compete to *stand in* for government service providers and do exactly what government employees *used to do*), it is their detachment from the intelligence agencies' counterterrorism agenda that makes them less likely to disregard the law in the name of national security.

Thus, given the Executive's uncompromising focus on thwarting terrorism and history of disregarding statutory and constitutional restrictions, the existence of, to borrow from Freeman's terminology, a decidedly non-"publicizated" private cohort, beholden to its own commitments, might provide a convenient counterweight. If so, it would be particularly advantageous for reformers in Congress to align (more clearly) the corporations' private interests with a regime of legal formality in intelligence collaborations.[205]

2. Inadequacy of "Search Warrant" Paradigm

Having discussed the basis for shifting the burdens of compliance to corporations, it is time to consider augmenting the accountability provisions and creating greater opportunities for effective oversight.

To accomplish this, we must appreciate that national-security investigatory operations are analogous to police searches mainly at the ex ante

---

204. *See* Freeman, *supra* note 201, at 1314-50.

205. Skeptics may stop here and challenge the claim that adversity between private interests and government interests can readily be assumed. They will, with justification, point to the state of government contracting today as evidence that the corporations are hardly likely to fear sanction or find a reason to distance themselves from their patrons in the Executive Branch. *Cf.* Jack M. Beermann, *Administrative-Law-Like Obligations on Privat[ized] Entities*, 49 UCLA L. REV. 1717, 1735 (2002) ("Government may be dominated by pro-privatization forces who favor strong deregulation as part of an effective privatization program. The political environment may force these people to engage in supervision for show, with a wink and a nod. In contracting-out situations, cozy relationships between private contractors and the government agents charged with monitoring them may help explain waste and mismanagement. Politicians may be able to deceive their constituents into believing they are doing their best in supervising privatized entities when in actuality they are not."). Indeed, contractors in Iraq or in New Orleans after Hurricane Katrina have effectively donned Teflon coating when it comes to being held accountable for gross mismanagement, and the federal government's ability to monitor procurement contracts is questionable at best. *See, e.g.*, Robert O'Harrow Jr. & Scott Higham, *Interior, Pentagon Faulted in Audits; Effort To Speed Defense Contracts Wasted Millions*, WASH. POST, Dec. 25, 2006, at A1. But here, the accountability factors are different, in no small part because unlike, say, with a no-bid major defense contract, the claims here would not be mismanagement (and possibly fraud), but violations of statutory law. That is, there is less of an upside for failure to comply (i.e., no "sweetheart" deal) and a greater downside. Thus, the comparison—to the extent any is warranted—is more to whether corporations are inclined to comply with corporate-securities disclosure requirements, *see infra* notes 223-225 and accompanying text, than whether they are going to be good corporate citizens when it comes time to bid on lucrative contracts.

stage, when intelligence agents, like police detectives, must clear initial authorization hurdles to proceed.[206] But outside of the instances where foreign-intelligence court orders expire (and need to be reauthorized),[207] there are otherwise relatively few opportunities for ongoing or ex post review of intelligence operations, let alone of the robust sort of review that is built into constitutional criminal procedure.[208]

First, even when an intelligence operation triggers a legal obligation, the standards for obtaining authorization are, as noted above, different and in some respects lower than those governing ordinary criminal search and surveillance law.[209] While there is good reason to keep the ex ante requirements to a minimum (e.g., to permit rapid responsiveness in emergency situations),[210] inevitably there is a cost associated with giving intelligence agents wider discretion to commence operations, and thus there ought to be a correspondingly greater need for corrective tools to remedy instances (not to mention patterns) of overreaching or abuse. Notwithstanding this greater need, the ex post corrective measure most common in the police-search context is largely unavailable here. In ordinary criminal law, the reasonableness and propriety of an investigatory search operation is subject to an *after-the-fact* check by an Article III judge in the form of a suppression hearing.[211] But because national-security investigations usually do not lead to regular, criminal trials but instead to detentions, deportations, or just further investigations (with the aim of catching the principals overseas in a military operation), there is no comparable deterrent on the U.S. intelligence agents.[212]

Second, national-security investigations are often *pattern*-based, rather

206. *See supra* note 86.

207. *Id.*; *see also* 50 U.S.C. § 1805(e) (2006).

208. *See supra* note 86.

209. *See id.*

210. Leaving aside the compliance problem, one might be tempted to propose raising the ex ante standards for securing authorization to initiate intelligence operations, thus eliminating the need for ex post corrective measures. But that ostensibly more surgical solution overlooks two major problems. First, we would want to avoid a chilling effect: if the ex ante hurdles are too high, worthwhile investigations may never get off the ground. Second, as much as this Article focuses on the need to restrain an overreaching Executive, I have not suggested that Congress or the courts are better positioned to decide in the first instance how to target, design, or commence intelligence operations.

211. *See supra* notes 105-109 and accompanying text.

212. *See, e.g.*, Robert M. Chesney, Panel Report, *Beyond Article III Courts: Military Tribunals, Status Review Tribunals, and Immigration Courts*, 5 CARDOZO PUB. L. POL'Y & ETHICS J. 27 (2006).

Even in the rare instances when foreign-intelligence investigations lead to regular criminal prosecutions, because foreign-surveillance court orders may not be required as a constitutional matter, *see* United States v. U.S. Dist. Court (*Keith*), 407 U.S. 297, 321-22 & n.20 (1972); Zweibon v. Mitchell, 516 F.2d 594, 613-14 (D.C. Cir. 1975), and because not all of the statutory laws that regulate foreign-intelligence operations provide suppression remedies, *see* Kerr, *Lifting*, *supra* note 107, at 824-25; Solove, *Reconstructing*, *supra* note 169, at 1285, aggrieved parties might not be able or prepared to challenge allegedly ill-begotten evidence.

than *subject*-driven. These searches purposely sweep in thousands if not millions of completely innocent persons. The idea of remediation for innumerable violations by way of an individualized challenge before a judge, however well it may work in the conventional criminal-trial context, does not carry over into the world of wide-scale intelligence operations.[213]

For these reasons, to counterbalance the permissive ex ante discretion and to compensate for the absence of an automatic and robust ex post suppression remedy, alternative mechanisms must be developed that allow independent actors to review and, if necessary, intervene with regard to *already* operational investigations.

B. Designing a Compliance and Disclosure Regime

Translating these realizations—both that compliance and accountability can be enhanced in situations where corporations can be made to regulate government overreaching and that efforts must be made to ensure greater opportunity for corrective interventions—into a plan of action, I propose a set of reforms that harness the resources of the private sector, Congress, the courts, as well as of officials within the Executive Branch who are further removed from the immediate pressures of combating terrorism. Utilizing a multi-layered strategy, in no small part because of the political and institutional limitations of each of the actors to serve, on its own, as the definitive line of defense against overreaching or extra-legal operations, the reforms focus on intra-governmental transparency and serve to provide security-cleared government officials with the requisite information and opportunity to recalibrate and restructure the legal framework. While in other contexts unabridged public disclosures might well be the preferable model of accountability and enforcement,[214] that avenue seems to be foreclosed in this national-security setting where the benefits of public disclosure to concerned citizens are more than offset by the dangers of tipping our hand to would-be terrorists.[215]

---

213. *See, e.g.*, Dempsey & Flint, *Commercial Data*, *supra* note 4, at 1464-68; Rubenstein et al., *supra* note 21, at 273-74.

214. *See, e.g.*, Council Directive 95/46, arts. 10, 11, 23, 24, 1995 O.J. (L 281) 31 (EC).

215. *See* Lawrence Wright, *The Spymaster: Can Mike McConnell Fix America's Intelligence Community?*, NEW YORKER, Jan. 21, 2008, *available at* http://www.newyorker.com/reporting/2008/01/21/080121fa_fact_wright (quoting Director of National Intelligence McConnell as suggesting, with respect to intelligence information, that "[i]f I have to inform the public, I am informing the adversary").

It is commonly suggested that Congress cannot keep secrets. *See* Eric A. Posner & Adrian Vermeule, *The Credible Executive*, 74 U. CHI. L. REV. 865, 885 (2007) (noting the "standard executive claim that Congress leaks like a sieve, so that sharing secret information with legislators will result in public disclosures"). In the framework I lay out, however, the information will flow in the first instance to members of the relevant oversight committees, typically intelligence and judiciary. The narrower scope of disclosure increases the likelihood that the information will remain closely held, and the committees, whose members will only continue to receive the information if they can rebut the presumption that they will leak, can impose informal sanctions on wayward members. Indeed, even Posner and Vermeule suggest that bringing potential

The reforms thus pivot on mandating (1) corporate insistence on being served with the requisite instruments (warrants, subpoenas, etc.) of legal compulsion, effectively creating a symmetrical burden that neither the government nor the third-party possessor of the sought-after information can waive; (2) corporate disclosures describing the nature of the collaborations to Congress and to the inspectors general of the agencies conducting the operations; and, (3) escalating burdens of proof that require agencies periodically to demonstrate to the FISA Court the continuing utility of ongoing operations. This framework of gatekeeping, reporting, and reviewing will ultimately engender a dynamic model of greater oversight and inter-branch management of novel intelligence programs.

1. Gatekeeping: Arm's-Length Partnerships

The first requirement placed on corporations should be that, irrespective of any other duties or responsibilities, they must make an independent determination whether the intelligence agencies are proceeding in accordance with the law. Failure to insist on being served with the proper warrants or subpoenas (where such instruments are legally necessary) would leave a participating corporation and its executives exposed to a range of penalties.

This obligation for corporations to insist on legal compulsion cannot be waived, and thus will be a burden on the government and the companies alike. This makes sense not only from the expected instrumental benefits we hope to enjoy in terms of greater overall compliance with existing rules, but also insofar as legislating symmetry will make this statutory regime a closer analogue to core Fourth Amendment doctrine.

For example, third parties that, as a constitutional matter, can waive the warrant requirement and consent to the police entering a home without a warrant tend to be those most closely trusted by the "target" of the given investigation.[216] Because they are spouses, family members, or roommates, cloaked with equal authority over a given domain and thus assumed to have been entrusted to look after the interests of the premises they share in common with their cohabitants, they are allowed to speak for one another.[217] That said,

whistleblowers into the deliberative processes will engender a greater trust relationship. *See id.* at 903. In any event, it is likely the case that the leaks that have exposed a range of post-September 11 intelligence operations were a product of internal frustrations within the Executive Branch, namely that the intelligence initiatives were not undertaken consistent with the expectations of the rule of law. In other words, given the availability of a formal outlet to other governmental actors, perhaps the impulse among Administration officials to leak might be lessened, insofar as those would-be leakers can rest easier knowing that there are more discreet ways to ensure oversight and remediation.

216. *See, e.g.*, United States v. Matlock, 415 U.S. 164, 171 n.7 (1974).

217. *See, e.g., id.* at 170 (holding that a fellow occupant of a home can consent to a warrantless search of that home); Frazier v. Cupp, 394 U.S. 731, 740 (1969) (determining that either person who jointly shared a duffel bag could consent to a warrantless search of that bag). *See generally* Georgia v. Randolph, 574 U.S. 103 (2006) (describing co-occupant consent-to-

courts have not extended third-party consent prerogatives to such individuals as hotel proprietors[218] or apartment landlords.[219] Notwithstanding the fact that landlords and hotel managers are allowed to enter an occupant's quarters for maintenance purposes,[220] they are not permitted to let the police in—in no small part because there is a wider divergence of interests between, on the one hand, a landlord-tenant or hotel-guest relationship and, on the other, a husband-wife or roommate relationship.[221] Surely the relationship between an individual and her bank or telephone company is more akin to the one she has with her landlord than with her roommate. The telephone company can, on its own, check the customers' records for errors and even monitor the content of calls for "quality assurance" purposes. But, it is a qualitative leap to assume that the companies can consent to government eavesdropping, and the courts have not come close to making that jump.[222]

2. Reporting: Corporate Disclosures

As a second step, corporations should be required by law to file reports explaining any informal or formal agreement to share or transfer information about U.S. persons to military or intelligence agencies. These reports, which would summarize the details of the collaboration and identify what type of legal process, if any, was used to secure cooperation, should be sent, under seal, to members of the House and Senate intelligence and judiciary committees, as well as to the inspector general of the participating government agency. Although the disclosure obligations might seem onerous, they are not very different from other instances in which private actors have been required by law to file reports to assist in public law-enforcement initiatives, involving capital-markets regulation,[223] anti-money-laundering efforts,[224] and public-

search cases).

218. Stoner v. California, 376 U.S. 483, 487-88 (1964).

219. Chapman v. United States, 365 U.S. 610, 616-17 (1961).

220. *See* United States v. Jeffers, 342 U.S. 48, 51 (1951) (noting that although the hotel proprietor had access to a guest's room for cleaning and maintenance purposes, there was no corresponding authority to allow the police to enter).

221. *See Randolph*, 574 U.S. at 111-12 ("[Co-tenants] understand that any one of them may admit visitors, with the consequence that a guest obnoxious to one may nevertheless be admitted in his absence by another. As [*United States v.*] *Matlock* put it, shared tenancy is understood to include an 'assumption of risk'. . . . [But a person] who identifies himself, say, as a landlord or a hotel manager calls up no customary understanding of authority to admit guests without the consent of the current occupant.").

222. I recognize that there is another line of Fourth Amendment doctrine that focuses on the reasonable expectation of privacy in certain information turned over to third parties, and I have cited the landmark opinions above. *See supra* note 23 (discussing *Miller* and *Smith*). While there are independent problems with the logic of those decisions, *see* Solove, *Digital Dossiers*, *supra* note 19, at 1134-37, those cases turned on a different question from whether, assuming the information is protected (either constitutionally or, as I propose, a matter of federal statutory law), the right of a third party to turn that over to the authorities, absent an instrument of legal compulsion, exists.

223. *See, e.g.*, Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, §§ 401-09, 116 Stat. 745,

corruption concerns.[225] Moreover, to the extent each of these other disclosure laws places the affected corporation at odds with even its law-abiding clients (who may prefer greater anonymity), the requirements here to report on partnerships with the Executive (the "client" in the intelligence-gathering contexts) are of a similar vein.[226]

a. Congressional Oversight

Armed with data far more detailed and more timely than what it currently receives,[227] Congress could decide to hold hearings (*in camera*, if necessary to preserve classified information) to investigate programs that it suspects are misguided, insufficiently attentive to privacy concerns, overly burdensome to the corporations, or exploitative of the status differentials that make it legally easier for the private sector to collect information and give it to the government than for the intelligence agencies to obtain the data in the first place.[228] Congress could also hold up confirmation votes on nominees as leverage to force the Executive to make concessions.[229] Or, it could de-fund a given

785-91 (amending reporting requirements pursuant to 15 U.S.C. § 78m). Note that because the Director of National Intelligence can now waive SEC reporting requirements to the extent they reveal anything about national-security matters, *see* Dawn Kopecki, *Intelligence Czar Can Waive SEC Rules*, BUS. WK. ONLINE, May 23, 2006, *available at* http://www.businessweek.com/bwdaily/dnflash/may2006/nf20060523_2210.htm, corporations are not currently required to turn over information of the sort contemplated in the proposals put forth herein.

224. *See, e.g.*, Bank Secrecy Act of 1970, Pub. L. No. 91-508, 84 Stat. 1114 (codified as amended at 31 U.S.C. §§ 5311-30); *see also* Sandra Block et al., *Banks, Insurers Required To Report Suspicious Activity*, USA TODAY, May 12, 2006, at B4.

225. *See, e.g.*, Lobbying Disclosure Act of 1995, Pub. L. No. 104-65, 109 Stat. 691 (codified at 2 U.S.C. §§ 1601-07). For a detailed description of what the disclosure requirements entail, see Office of the Clerk, U.S. House of Representatives, Guide to the Lobbying Disclosure Act, http://lobbyingdisclosure.house.gov/lda_guide.html#section6 (last visited Feb. 18, 2008).

226. Indeed, as evidence of the feasibility of pursuing a project of this sort, it should be noted that Congress has at various times contemplated enhanced disclosure requirements that would be close to what I am proposing here. *See, e.g.*, Carl Hulse, *House Democrats Planning New Intelligence Oversight*, N.Y. TIMES, Dec. 15, 2006, at A36.

227. *See supra* notes 86, 103 and accompanying text.

228. *See* Minow, *Constitution*, *supra* note 143, at 604-05 (suggesting *in camera* congressional and judicial oversight as a fair compromise between security and liberty imperatives); Sam Nunn, *The Impact of the Senate Permanent Subcommittee on Investigations on Federal Policy*, 21 GA. L. REV. 17, 18 (1986); *see also* WOODROW WILSON, CONGRESSIONAL GOVERNMENT: A STUDY IN AMERICAN POLITICS 303 (1885) ("It is the proper duty of a representative body to look diligently into every affair of government. . . . It is meant to be the eyes and the voice, and to embody the wisdom and will of its constituents. . . . The informing function of Congress should be preferred even to its legislative function.").

229. *See generally* THE FEDERALIST NO. 77 (Alexander Hamilton); *see also, e.g.*, YOO, *supra* note 7 at 125 (emphasizing the Senate's confirmation power as a tool to influence the Executive); Susan Chandler, *McCain Rips Air Force over Boeing Dealings*, CHI. TRIB., Dec. 9, 2003, at C1 (describing Senator John McCain's refusal to allow a confirmation vote for a Pentagon nominee, based on the Defense Department's failure to cooperate fully with a Senate investigation).

program, which it has previously done when it disapproved of an intelligence or national-security operation.[230] (It should be underscored, of course, that even a minority within Congress can wield tremendous influence, by insisting on various amendments to critical bills, by itself trying to hold up nominees, or, at least in the Senate, by filibustering.)

The appropriations power[231] may be particularly potent in the intelligence budgetary arena. Intelligence budgets are treated differently from much of the rest of the overall federal budget,[232] and to the extent intelligence line appropriations can remain classified yet be subject to programmatic-level revisions, Congress would have both the dexterity and political cover to exercise aggressively its co-ordinate powers over intelligence policy. That is, the ability to tinker with funding streams on a regular basis gives the legislature a means of acting promptly upon its concerns.[233] What is more, the concomitant opportunity to appropriate in a manner largely occluded from the public gives lawmakers the political freedom to challenge imprudent intelligence policies with less fear of being harshly punished at election time for their so-called "soft-on-terrorism" vote—a fear that routinely prevents many a member from voting against (publicly recorded) military-spending bills. When a vote to deny military appropriations is taken as an article of disloyalty, as it often is, representatives lose perhaps the most straightforward and valuable means of influencing foreign policy.[234] None of this is, of course, to say that Congress

230. *See* Homeland Security Act of 2002, Pub. L. No. 107-296, § 880, 116 Stat. 2135, 2245 (codified at 6 U.S.C. § 460) (de-funding the Terrorist Information and Prevention System); Pub. L. No. 108-87, § 8131, 117 Stat. 1054, 1102 (2003) (de-funding Terrorism Information Awareness data-mining project); *see also* Michaels, *Beyond Accountability*, *supra* note 7, at 1057 n.191 (cataloging instances where Congress has restricted funds to curtail or register opposition to military engagements).

231. U.S. CONST. art. I, § 9, cl. 7.

232. The intelligence budget, and the underlying intelligence appropriations process, is largely shielded from public scrutiny. Indeed, only twice has the numerical dollar amount of the intelligence budget ever been released, and the public has never been provided with any significant budget breakdown by agency, program, or activity. *See* STEVEN DAGGETT, CONG. RESEARCH SERV., THE U.S. INTELLIGENCE BUDGET: A BASIC OVERVIEW (2004), *available at* http://www.fas.org/irp/crs/RS21945.pdf.

233. A proposal by Speaker Nancy Pelosi to merge appropriations and intelligence oversight into one committee, though different from my recommendations, especially with respect to the degree of public disclosure involved, reflects the type of innovative thinking that Congress must embrace if it is to take seriously its duties to weigh in on important matters of intelligence policy that intimately affect issues of security and privacy. *See* Hulse, *supra* note 226.

234. *See generally* Kate Stith, *Congress' Power of the Purse*, 97 YALE L.J. 1343 (1988); *see also* WILLIAM C. BANKS & PETER RAVEN-HANSEN, NATIONAL SECURITY LAW AND THE POWER OF THE PURSE 119, 137-57 (1994); Lori Fisler Damrosch, *Covert Operations*, 83 AM. J. INT'L. L. 795, 797-98 (1989) (suggesting that once Congress is informed of a covert operation that it does not support, it can work to cut off its funding); John Hart Ely, *The American War in Indochina, Part II: The Unconstitutionality of the War They Didn't Tell Us About*, 42 STAN. L. REV. 1093, 1105 (1990) ("Even the staunchest supporters of presidential power . . . [concede] that if Congress does not like the way a war is being conducted it can pull the financial plug on it."); Harold Hongju Koh, *Why the President (Almost) Always Wins in Foreign Affairs: Lessons of the*

will need to scrutinize every penny spent on intelligence matters. Most operations, like most expenditures in the larger budget or, say, most military promotions requiring Senate confirmation, will be approved as a matter of course.[235] But the option to affect funding when necessary to redirect misguided policy is not an inconsequential one.

Moreover, Congress's power to conduct investigations[236] must be strengthened internally. No doubt the Democratic takeover of Congress in 2007, and the new majority's decision to make broader inquiries into the Executive's handling of intelligence policy,[237] influenced the Bush Administration's decision to submit the TSP to FISA Court review[238] and, ultimately, to seek legislative authorization.[239] But, as the prior six years showed, when the same party controls both ends of Pennsylvania Avenue, the congressional majority may be reluctant to investigate or pressure its friends in the White House.[240] Thus, for the long-term benefit of Congress as an institution, the legislature should consider establishing limited subpoena power rights for the minority party.[241] Extending minority rights for *in camera*

Iran-Contra Affair, 97 YALE L.J. 1255, 1267 (1988) (noting that in the 1970s "Congress enacted seven separate provisions declaring that no funds authorized or appropriated . . . could be expended to support United States military . . . forces in Vietnam, Cambodia, or Laos").

235. After all, the Senate voluntarily takes on the responsibility of endorsing (or refusing to endorse) the promotion of *every* military officer at and above the rank of major in the Army, Air Force, and Marines, and lieutenant commander in the Navy. 10 U.S.C. § 531 (2004); *see also* Weiss v. United States, 510 U.S. 163, 182 (1994) (Souter, J., concurring) (noting that Senate confirmation of "inferior" military officers is not a constitutional obligation but one Congress affirmatively chose to establish).

236. *See, e.g.*, Louis Fisher, *Congressional Access to Information: Using Legislative Will and Leverage*, 52 DUKE L.J. 323 (2002).

237. *See, e.g.*, David Johnston, *Stormy Outlook as Gonzales Faces Senate Democrats*, N.Y. TIMES, Jan. 13, 2007, at A13; David Johnston & Scott Shane, *Senators Demand Details on New Eavesdropping Rules*, N.Y. TIMES, Jan. 19, 2007, at A18; *see also Preserving Prosecutorial Independence: Is the Department of Justice Politicizing the Hiring and Firings of U.S. Attorneys? – Part IV: Hearing Before the S. Judiciary Comm.*, 110th Cong. (2007) (statement of James B. Comey, Former Deputy Att'y Gen.), *available at* http://gulcfac.typepad.com/georgetown_university_law/files/comey.transcript.pdf (describing a standoff between Justice Department and White House lawyers regarding the legality of what is believed to be the TSP); Dan Eggen, *White House Secrecy on Wiretaps Described*, WASH. POST, Oct. 3, 2007, at A5 (quoting Jack Goldsmith as informing the Senate Judiciary Committee that he "could not find a legal basis for some aspects of the [warrantless surveillance] program").

238. *See* Lichtblau & Johnston, *supra* note 30.

239. *See supra* notes 30, 86, and 132 and accompanying text.

240. *See* Daryl J. Levinson & Richard H. Pildes, *Separation of Parties, Not Powers*, 119 HARV. L. REV. 2311, 2344-45 & n.147 (2006) (noting that "divided government was associated with greater congressional investigatory zeal"); *see also* Robert F. Blomquist, *Congressional Oversight of Counterterrorism and Its Reform*, 11 ROGER WILLIAMS U. L. REV. 1, 68 (2005); David Nather, *Congress as Watchdog: Asleep on the Job?*, CONG. Q. WKLY., May 22, 2004, at 1190; Yen, *supra* note 104 (describing the White House's designated oversight board as endorsing the position that the TSP does not require FISA authorization).

241. *See* Katyal, *supra* note 5, at 2342 (recommending that the minority party in each house be given the power to hold oversight hearings). *Cf.* ACKERMAN, *supra* note 101, at 85, 86, 103 (describing general and specific ways in which the minority party could be ensured better

hearings only, precisely because those venues do not provide opportunities for grandstanding among backbenchers, might be sufficiently modest to be palatable, and would work quite well for monitoring confidential intelligence programs.

In shifting the expectations and understanding away from an ex-ante-authorization-only model and toward a dynamic, disclosure model (wherein prior approval becomes just one part of the larger multi-branch dialogue), Congress's role is itself reformulated.[242] To borrow from the seminal McCubbins and Schwartz typology, Congress would be gravitating away from the "fire alarm" model of involvement and toward a "police sweep" paradigm.[243] Within the fire-alarm framework, which more accurately describes Congress's current posture vis-à-vis intelligence oversight, Congress passes legislation and then awaits word of trouble before re-entering the fray.[244] But, by operating akin to a sweep, Congress can maintain a constant state of vigil, in this instance through its active role in the ongoing dialogue with the intelligence agencies, participating corporations, and, as will be discussed below, the agencies' inspectors general.[245] As Jack Beermann has written, reporting requirements in general signal Congress's willingness to perform "police patrol type oversight," and to seek out "problems even in the absence of a pulled alarm."[246]

---

access to information and opportunities to weigh in on policy matters); Posner & Vermeule, *supra* note 215, at 887 & n.53 (discussing the significance of ensuring partisan minorities retain the power to monitor the Executive). Once passed, the measures of the sort described above would be particularly durable in the Senate, where subsequent rule changes would require a supermajority. *See* STANDING RULES OF THE SENATE, R. XXII (2007), *available at* http://rules.senate.gov/senaterules/.

242. *See* William G. Howell, *Political Checks on a Politicized Presidency: A Response to Neal Katyal's "Internal Separation of Powers,"* 116 YALE L.J. POCKET PART 111, 113 (2006), http://thepocketpart.org/2006/10/26/howell.html ("By holding hearings, launching investigations, advancing criticisms, and issuing public appeals for a change in course, members can materially raise the President's political costs of unilateral action, just as they make it more difficult for Presidents to credibly convey resolve to would-be allies and enemies alike.").

243. *See* Matthew D. McCubbins & Thomas Schwartz, *Congressional Oversight Overlooked: Police Patrols Versus Fire Alarms*, 28 AM. J. POL. SCI. 165 (1984); *see also* Kathleen Bawn, *Choosing Strategies To Control the Bureaucracy: Statutory Constraints, Oversight, and the Committee System*, 13 J.L. ECON. & ORG. 101, 103 (1997); Tara M. Sugiyama & Marisa Perry, Note, *The NSA Domestic Surveillance Program: An Analysis of Congressional Oversight During an Era of One-Party Rule*, 40 U. MICH. J.L. REFORM 149 (2006). Professors McCubbins and Schwartz emphasize that Congress is often aided by individual and interest group vigilance to supplement its oversight efforts. *See* McCubbins & Schwartz, *supra*, at 173. In this context, because the information about international partnerships ought not to be publicly disclosed, the burden falls on the corporations alone to advise Congress.

244. *See* Solove, *Reconstructing*, *supra* note 169, at 1295-96 (describing Congress's current approach of reacting to scandals).

245. *See* Jonathan G. Pray, Comment, *Congressional Reporting Requirements: Testing the Limits of the Oversight Power*, 76 COLO. L. REV. 297 (2005).

246. Jack M. Beermann, *Congressional Administration*, 43 SAN DIEGO L. REV. 61, 66-67 (2006). For this reason, assuming the reporting-to-Congress (via the FISA Court) process yields extensive inter-branch disclosures, there is also less of a need for Congress to rely on leaks and

Tangibly speaking, the institutional effect I am proposing shifts the default position from one of no disclosure (unless a report is leaked and then Congress marshals the political and legal will to insist that the Executive share information), to one of automatic disclosure. The current need to mobilize resources in order to "insist" each time a scandal occurs is very costly in terms of time (we know only after the story leaks), political capital, and scope (what if ten considerably more disconcerting operations are never leaked?). But under the framework I propose, it takes just one initial push, in the form of requiring corporate disclosures, to open that channel of information, ideally in perpetuity.

b. Inspector General Monitoring and Auditing

Despite its many powers to generate disclosures under this new framework, Congress may not always be up to the task of taking the lead vis-à-vis corrective interventions. Its oversight resources are limited,[247] its tools (notably, its purse power) may sometimes be too blunt,[248] and its political will may at critical times prove faint-hearted.[249] Moreover, although it is the case

---

newspaper exposés, both of which are important to a fire-alarm legislature that lacks first-hand information and a ready alternative means of getting it. Reliance on exposés are dangerous, first, because public reporting may generate an overexposure of the information, potentially indiscriminately compromising legitimate and extra-legal operations alike in ways that intra-governmental information sharing would not. *See* Byron Calame, Editorial, *Secrecy, Security, the President and the Press*, N.Y. TIMES, July 2, 2006, at D10 (arguing that the legality of the SWIFT program was the principal reason not to expose it in print). Second, to the extent that journalists may be particularly chilled from reporting on secret-intelligence initiatives, and perhaps not without justification given the recent spike in threats that they will face prosecution under the federal Espionage Act or be held in contempt of court, *see* Devlin Barrett, *Lawmaker Wants Times Prosecuted*, WASH. POST, June 26, 2006, at A2; Adam Liptak, *Gonzales Says Prosecutions of Journalists Are Possible*, N.Y. TIMES, May 22, 2006, at A14; *supra* note 173, the media may not be a particularly reliable source of information.

247. *See* Posner & Vermeule, *supra* note 215, at 888 (suggesting congressional monitoring is difficult as a matter of resources, "especially in domains of foreign policy and national security, where the scale of executive operations is orders of magnitude larger than the scale of congressional operations").

248. The purse power might also prove to be of limited utility insofar as the Executive could re-route defunded programs through other, untouched operations. *See, e.g.*, Shane Harris, *TIA Lives On*, NAT'L J., Feb. 23, 2006, *available at* http://nationaljournal.com/about/njweekly/stories/2006/0223nj1.htm ("A controversial counter-terrorism program [TIA], which lawmakers halted more than two years ago amid outcries from privacy advocates, was stopped in name only."); *Data Mining Project Goes On*, PITTSBURGH POST-GAZETTE, Feb. 23, 2004, at A-9 (noting that the TIA program was essentially transferred to non-de-funded offices). Moreover, anything approximating a complete funding cutoff might be too broad and crippling from a national-security perspective to be at all politically or logistically feasible.

249. *See, e.g.*, SCHWARZ & HUQ, *supra* note 35, at 125 ("Blame for these unwise [surveillance] policies does not lie entirely at the President's door. Congress too fell far short of its constitutional obligations."); Katyal, *supra* note 5, at 2316 ("[L]egislative abdication is the reigning modus operandi."); Koh, *Setting*, *supra* note 11, at 2359 ("In the five years since September 11, Congress has been remarkably pliant in refusing to stand up to the President's repeated assertions of unilateral power.").

that opportunities exist for Congress to intervene in a discreet manner, it is at the same time true that legislators have correspondingly less of an incentive to expend time and political capital on issues that do not generate splashy headlines that play well in their home districts.[250]

Thus, given the ways in which Congress may find itself constrained,[251] corporations should also be required to make additional disclosures to the inspectors general of the agencies requesting their assistance. The inspector-general disclosures would serve a similar purpose to those sent to Capitol Hill, but with the understanding that the quasi-independent actors within the Executive Branch have their own unique corrective tools to complement those of Congress.

The inspectors general would now have the opportunity to review overall patterns of intelligence operations almost in real time, with an eye toward detecting evidence of overreaching or abuse. They also would be in a position to see early on whether the corporations acted properly in the first instance, that is, in determining whether a partnership went forward without the necessary legal authorization.

Inspectors general are particularly well-suited for this task, as they have the resources, ostensible political independence from the departmental chain of command, and legislative charge to investigate agency wrongdoing.[252] For

250. *See, e.g.*, Posner & Vermeule, *supra* note 215, at 886 (suggesting that the collective-action problem in Congress with respect to monitoring executive discretion may make the legislature a less-than-ideal locus of effective oversight).

251. An obvious question is why would Congress have the will and fortitude to legislate a more comprehensive framework of reforms when, for the reasons acknowledged, it is quite possible that it could not successfully mount a more direct challenge to Executive overreaching. Neal Katyal provides at least one reason—that the breadth of such institutional reform itself may pose challenges for special interest groups that oppose the measure but find it difficult to assess the impact amid multiple benefits and losses. *See* Katyal, *supra* note 5, at 2323. I would add here that Congress has familiarity with indirect institutional legislating, particularly in instances where the political difficulties of addressing the policy directly would prove insurmountable. *See, e.g.*, National Defense Authorization Act for Fiscal Year 1991, Pub. L. No. 101-510, §§ 2902-2903, 104 Stat. 1485, 1808-12 (1990) (codified as amended at 10 U.S.C. § 2687 note (2000)); Mark Seidenfeld, *A Civic Republican Justification for the Bureaucratic State*, 105 HARV. L. REV. 1511, 1542 (1992) (noting that "Congress was unable to close any, or even set the criteria for deciding which bases should be closed," but was able to pass legislation directing an independent commission to do so).

252. *See* Inspector General Act of 1978, Pub. L. No. 95-452, 92 Stat. 1101 (codified in scattered sections of 5 U.S.C.); *see generally* GOLDSMITH, *supra* note 7, at 93-94 (suggesting inspectors general in the Bush Administration took their charges seriously, indeed sometimes acting too aggressively); PAUL C. LIGHT, MONITORING GOVERNMENT: INSPECTORS GENERAL AND THE SEARCH FOR ACCOUNTABILITY (1993); Isaacharoff & Pildes, *supra* note 13 (emphasizing the significant role inspectors general have played in checking the Executive in post-September 11 national-security matters). It is, of course, incumbent on the Senate to vet the President's appointees for positions as inspectors general and to seek from them assurances of independence and vigilance. *See, e.g.*, David Stout, *Democrat Opens Inquiry into Whether State Dept. Official Impeded Investigations*, N.Y. TIMES, Sept. 19, 2007, at A10.

example, pursuant to a congressional directive,[253] the Inspector General for the Justice Department recently published eye-opening reports on systematic abuses by the FBI in issuing NSLs and collecting information without proper legal bases.[254] As part of a separate inquiry, the Inspector General released a report detailing the FBI's mishandling of the investigation of an American suspected of being involved in the Madrid terrorist bombing in 2004.[255] Similarly, the Inspector General of the Department of Homeland Security worked with various offices within the agency to scrap an overreaching data-mining project, which evidently had been operating outside of the departmentally prescribed privacy safeguards.[256]

With regard to this reporting prong of the proposal, the objective would be that the inspectors general can act quickly to counsel intelligence agents (and their principals) to revise their approaches, thus staving off the necessity of issuing a public critique, which might then motivate Congress to pass legislation that ultimately and significantly binds the intelligence agencies' hands.[257]

c. Generating Greater Executive-Congressional Dialogue Through Corporate "Adversity"

The fact that the corporations will be submitting reports and will be obligated to insist on being served with the proper instruments of legal compulsion provides strong incentives for the Executive to take the appropriate steps to obtain whatever ex ante authorization is required before it proceeds with a foreign-surveillance operation. After all, under this new regime, the intelligence agencies will have every reason to believe that the corporations will take their legal obligations seriously.[258]

---

253. *See* USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, § 119, 120 Stat. 192, 219-21 (2006).

254. *See* OFFICE OF THE INSPECTOR GEN., U.S. DEP'T OF JUSTICE, A REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION'S USE OF NATIONAL SECURITY LETTERS (2007), *available at* http://www.usdoj.gov/oig/special/s0703b/final.pdf; 2008 OIG REPORT ON NSL AUTHORITY, *supra* note 131.

255. *See* OFFICE OF THE INSPECTOR GEN., U.S. DEP'T OF JUSTICE, A REVIEW OF THE FBI'S HANDLING OF THE BRANDON MAYFIELD CASE (2006), *available at* http://www.usdoj.gov/oig/special/s0601/final.pdf.

256. *See* Sniffen, *supra* note 86.

257. *See supra* note 136 and accompanying text.

258. *See supra* note 86. So long as the Executive is reasonably sure that the corporations will issue reports, it too will feel compelled to "talk," and to talk as descriptively as possible to assure Congress that the operation is subject to careful intelligence oversight. *See infra* notes 263-264 and accompanying text.

That impulse also works between and among corporations within an industry. If, say, Verizon and Bell South provide the same telecommunications service to adjacent parts of the country and both are assisting the NSA, each will feel particularly acute pressure to disclose information about its intelligence partnerships. This is so because Verizon knows that if Bell South were to report on its own relationship with the government, invariably oversight agents would assume that the intelligence agencies also struck a similar deal with Verizon and any other non-disclosing,

Moreover, to the extent the new burdens on industry make corporations balk at the idea of agreeing to informal collaboration[259] (particularly in those operations, such as the NSA Call-Data Program, that involve activities that fall within a gap in the legal framework), such a standoff would simply force intelligence agents currently lacking the power to compel cooperation to go to Congress and request formal authorization. The Bush Administration has successfully done so already on a number of occasions.[260] Whatever modest cost is incurred in terms of a time lag (and it typically has been very modest)[261] is more than offset by the greater legal clarity that congressional authorization will ultimately provide.[262]

Finally, when informal, but not unlawful, collaborations do commence, the Executive now has incentives to establish operating guidelines that convey to oversight agents not only a recognition of the potential dangers that might worry Congress or an inspector general, but also specifically show how those dangers will be mitigated through internal constraints. That is, the Executive can and should "signal," to use Eric Posner and Adrian Vermeule's term, that it is a well-motivated, good-faith actor and thus take pains to reassure government monitors rather than alarm them.[263]

For example, the promulgation of clear minimization procedures, such that information obtained from a corporation would not be used for ordinary law-enforcement purposes, or the implementation of some privacy safeguards overseen by otherwise walled-off officials each would provide a low-cost means of "demonstrating credibility," such that the oversight agents would be

---

similarly situated parties. For the oversight agents to go only to Bell South, would leave a hole in the surveillance web. Thus, the external pressure that some rival entity *is* complying with Congress's reporting requirement provides a greater incentive for overall cooperation. In this way, the mechanism proposed herein is more robust than, say, the Bank Secrecy Act, *see supra* note 224, because in that context there is no underlying expectation by government officials that all banks would be simultaneously besieged by money launderers.

259. As I will explain immediately below, there will be new safe-harbor immunity incentives for the corporations to embrace this new formality, as an alternative both to succumbing to informal collaboration *and* to refusing the government's request of assistance.

260. *See, e.g.*, Protect America Act of 2007, Pub. L. No. 110-55, 121 Stat. 552; *see also* Joby Warrick & Walter Pincus, *How the Fight for Vast New Spying Powers Was Won*, WASH. POST, Aug. 12, 2007, at A1. *See generally* GOLDSMITH, *supra* note 7, at 136-40 (noting the ease with which the Bush Administration has been unfailingly successful in securing congressional support for its national-security objectives).

261. Modest is the operative word, as Congress has been quick to ratify presidential requests for counterterrorism authority since September 11, 2001. *See, e.g.*, Jim McGee, *An Intelligence Giant in the Making*, WASH. POST, Nov. 4, 2001, at A4 (describing the USA PATRIOT Act of 2001 as having been passed with "furious haste"); Risen, *supra* note 198 (describing how the Protect America Act "was rushed through both the House and Senate in the last days before the August recess began").

262. Left unstated is what to do about the so-called fourth-party data brokers. The challenges they present, however, seemingly call for a different type of reform, more substantive than procedural insofar as the goal would be to define and limit the terms under which private information can be transferred.

263. *See* Posner & Vermeule, *supra* note 215, at 894-95.

less apt to intervene and regulate in a heavy-handed manner.[264]

3. Immunity as an Incentive To Encourage Corporations To Opt In

The penalties for corporations that fail to insist on being legally compelled or that fail to make the required disclosures should be criminal or civil liability for the designated executives in charge;[265] in addition, the firms should also be subject to administrative sanction, including government-contract debarment.

As for positive incentives, the guarantee of full immunity from civil suit should induce corporations both to cooperate with the Executive and to comply with Congress's gatekeeping and reporting requirements. This immunity should, however, be commensurate with the scope of the disclosure, meaning that only those information-gathering processes documented in the disclosure reports will be protected from private lawsuits alleging, for example, breach of contract with consumers or breach of fiduciary duties.[266] This limiting condition gives the corporations every reason to be comprehensive and every reason to submit updates if and when partnerships start expanding or drifting.[267]

In effect, the quid pro quo of immunity for gatekeeping and disclosure not only makes sense from the perspective of encouraging potentially worthwhile partnerships, but also from the perspective of effectively extending, by statute,

---

264. *Id.* at 898-99; *see also id.* at 910-13 (discussing costs of signaling). Posner and Vermeule suggest that those "who implicitly distrust" the Executive might well not believe that an ill-motivated Executive would engage in such signaling. *Id.* at 898. Assume, for argument's sake, that I share that implicit distrust; I would nevertheless take the view that I could be convinced by an Executive willing to be demonstrative in its signaling. Moreover, the Executive would have reasons for wanting to be demonstrative, willingly ceding some discretion in the hope that Congress would be satisfied and lose its taste for more intrusive intervention. *See id.* at 911 ("[T]o gain credibility, presidents must surrender part of their control over policy choices, partially constraining executive discretion in the present in return for more trust, *which will then translate into more discretion in the future.*") (emphasis added).

265. *Cf.* Lobbying Disclosure Act of 1995, Pub. L. No. 104-65, § 7, 109 Stat. 691, 699 (codified at 2 U.S.C. § 1606) (establishing civil penalties for failures to make proper representations of lobbying activities); Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, § 906, 116 Stat. 745, 806 (codified at 18 U.S.C. § 1350) (penalizing knowing misrepresentations).

266. An apt example of a regulation that provides immunity in exchange for corporate-disclosure reports is the Critical Infrastructure Information Act of 2002 (CIIA), 6 U.S.C. §§ 131-34, part of the Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135. The CIIA immunizes corporations from civil liability for weaknesses in their infrastructure, provided those weaknesses are first disclosed to the government. *See* 6 U.S.C. § 133(a)(1). Note that immunity for good-faith reliance on court orders also exists under the Electronic Communications Privacy Act. *See* 18 U.S.C. § 2707(e) (2002).

267. The type of demands placed on the intelligence agencies may seem extensive, but, in truth, the compliance structure proposed herein draws from an array of existing and ostensibly well-functioning statutory measures that are in place in a variety of settings within and outside the national-security context. For examples within the national-security realm, see 1 U.S.C. § 112b (2004), the Arms Export Control Act, 22 U.S.C. § 2751 (2008), and 6 U.S.C. § 133 (2004). Moreover, among the Improving America's Security Act of 2007, the USA PATRIOT Improvement and Reauthorization Act of 2005, and the Intelligence Reform and Terrorism Prevention Act of 2004 alone, there are approximately twenty-eight different reporting-to-Congress requirements.

the benefits of qualified immunity[268] to the private actors insofar as they are collaborating on entirely public, and highly sensitive, matters. Generally speaking, qualified immunity cloaks state actors such as police officers, but not, say, private bounty hunters; unlike the police, bounty hunters lack reciprocal responsibilities to, and are not under the control of, the state.[269] For the recipients of immunity, the reciprocity comes by way of faithful adherence to the public-law-reinforcing gatekeeping and disclosure imperatives.

Punishing the non-compliant corporations does pose some difficulties, as there may be instances in which the Justice Department is less than enthusiastic about bringing charges against corporations that are "too cooperative" with intelligence operations. It is also particularly likely that the Executive would try to quash private suits on state secrets grounds, or limit disclosures on executive privilege grounds.[270] Thus, a private right of action ought to be created that allows "affected U.S. persons" to bring suits against corporations, both for

268. *See generally* Harlow v. Fitzgerald, 457 U.S. 800, 807-12 (1982) (describing justifications for qualified immunity); Gillian E. Metzger, *Privatization as Delegation*, 103 COLUM. L. REV. 1367 (2003) (discussing the possibility of extending state-action doctrine to private agents acting in public capacities). Given the largely, if not entirely, public function of these collaborations (distinct from corporations' normal dealings with and for the government), one might find occasion to recall nineteenth century understandings of corporations as public entities restrained by various mechanisms of public accountability. *See, e.g.*, Kent Greenfield, *Ultra Vires Lives! A Stakeholder Analysis of Corporate Illegality (with Notes on How Corporate Law Could Reinforce International Law Norms)*, 87 VA. L. REV. 1279, 1303-04 (2001) ("The ultra vires doctrine also embodied the notion that the corporation was a creature of the state. The nineteenth century conception of the firm, as a historical matter, included a much stronger nod toward the public purpose of the firm than does the modern view. Moreover, at least until the late nineteenth century the corporation was considered a public entity, in that it arose from a concession by the state. As Woodrow Wilson urged in his inaugural address as Governor of New Jersey, '(a) corporation exists, not of natural right, but only by license of law, and the law, if we look at the matter in good conscience, is responsible for what it creates.' The ultra vires doctrine gave force to these notions in that it established the corporation as a legal entity of enumerated powers, beyond which the firm could not go.") (internal citation omitted). I thank Bob Hockett for suggesting this connection.

269. *See, e.g.*, Brentwood Acad. v. Tenn. Secondary Sch. Athletic Ass'n, 531 U.S. 288, 296-302 (2001) (conditioning state-actor status on whether private actors are sufficiently under public control); Richardson v. McKnight, 521 U.S. 399, 413 (1997) (denying qualified immunity to private prison guards not closely supervised by public officials, but reserving judgment on whether qualified immunity would attach were a private actor "serving as an adjunct to government in an essential governmental activity, or acting under close official supervision").

270. *See supra* note 173 and accompanying text. *See generally* Akhil Reed Amar & Neal Kumar Katyal, *Executive Privileges and Immunities: The* Nixon *and* Clinton *Cases*, 108 HARV. L. REV. 701 (1995); Eric A. Posner & Adrian Vermeule, *Constitutional Showdowns* (John M. Olin Law & Econ. Working Paper No. 348 (2d series), Pub. Law and Legal Theory Working Paper No. 173, 2007); *see also* United States v. Reynolds, 345 U.S. 1 (1953) (invoking state secrets doctrine to dismiss claim); Totten v. United States, 92 U.S. 105 (1876) (same); El-Masri v. Tenet, 437 F. Supp. 2d 530 (E.D. Va. 2006) (same). *Cf.* Pamela Hess, *Telecoms Barred From Disclosing Spying*, ABCNEWS.COM, Oct. 15, 2007, http://abcnews.go.com/Politics/wireStory?id=3733087 (noting that the telecommunications companies declined to provide details to Congress regarding domestic intelligence collaborations on the basis of National Intelligence Director McConnell having "formally invoked the state secrets privilege").

statutory violations and for (un-immunized) tort or contractual claims, and concurrent trial-court jurisdiction should be given to the FISA Court (which could deliberate more secretively and thus blunt the salience of state secrets protests).[271]

4. Reviewing: Requiring Closer Scrutiny by the FISA Court

In addition, while leaving the current patchwork of ex ante authorization requirements undisturbed,[272] opportunities for ongoing review to, among other

---

271. *See, e.g.*, FISA Amendments Act of 2008, H.R. 3773, 110th Cong. (2008) (mitigating the effectiveness of a state secrets claim in civil litigation against corporations involved in intelligence operations by allowing evidentiary hearings to proceed ex parte and *in camera*); *see also supra* note 115 and accompanying text. *But see* The Foreign Surveillance Act of 1978 Amendments Act of 2008, Pub. L. No. 110-261, 122. Stat. 2436.

The Stored Communications Act ("SCA"), 18 U.S.C. §§ 2701-11 (2006), part of the Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848, shows both the strengths and weaknesses of a proposal that pivots on corporate compliance. Among other things, the SCA insists that certain types of information, seemingly including the "call data" that the telecommunications firms voluntarily turned over to the NSA, cannot be released by providers of electronic communications services, 18 U.S.C. § 2510(15) (2002), so long as those providers offer services to the "public," 18 U.S.C. § 2702(a), unless the government compels cooperation by force of legal process or some other exception, such as express customer consent or exigent circumstances, applies. *See* 18 U.S.C. §§ 2702-03; Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1213, 1221-22 (2004) [hereinafter Kerr, *User's Guide*]. Given the statute's requirement that certain classes of providers may not voluntarily give information to the government and the considerable financial liability the corporations face if caught voluntarily turning it over, see 18 U.S.C. § 2707 (2002), one might conclude that the system I propose already exists—and just does not work well.

Yet I believe the opposite is true. First, the NSA Call-Data scandal served as a wakeup call. No comparably high-profile, high-stakes private suit had previously been brought under the SCA; now that companies better appreciate their exposure, *see supra* note 48, a compliance regime built around such corporate responsibilities (with fuller coverage and with the added sticks of criminal sanctions) might follow nicely on the heels of the corporations' sudden awareness of the costs of informality. Second, drawing too close of an analogy between the SCA's provisions and my stylized proposals does not take adequate account of the differences between the two regimes. For starters, the SCA apparatus, like current intelligence law writ large, contains many loopholes and coverage gaps, a fact that ought to make the type of all-encompassing procedural requirements I am proposing particularly welcome. *See* Kerr, *Lifting*, *supra* note 107, at 820; Kerr, *User's Guide*, *supra*, at 1214, 1230-31; Solove, *Reconstructing*, *supra* note 169, at 1292 (discussing loopholes, gaps, and complexities associated with the Electronic Communications Privacy Act). Indeed, given the loopholes and exceptions, it is at least debatable whether the telecommunications companies ever really violated the SCA in turning over call-data. *See* Posting of Marty Lederman, Further Thoughts on the Lawfulness of the Newly Disclosed NSA Program, to Balkinization, http://balkin.blogspot.com/2006/05/further-thoughts-on-lawfulness-of.html (May 11, 2006, 22:08 EST).

Moreover, even when it is clear that the communications providers *are* regulated under the SCA and *no exception* applies, the firms can give non-content information (such as call data) to unregulated non-governmental actors, including fourth parties such as LexisNexis or ChoicePoint. 18 U.S.C. § 2702(c)(6) (2006); *see also* Kerr, *User's Guide*, *supra*, at 1223. In turn, those actors could then readily share the intelligence with the government with impunity. *See id.* at 1220 (characterizing 18 U.S.C. § 2702(c)(6)).

272. *See supra* note 210.

things, provide mechanisms for distinguishing the worthwhile projects from the materially questionable or legally dubious ones[273] should also be given to FISA Court judges. As such, all foreign-intelligence operations in which U.S. persons are targeted (or significantly investigated, albeit indirectly),[274] whether or not those operations require ex ante authorization from the FISA Court, would be subject to review and re-authorization every ninety days. This means that programs (1) that are not even regulated under the current framework, or (2) that carry the force of law by virtue of an administrative subpoena, or (3) that, from the outset, require the blessing of an independent magistrate, *all* must subsequently be sent to the FISA Court for quarterly approval.[275]

The standards for review and re-authorization will be pegged to the ex ante framework. Thus, an operation that did not require any prior approval will not be forced to overcome the same probative hurdles every ninety days as a program that had to be cleared from the outset by the FISA Court. But whatever the standards are for keeping a given program operational, they will be correspondingly greater than those that were required to commence that program.[276] Thus, there will be a built-in "escalator," that is, an expectation that the operations can be more definitively shown to be of continuing usefulness or else be subject to termination.[277]

At the review and re-authorization stage, the FISA Court must evaluate briefings on the evidentiary support justifying the program, the utility of the information obtained as weighed against the invasiveness of the inquiries, and the potential for false positive identifications (and the harms that those false positives spawn). As it already does, the FISA Court can approve or reject the program or ask for modifications.[278] Again, most of the covered programs will

273. *See* Solove, *Data Mining*, *supra* note 184, at 352-53 (noting the difficulties associated with gauging whether data-mining projects have been successful); Schwartz, *Reviving*, *supra* note 86 (claiming that it is difficult to evaluate the success of surveillance operations under existing disclosure standards).

274. For a helpful definition of foreign-intelligence operations, see MASSE, *supra* note 2, at 12-15.

275. As noted, FISA court orders already require periodic reauthorization. *See* 50 U.S.C. § 1805(e) (2006).

276. *Cf.* ACKERMAN, *supra* note 101, at 4, 80 (proposing a supermajority "escalator" to require greater congressional support for reauthorizing executive emergency powers as time passes). The connection to Professor Ackerman's proposal is that, like in the combat context, the longer intelligence programs remain in operation the more demanding Congress should be in insisting that those programs are still worthwhile.

277. In many instances, it is difficult to prove whether counter-terrorism measures work. *See generally* POSNER, PREVENTING, *supra* note 2. If a country builds a wall around its borders, and afterward, there are no terrorists who try to sneak into the country, showing how many would-be attackers were deterred is a difficult feat. If, however, a country undertakes a secretive initiative, such as one of the surveillance measures discussed in this Article, there should be no intended or realized deterrent effect. Thus, if eavesdropping on telephone calls reveals no instances of terrorist chatter, then the intrusiveness of wiretapping may be shown to outweigh the utility of the operation.

278. Modifications to applications for surveillance operations are already made at the

not raise serious concerns and will be approved as a matter of course. Regardless of the outcome, and in the interest of ensuring inter-branch dialogue, the briefing papers and a copy of the FISA Court's transcript should be delivered under seal to the congressional oversight committees and to the relevant inspector general.

CONCLUSION

Whatever policy and legal decisions are made in the coming years vis-à-vis striking the proper balance between security and privacy interests, it is essential that they are informed ones. This Article has endeavored to take important steps to ensure greater understanding of the underlying mechanics of intelligence gathering, of the incentives that shape vital private-public partnership arrangements, and of the current misallocation of compliance and oversight responsibilities.

Of course, having private actors serve as government watchdogs in the face of Executive non-compliance is not the most normatively attractive model of separation of powers, and it may even be seen as excusing (or creating a basis for normalizing) bad behavior by the Executive. I acknowledge these shortcomings, with the qualifiers, however, that true reform of the sort that is necessary in terms of better allocating war-making and intelligence powers is not likely to occur until after the terrorism crisis abates (and there are opportunities for self-reflection).[279] In addition, because private actors are often asked or required to serve similar enforcement roles across a wide range of policy domains,[280] the use of corporate intermediaries is not necessarily a bad, or wholly untested, solution.

Moreover, notwithstanding the instrumental focus of my project, neither the enterprise of increasing formality (gatekeeping-reporting-reviewing) nor the consideration of private actors as the conduits of compliance is divorced from normative aspirations. As noted earlier, engendering dynamic interactions among a variety of responsible government actors—at varying degrees of distance from the immediacy of combating terrorism—is an important foundational step in ensuring the prospects of effective legislative, oversight,

---

request of the FISA Court. *See* Electronic Privacy Information Center, Foreign Intelligence Surveillance Act Orders 1979-2006, http://www.epic.org/privacy/wiretap/stats/fisa_stats.html (last visited Feb. 19, 2008).

279. *See, e.g.*, Harold Hongju Koh, *A Law unto Itself?*, 115 YALE L.J. POCKET PART 79, 83 (2006), http://www.thepocketpart.org/2006/03/a_law_unto_itself.html ("After Vietnam and Watergate, Congress wisely seized th[e] opportunity when it passed framework legislation such as FISA."); Solove, *Reconstructing*, *supra* note 169, at 1276 (noting that congressional investigatory committees were "[s]purred by the Watergate scandal"); Swire, *System*, *supra* note 3, at 1341 (suggesting that FISA's passage was prompted in part by the Watergate scandal).

280. *See supra* notes 223-225; *see also* Arms Export Control Act, 22 U.S.C. §§ 2751-99 (2008); Critical Infrastructure Information Act of 2002, 6 U.S.C. §§ 131-34; Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (1994) (requiring telecommunications providers to ensure that law enforcement can access their technologies).

and appropriations decisions (and for unambiguously undercutting the prospects of future corporate acceptance of informality). Indeed, it also may serve as a model for creating additional opportunities for legislative oversight even in more formalized government contracting settings, particularly where monitoring is difficult and there is dissensus between the legislature and the Executive on the direction of a given outsourced initiative.

Looking forward, it should be recognized that the reforms mentioned herein do not just service the instant accountability deficit. Rather, they also provide a platform for addressing some of the most pressing and novel questions of our times, including privatization in intelligence and national-security operations, separation of powers in policy domains dominated by the discourse of secrecy and unitary-executive governance, and the prospects and pitfalls of a more involved national-security court, with jurisdiction and responsibilities beyond vetting applications for surveillance missions. Thus, this Article has sought not only to provide practical insights into the current problems with unchecked intelligence operations, but also to spark thinking about how we manage a counterterrorism policy that is outgrowing the traditional, binary boundaries of foreign versus domestic investigations, private versus public governance, transparent versus secretive policymaking, and "ordinary criminal" versus "national security" prosecutions.