UCLA
UCLA Public Law & Legal Theory Series

Title
Deputizing Homeland Security

Permalink
https://escholarship.org/uc/item/8ms120ps

Journal
Texas Law Review, Vol. 88, p. 1435, 2010

Author
Michaels, Jon

Publication Date
2010-10-01

eScholarship.org Powered by the California Digital Library
University of California

Deputizing Homeland Security

Jon D. Michaels*

Introduction

In the wake of the attacks of September 11, 2001, private actors have come to occupy a remarkably prominent place in efforts to identify and counter threats of domestic terrorism. Today, seemingly no transaction, whether social, political, or economic, is comfortably beyond eye or earshot of the newly deputized national security apparatchiks. Corporations representing all of the major retail and service industries—including telecommunications, finance, and commercial travel—are routinely turning over reams of information to the government.[1] And, it's not just corporate data dumps; it's also doormen,[2] pilots,[3] truck drivers,[4] retail clerks,[5]

---

* Acting Professor of Law, UCLA School of Law. The author thanks Frederic Bloom, Toni Michaels, Paul Schwartz, David Super, Jonathan Zasloff, and Noah Zatz for their helpful comments. Further thanks are owed to his fellow Symposium participants, to Laura Podolsky, Ira Steinberg, and the UCLA Law Library for invaluable research assistance, to the staff of the Texas Law Review, and to Bobby Chesney for his leadership as Symposium organizer and host.

1. *See, e.g.*, Chris Jay Hoofnagle, *Big Brother's Little Helpers: How Choicepoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement*, 29 N.C. J. INT'L L. & COM. REG. 595, 621 (2004) (noting increased government outreach to corporations for customer information); JAY STANLEY, THE SURVEILLANCE-INDUSTRIAL COMPLEX 10–11 (2004), http://aclu.org/files/FilesPDFs/surveillance_report.pdf (providing examples of corporations sharing data with the government); *see also* Leslie Cauley & John Diamond, *Telecoms Let NSA Spy on Calls*, USA TODAY, Feb. 6, 2006, at A1 (reporting on telecom companies' role in facilitating government wiretapping of international communications without warrants or court orders); Mark Glassman, *4 More Airlines Named in Release of Data*, N.Y. TIMES, June 24, 2004, at A17 (describing the practice among airlines of turning over passenger information to government contractors); Philip Shenon, *Airline Gave Defense Firm Passenger Files*, N.Y. TIMES, Sept. 20, 2003, at A1 (reporting that JetBlue voluntarily gave the Defense Department information on more than one million of its customers); Mike Snider, *Privacy Advocates Fear Trade-off for Security*, USA TODAY, Sept. 13, 2001, at D8 (describing Internet service providers' cooperation with federal authorities); Becky Yerak, *"Suspicious Activity" Reports Soar from Banks, Other Depositories*, CHI. TRIB., Nov. 23, 2007, at B3 (reporting on commercial institutions' increased filing of "suspicious activity reports" to the U.S. government); Josh Meyer & Greg Miller, *U.S. Secretly Tracks Global Bank Data*, L.A. TIMES, June 23, 2006, at A1 (detailing financial institutions' cooperation with the government in efforts to detect terrorist financing patterns). When referring to the *government* in this Article, typically it is to the federal government. At times, however, the term *government* refers to state or local authorities, or some combination of "state actors" at the local, state, and federal level.

2. *See* Stevenson Swanson, *Truckers, Doormen Vigilant for Threats*, CHI. TRIB., Aug. 2, 2005, at C11 (reporting that thousands of doormen at residential buildings nationwide have received training to detect terrorist threats and encouragement to alert the authorities if they observe suspicious activity).

3. *See* Ricardo Alonso-Zaldivar, *Pilots Asked To Be Vigilant*, L.A. TIMES, Mar. 4, 2003, at A14 (noting the collaboration between the Transportation Safety Administration and the 500,000-member Aircraft Owners and Pilots Association to detect and report perceived security threats).

repairmen,[6] and parcel couriers,[7] who have been enlisted by the government, their employers, and even their own unions to detect and report suspicious activities on the ground. Finally, there is the role being played by ordinary folks, who have been bombarded with calls from government officials to do their part to keep America secure.[8]

Four factors help explain this dramatic rise in citizen and corporate participation: first, a post-9/11 demand for greater surveillance and

---

4. OFFICE OF INSPECTOR GEN., DEP'T OF HOMELAND SEC., EFFECTIVENESS OF THE FEDERAL TRUCKING INDUSTRY SECURITY GRANT PROGRAM 1 (2008), http://www.dhs.gov/xoig/assets/mgmtrpts/OIG_08-100_Sep08.pdf; *see also* Amanda Ripley, *Eyes and Ears of the Nation*, TIME, June 27, 2004, at 38 (describing the private–public Highway Watch program involving truck drivers in counterterrorism surveillance).

5. *See, e.g.*, Josh Meyer, *As Terrorism Plots Evolve, FBI Relies on Agent John Q. Public*, L.A. TIMES, May 12, 2007, at A1 (describing how the Fort Dix terrorist plot was foiled in part by a Circuit City employee alerting the authorities to suspicious materials on a laptop he was servicing).

6. *See* Larry Atkins, *Beware of Cable Guys Snooping Around the Neighborhood*, CHI. TRIB., July 23, 2002, at N19 (describing the practice of repairmen being enlisted to assist the authorities in reporting on suspicious activities in their customers' homes); Stephanie Erickson, *"Bright Eyes" Keeping Watch in 7 Counties*, ORLANDO SENTINEL, July 21, 2005, at H1 (noting that Bright House technicians "are hooking up cable television lines and checking Internet connections on the fritz—all while keeping an eye out for terrorism"); Stacy Humes-Schulz, *Alarm Bells Ring Over Terrorism Reporting System*, FIN. TIMES, July 23, 2002, at 6 (reporting on the role repairmen and other service technicians, who do their work in clients' homes, would play in the Justice Department's Operation TIPS).

7. *See* Robert Block, *Private Eyes: In Terrorism Fight, Government Finds a Surprising Ally: FedEx*, WALL ST. J., May 26, 2005, at A1 (detailing FedEx's post-9/11 assistance in counterterrorism efforts).

8. *See* Associated Press, *Excerpts from Bush's Briefing*, CHI. TRIB., Oct. 12, 2001, at I18 ("The American people, obviously if they see something out of the norm that looks suspicious, they ought to notify local law authorities . . . ."); Michael Cabanatuan, *BART Riders Will Be Asked To Stay Alert*, S.F. CHRON., Aug. 30, 2002, at A24 (noting that mass transit users are encouraged to report suspicious activities); John J. Goldman, *Workers Get Anti-terror Lessons*, L.A. TIMES, May 27, 2004, at A26 (noting that the Attorney General and the FBI Director "called on the nation . . . to help find seven suspected al Qaeda operatives and to head off a possible attack in the U.S."); *Passengers Asked To Help Keep Transit Safe*, USA TODAY, July 8, 2005, at A5 (reporting on government efforts to urge public transit users to advise the police if they see suspicious activities or items); *Transcript of News Conference by Ashcroft and Ridge on Increased Alert*, N.Y. TIMES, Sept. 11, 2002, at A12 (encouraging citizens to report suspicious activity).

It is, to be sure, these ordinary folks who have been asked to be vigilant in their neighborhoods and who have also—now on several commercial flights—been the only ones standing between us and, perhaps, a handful of 9/11-like recurrences. *See* Brian Harmon et al., *Jet Passengers Foil Shoe-Bomb Suspect*, N.Y. DAILY NEWS, Dec. 23, 2001, at 3; Charles Lane et al., *A Sky Filled With Chaos, Uncertainty and True Heroism*, WASH. POST, Sept. 17, 2001, at A3; Scott Shane & Eric Lipton, *Passengers' Actions Thwart a Plan To Down a Jet*, N.Y. TIMES, Dec. 27, 2009, at A1. *See generally* David Brooks, Op-Ed. Column, *The God that Fails*, N.Y. TIMES, Jan. 1, 2010, at A29.

Brooks, writing in the immediate aftermath of a thwarted attempt to ignite a bomb on a Detroit-bound flight, notes:

> At some point, it's worth pointing out that it wasn't the centralized system that stopped terrorism in this instance. As with the shoe bomber, as with the [United 93] plane that went down in Shanksville, Pa., it was decentralized citizen action. The plot was foiled by nonexpert civilians who had the advantage of the concrete information right in front of them—and the spirit to take the initiative.

Id.

intelligence-gathering capacity;[9] second, a growing comfort with private actors handling sensitive national security tasks;[10] third, a recognition that much of the desired information is easier for private actors to access or acquire in the first place;[11] and, fourth, widespread interest on the part of a patriotic, frustrated public to help.[12]

Enter our new cadre of private snoops, data crunchers, and (yes) vigilantes. This assortment of "deputies," some trained and ostensibly commissioned,[13] some solicited as part of a general, mass invitation,[14] and some merely self-declared and possibly unwelcomed,[15] have expanded

---

9. *See* NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., THE 9/11 COMMISSION REPORT, at xv–xvi, 339 (2004) [hereinafter 9/11 COMMISSION REPORT] (describing the need to devote greater resources to intelligence gathering); Anne Joseph O'Connell, *The Architecture of Smart Intelligence: Structuring and Overseeing Agencies in the Post 9/11 World*, 94 CAL. L. REV. 1655, 1655 (2006) (stating that the attacks of September 11 "resulted, at least in part, from a massive breakdown in the intelligence system designed to identify threats to the nation's security and to provide policymakers with sufficient information to protect against them"); Jon D. Michaels, *All the President's Spies: Private–Public Intelligence Partnerships in the War on Terror*, 96 CAL. L. REV. 901, 901–02 (2008) (describing the need for greater intelligence-gathering capacities).

10. *See, e.g.*, Jon D. Michaels, *Beyond Accountability: The Constitutional, Democratic, and Strategic Problems with Privatizing War*, 82 WASH. U. L.Q. 1001 (2004) (describing private military firms' responsibilities in supplementing, complementing, and, at times, standing in for U.S. military personnel in zones of armed engagement); Martha Minow, *Outsourcing Power: How Privatizing Military Efforts Challenges Accountability, Professionalism, and Democracy*, 46 B.C. L. REV. 989, 992–93 (2005) (discussing private contractors' involvement in U.S. military engagements, surveillance programs, and military-detention operations); PAUL R. VERKUIL, OUTSOURCING SOVEREIGNTY 23–42 (2007) (describing private-sector involvement in a range of national security domains); James Risen & Mark Mazzetti, *Blackwater Guards Tied to Secret Raids by C.I.A.*, N.Y. TIMES, Dec. 11, 2009, at A1 (reporting on the role private security guards played in CIA operations in Iraq and Afghanistan).

11. *See* Michaels, *supra* note 9 at 902 (indicating that the private sector's "comparative advantage over the government in [data gathering] is a function both of industry's unparalleled access to the American public's intimate affairs . . . and of regulatory asymmetries" that at times enable private organizations to "obtain and share information more easily and under fewer legal restrictions than the government can"). For background on data gathering and analysis, see DANIEL J. SOLOVE, DIGITAL PERSON (2004); *see also infra* notes 26 and 70. As Solove notes,

> 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.

SOLOVE, *supra*, at 166.

12. *See infra* note 37 and accompanying text.

13. *See, e.g.*, OFFICE OF INSPECTOR GEN., *supra* note 4, at 1 (noting that the Highway Watch program trains and certifies truck drivers to assist in counterterrorism surveillance).

14. *See* Andy Newman, *Citizen Snoops Wanted (Call Toll-Free)*, N.Y. TIMES, July 21, 2002, at D1; Eileen Sullivan & P. Solomon Banda, *Anti-terror Citizens Watch Endorsed by Police Chiefs*, STAR-LEDGER (Newark, N.J.), Oct. 4, 2009, at 11.

15. For example, the private, border-patrol "militias" might fall into this category of self-appointed deputies, as might the so-called private Internet vigilantes who monitor and seek to disable Jihadist Web sites and chat rooms. For further discussion of these groups, *see infra* notes 124–25.

homeland security coverage in profound ways.[16] Deputies are force multipliers; as a matter of sheer numbers, a mobilized, vigilant public can reach more broadly than the government, on its own, can. The public does so simply by going about its routine social, civic, and commercial activities in a more mindful manner. Additionally, deputies may have superior physical and electronic access to private spaces and stores of data than government agents have on their own—a function both of there sometimes being greater legal constraints imposed on government agents than on private actors[17] and of the greater caution and reserve people typically exercise when they are interacting with the government, as opposed to when they are engaging with neighbors and merchants, or when they are relying on commercial service providers to facilitate their transactions.[18]

Notwithstanding the apparent utility of harnessing the private sector for force multiplication and superior access,[19] deputization has changed us—our

16. STANLEY, *supra* note 1, at 2; *cf.* Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1, 7 (2008) (describing the "National Surveillance State" and noting that "[i]n the National Surveillance State, the line between public and private modes of surveillance and security has blurred if not vanished. Public and private enterprises are thoroughly intertwined.").

17. *See infra* section II(B)(4).

18. Some classic Fourth Amendment cases provide support for the rationale that people do not assume—and, at least in this context, aren't penalized for not assuming—that business relations with access to their personal property will use that access to facilitate criminal investigations. *See* Stoner v. California, 376 U.S. 483, 489 (1964) (holding that hotel managers may not admit police into guests' rooms absent a warrant); Chapman v. United States, 365 U.S. 610, 617 (1961) (holding that a landlord may not grant the police warrantless entry into a tenant's residence); United States v. Jeffers, 342 U.S. 48, 51 (1951) (indicating that a hotel staff had access to a room for purposes of cleaning and maintenance but not the authority to admit police). There is, however, no corresponding Fourth Amendment protection where third parties, such as banks and telecoms, transfer customer data to the government absent the production of a warrant or the customer's consent. *See* Smith v. Maryland, 442 U.S. 735, 743–45 (1979) (holding that there is no constitutional expectation of privacy that prohibits telecoms from facilitating warrantless government pen registers); United States v. Miller, 425 U.S. 435, 440–41 (1976) (holding that the Fourth Amendment does not prevent banks from turning over customer financial records even in the absence of a warrant or customer consent).

19. Anecdotal evidence suggests that private-sector support for counterterrorism operations has at times proven quite valuable. *See* OFFICE OF THE INSPECTOR GEN., DEP'T OF DEF. ET AL., UNCLASSIFIED REPORT ON THE PRESIDENT'S SURVEILLANCE PROGRAM 36 (2009) (noting that the Terrorist Surveillance Program "may have contributed to a counterterrorism success"); Brian Harmon et al., *Jet Passengers Foil Shoe-Bomb Suspect: "We Tied Him Up with Everything We Had,"* N.Y. DAILY NEWS, Dec. 23, 2001, at 3 (reporting that airline passengers and flight attendants overpowered a man with explosives packed in his shoe); Meyer, *supra* note 5 (describing a retail service technician's assistance in foiling a domestic terrorism plot); Matthew Purdy & Lowell Bergman, *Unclear Danger: Inside the Lackawanna Terror Case*, N.Y. TIMES, Oct. 12, 2003, at A1 (noting the significance of an anonymous tip from an Arab-American citizen in identifying the Lackawanna Six); Shane & Lipton, *supra* note 8 (describing how airline passengers extinguished a fire and restrained the so-called Shoe Bomber when he tried to ignite a bomb on a commercial flight and how passengers did the same when Farouk Abdulmutallab attempted to ignite a bomb on a Christmas Day 2009 flight to Detroit); Jim VandeHei & Dan Eggen, *Cheney Cites Justifications for Domestic Eavesdropping*, WASH. POST, Jan. 5, 2006, at A2 (reporting on former Vice President Cheney's claim that warrantless eavesdropping on U.S. persons helped thwart terrorist attacks). *But see* Lowell Bergman et al., *Spy Agency Data After Sept. 11 Led F.B.I. to Dead Ends*, N.Y. TIMES,

identities, institutions, and laws—in equally profound ways. This Symposium is devoted to big and pressing questions that arise at the intersection of national security, privacy, and technology. This contribution focuses on the proliferating deputization arrangements that operate at that intersection.

In what follows, I first describe the deputization phenomenon and survey a sampling of its manifestations, sophisticated and low-tech alike. Here, attention is devoted primarily to deputization arrangements of a corporate or employment nature to the exclusion of those programs targeting the general public.

Second, I identify and address the legal uncertainties and ambiguities underlying some of these deputization programs. The ambiguities arise as private actors-*turned*-deputies move out of the purely private realm, occupy unregulated or underregulated, hybridized private–public space, and participate in the exercise of sovereign power often far beyond what society currently contemplates and what the law currently constrains. These ambiguities in the deputies' legal status at times enable the formation, operation, and success of many deputy partnerships, particularly those where private assistance is about something more than just force multiplication. Yet, they are just as relevant in creating or exacerbating the challenges these partnerships pose—challenges of social and economic dislocation, legal evasion, and even compromised security policy.

Third, by way of conclusion, I place homeland security deputization in some context. I begin this Part by considering possible contemporary analogues to deputization in the areas of criminal justice and economic regulation. I then sketch an analytical and normative framework—applicable in the homeland security context and, perhaps, beyond—for assessing whether, as an institutional matter, individual deputization arrangements operating in legally uncertain space ought to be deemed acceptable or rendered subject to greater regulatory constraints.[20]

I. Surveying Deputies

Private involvement in matters of homeland security is hardly novel. Corporate and citizen cooperation in informing the government of supposedly anti-American activities at home and abroad dates far back in our

---

Jan. 17, 2006, at A1 (citing intelligence officials' admissions that "virtually all" of the information that the National Security Agency collected in the aftermath of 9/11 led to dead ends).

20. It bears mentioning that this contribution builds on two of my recent projects—one that examines how private–public intelligence operations inhibit meaningful congressional and judicial oversight, see Michaels, *supra* note 9, and another that considers how privatization can and does expand the Executive's ability to carry out policy objectives otherwise beyond its reach, see Jon D. Michaels, *Privatization's Pretensions*, 77 U. CHI. L. REV. 717 (2010). This contribution provides a platform for synthesizing some of the material covered in that other work, and it builds on that platform to make novel interventions into the study of the use and misuse of legal-status distinctions between government actors and private actors in structuring private–public partnerships.

history.[21] It is beyond the scope of this Article to recount this history with any depth or precision. For purposes of this inquiry, it suffices to note that by the mid-1970s, many of these private–public partnerships, especially the ones lacking a statutory or regulatory underpinning, had fallen into disfavor. In no small part, it was the post-Watergate hearings and investigations and the subsequent legislative enactments by a muscular majority in Congress hostile to executive prerogatives and secrets that served to rein in the Intelligence Community as well as its private collaborators.[22]

When the demand for intelligence and intelligence operatives spiked after 9/11, the wide-scale solicitation of private assistance suddenly re-emerged as a respectable and perhaps even necessary practice. Some of the 9/11 hijackers had been living and training on U.S. soil for extended periods

---

21. *See* JAMES BAMFORD, BODY OF SECRETS 22 (2001) (recounting Western Union's assistance during World War II and the Cold War in providing the U.S. government with copies of foreign diplomatic dispatches); RON SUSKIND, THE ONE PERCENT DOCTRINE 35 (2006) (describing private intelligence and security assistance that dates back to the Civil War); TIM SHORRICK, SPIES FOR HIRE 76 (2008) (noting the corporate assistance to the NSA and CIA during the Cold War); Laura K. Donohue, *Anglo-American Privacy and Surveillance*, 96 J. CRIM. L. & CRIMINOLOGY 1059, 1080–81 (2006) (describing Operation SHAMROCK, an NSA–telecom collaboration that facilitated U.S.-intelligence operations during the Cold War). While routinized, the relationships between the private sector and the government remained largely informal collaborations that lacked, for instance, a statutory or regulatory foundation. *See* INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS: HEARINGS BEFORE THE SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, 94th Cong. 57–58 (1975) (statement of Sen. Frank Church, Chairman, Select Comm. to Study Governmental Operations with Respect to Intelligence Agencies) (noting corporate–government collaborations that were intentionally kept informal); Donohue, *supra* ("To keep [Operation SHAMROCK] under the radar, NSA deliberately refrained from formalizing the relationship in any sort of (traceable) document.").

22. See Kathryn S. Olmsted, CHALLENGING THE SECRET GOVERNMENT: THE POST-WATERGATE INVESTIGATIONS OF THE CIA AND FBI 175–76 (1996) (describing legislative efforts to curb Executive discretion in domestic and foreign intelligence domains); Harold Hongju Koh, *Why the President (Almost) Always Wins in Foreign Affairs: Lessons of the Iran-Contra Affair*, 97 YALE L.J. 1255, 1270–71 (1988) (noting post-Watergate legislative initiatives seeking to narrow presidential discretion in matters of foreign affairs and intelligence gathering); 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 telecoms insisted on more formal legal processes instead of continuing to cooperate informally with intelligence agencies); Scott Shane, *Attention in NSA Debate Turns to Telecom Industry*, N.Y. TIMES, Feb. 11, 2006, at A11 (noting that in the wake of the 1970s' legislative inquiries and reforms the telecommunications industry insisted on arm's-length dealings with the intelligence agencies). *See generally* INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS: HEARINGS BEFORE THE SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, *supra* note 21.

Notwithstanding the apparent hostility to private–public intelligence and security collaborations, some programs, ranging from workaday neighborhood watch associations to cutting-edge telecom partnerships, were created or expanded in the post-Watergate, pre-9/11 years. *See, e.g.*, Communications Assistance for Law Enforcement Act (CALEA) of 1994, Pub. L. No. 103-414, 108 Stat. 4279 (codified at 47 U.S.C. §§ 1001–1010 and in scattered sections of 18 U.S.C.) (imposing requirements on telecommunications carriers to assist in law enforcement efforts); OFFICE OF INSPECTOR GEN., *supra* note 4, at 2 (noting among other things that the Department of Transportation developed Highway Watch in 1998); Infragard: Public Private Partnership, http://www.infragard.net/faq.php (describing the joint FBI–private sector collaboration that in 1996 led to the founding of Infragard).

of time, interacting on a daily basis with flight instructors, neighbors, landlords, merchants, co-religionists, and classmates from language-training schools.[23] They also had been using banks, telecommunications providers, and airlines to facilitate their conspiracy.[24] Because of the inescapability of many of these points of contact[25] and the useful information that potentially could have been gleaned from these varied contacts (had civilians been primed to think of themselves as deputies), the Intelligence Community perceived the benefits of reaching out to citizens, employees, and corporations alike for assistance in identifying suspicious activity and preventing the next attack.[26]

And, as the efforts of passengers who forced the crashing of United Flight 93 (rather than allow the hijackers to use the jet as a weapon) attested to,[27] it became clear that impromptu physical interventions might also be necessary, at least as a last line of defense in thwarting imminent attacks.[28]

---

23. *See* 9/11 COMMISSION REPORT, *supra* note 9, at 215–53 (describing the social, commercial, financial, and employment-related interactions between the 9/11 hijackers and the American public); *see also* Wes Allison, *The Terrorists Next Door*, ST. PETERSBURG TIMES, Oct. 2, 2001, *available at* http://www.sptimes.com/News/100201/Floridian/The_terrorists_next_d.shtml (reporting on the lives of those 9/11 hijackers who lived in South Florida in the lead up to 9/11); Pam Belluck, *A Mundane Itinerary on the Eve of Terror*, N.Y. TIMES, Oct. 5, 2001, at A1 (recounting the activities of two 9/11 hijackers who had spent the day before the attacks in suburban Maine); John Cloud, *Atta's Odyssey*, TIME, Sept. 30, 2001 (describing Mohamed Atta's routine interactions with Americans); Rich Connell & Robert J. Lopez, *Portrait Emerges of an Islamic Hard-Liner*, L.A. TIMES, Dec. 12, 2001, at A18 (recounting Zacarias Moussaoui's life in Oklahoma).

24. *See* Prosecution's Ex. OG00020.2: Chronology of Events for Hijackers, United States v. Moussaoui, No. 01-455-A (E.D. Va.) http://www.vaed.uscourts.gov/notablecases/moussaoui/exhibits/prosecution/OG00020-02.pdf (detailing the hijackers' pre-9/11 use of ATMs for cash withdrawals, use of the Internet to access online travel records, and use of commercial airline services to travel around the United States); THOMAS R. ELDRIDGE ET AL., NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., 9/11 AND TERRORIST TRAVEL: STAFF REPORT OF THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES (2004), http://govinfo.library.unt.edu/911/staff_statements/ 911_TerrTrav_Monograph.pdf (detailing the hijackers' activities and interactions in the United States prior to the attacks).

25. *See, e.g.*, William K. Rashbaum, *Police Tactic Against Terror: Let's Network*, N.Y. TIMES, Aug. 14, 2004, at B1 (quoting the New York City Deputy Commissioner for Intelligence as saying that "[t]he next Mohamed Atta is far more likely to intersect with someone from the private sector than a law enforcement officer").

26. *See, e.g.*, SOLOVE, *supra* note 11, at 166 (describing how intelligence officials can compile extensive personal profiles on suspects by examining the data generated by those suspects when they use the services of banks, telecoms, and airlines); James X. Dempsey & Lara M. Flint, *Commercial Data and National Security*, 72 GEO. WASH. L. REV. 1459, 1459 (2004) (noting the "depth and breadth of personally identifiable information available from private [commercial] sources, and the capacity to analyze such data and draw from it patterns, inferences, and knowledge"); Michaels, *supra* note 9, at 908–09 (describing the pivotal role the private sector can play in assisting government surveillance and intelligence-gathering efforts).

27. *See* Lane et al., *supra* note 8 (discussing the passenger-led revolt against hijackers on United 93).

28. *See* Brooks, *supra* note 8 (remarking on the initiative taken by passengers on commercial airlines in attempting to thwart terrorist attacks); *see also* Blake Morrison, *Airlines Push Passengers To Police Cabins*, USA TODAY, Oct. 17, 2001, at 1A (quoting one pilot as instructing the

The government thus likewise recognized the value of a mobilized citizenry cognizant of their responsibilities on public transit, around critical infrastructure, and elsewhere in times of crisis.[29]

As it turns out, there was a convergence of interests. After 9/11, many corporate managers, rank-and-file workers, and average citizens were eager to do "their part"—and being encouraged to assist with safeguarding the nation from terrorism was more than adequate prompting.[30]

This Part of the Article provides a brief overview of some of this outreach to the private sector. It focuses on actors who have been invited or solicited in their capacities as corporate executives or employees to provide counterterrorism assistance to the government.[31] I call them "deputies" insofar as they are exercising some sovereign assistance, authority, or discretion far beyond what private individuals and organizations ordinarily are permitted or expected to do. Because I prioritize (1) the voluntary nature of deputy participation and (2) the uncertain legal terrain which they (and the government) must navigate in furthering these voluntary arrangements, I do not include within the ambit of discussion those operating pursuant to government contracts to assist in homeland security programs, or those compelled to support investigations through legal instruments such as court orders, subpoenas, or regulatory directives. Furthermore, because of the limited scope of this Symposium contribution, I do not attend to those individuals solicited as part of mass, open-ended appeals to the general public—even though they too could be considered deputies.[32]

---

passengers: "Throw your shoes at them. A couple of you get up and tackle him. Beat the snot out of him. I don't care.").

29. *See* President George W. Bush, Address to Joint Session of Congress (Sept. 20, 2001), *in* H.R. DOC. NO. 107-122 (2003) (honoring a victim of United Flight 93 who risked his life endeavoring to stop the 9/11 hijackers from using the airplane as a weapon); Joe Sharkey, *There's a New Deputy in the Sky*, N.Y. TIMES, Mar. 25, 2003, at C8 (noting that post-9/11 passengers are "much more vigilant now than ever").

30. *See* Karen Brandon & Dahleen Glanton, *Americans on Alert for Terror: Agencies Swamped by Calls Reporting Suspicious Activity*, CHI. TRIB., Nov. 25, 2001, at C7 ("President Bush has asked citizens to help avert further terrorist attacks by looking out for suspicious activity, and Americans have responded with vigor."); Ariana Eunjung Cha, *Watchdogs Seek Out the Web's Bad Side*, WASH. POST, Apr. 25, 2005, at A1 (profiling a leading Internet vigilante who gravitated to online surveillance of Jihadist Web sites and chat rooms after being unable, for health reasons, to enlist in the military after 9/11); Ann Davis et al., *The Tattlers: A Nation of Tipsters Answers FBI's Call in War on Terrorism—It's Neighbor vs. Neighbor, as Agents are Swamped by 435,000 Citizen Leads*, WALL ST. J., Nov. 21, 2001, at A1 (describing an influx of calls to the authorities by members of the public reporting on what they perceive to be suspicious activities in their neighborhoods); Sam Howe Verhovek, *Air Passengers Vow To Resist Any Hijackers*, N.Y. TIMES, Oct. 11, 2001, at A1 (describing post-9/11 airline passengers' apparent willingness to counter efforts by hijackers to take control of the plane); Ripley, *supra* note 4, at 39 (noting the enthusiasm among truckers for Highway Watch and characterizing it as a "morale booster for drivers").

31. Several of the examples discussed in section B of this Part were examined in greater detail in Michaels, *supra* note 9, at 910–16.

32. To be sure, it would not be a stretch to call those individuals "deputies." But the entreaties to the public are of a character quite different from the more direct and targeted appeals made by the government to specific industries, firms, and employee cohorts. Moreover, those members of the

Most of the deputy involvement is nonconfrontational. By and large, the government asks deputies to report on suspicious events viewed either in plain sight or in the course of having privileged access to private space, privileged access given to the deputies in their commercial capacities; or, the government requests access to the deputies' stores of data. But some involvement is more interventionist, including opening suspicious packages and independently analyzing data patterns for evidence of terrorist activity. Immediately below, I divide the deputy relationships into two groupings: programs targeting employees in the field (e.g., truck drivers, repair technicians, doormen) and programs geared toward corporate involvement at the management or institutional level. This division is not perfect, and there can be overlap between the two. Nevertheless, the division tracks four general, albeit not categorical, distinctions. First, whereas employees in the field are, by and large, deputized to be entrepreneurial in the assistance they provide—making their own determinations about what they view as unusual, dangerous, or suspicious—corporate management is typically responding to specific government queries and thus are providing more passive support. Second, employees in the field customarily offer eyewitness information about a specific person, incident, or transaction. The narratives they provide might be quite descriptive, but are just snapshots capturing a short period of time. By contrast, corporations tend to give the government aggregated information, numerous data points (about travel, purchases, or communications) on individuals and even large groups of individuals, often over extended periods of time. Third, employee-targeted programs are more difficult to keep secret than are corporate, data-driven programs. Many people are necessarily looped in for operations calling for thousands, or tens of thousands, of truck drivers, doormen, or service technicians to act as the government's eyes and ears. By contrast, data-driven initiatives can be administered far more discreetly, as they require the consent and cooperation of a comparatively small cohort of executives and IT specialists. Fourth, because the corporate-oriented partnerships tend to involve responding to specific queries, it may be easier for the government to monitor, assess, and control those relationships than it is for the authorities to do the same vis-à-vis employees in the field tasked with more open-ended surveillance responsibilities. As will be apparent in later parts of the Article, these differences are of significance, too, in gauging the types of challenges deputization engenders or exacerbates. For example, of the four challenges that will be highlighted in Part II, all four appear to be implicated by corporate-institutional deputization, but only two are likely to apply with any regularity to employee-oriented operations.

---

general public who heed the government's call typically occupy the force-multiplying space. For reasons explained below, this Article is particularly interested in deputies who serve the complementary purpose of providing the government with strategic advantages distinct from mere manpower support.

A. Employee-Oriented Programs

Because of their job responsibilities or the nature of their interactions with the public, segments of the American workforce have been identified as key homeland security resources. Included in this category of opportunistically situated workers are retail clerks, technicians who provide installation and repair services (cable TV, telephone, Internet, electricity, etc.), doormen, truckers, and longshoremen. By reaching out directly to workers or by entering into arrangements with their employers, unions, or industry trade associations,[33] the government has effectively deputized them to assist in security monitoring and enforcement.

Any discussion of labor-focused surveillance programs must begin with Operation TIPS. First referenced in President Bush's 2002 State of the Union Address,[34] TIPS was developed by the Justice Department as 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."[35] The government believed these workers were "well-positioned to recognize unusual events" and "report suspicious activity."[36] Especially significant were maintenance and delivery workers with direct access to individuals' homes (and thus well-positioned to observe that which is normally shielded from public scrutiny).[37] All of the

---

33. *See, e.g.*, BART ELIAS, CONG. RESEARCH SERV., SECURING GENERAL AVIATION 21 (2009), *available at* http://www.fas.org/sgp/crs/homesec/RL33194.pdf (discussing the Airport Watch program); Sara Kehaulani Goo, *Private Pilots Enlisted for Security*, WASH. POST, Oct. 10, 2002, at A14 (describing Airport Watch and Operation TIPS); Swanson, *supra* note 2 (reporting on Highway Watch).

34. *See* President George W. Bush, *State of the Union Address*, WASH. POST, Jan. 30, 2002, at A16 (announcing the establishment of USA Freedom Corps, which included Operation TIPS); *see also* STANLEY, *supra* note 1, at 3–4 (distinguishing the surveillance-oriented TIPS program from the other Freedom Corps initiatives promoting citizen preparation and training in the event of civil emergencies).

35. Documents relating to Operation TIPS have long been removed from Justice Department Web sites, but have been preserved elsewhere. *See, e.g.*, The Memory Hole: Website for Operation TIPS Quietly Changes, http://www.thememoryhole.org/policestate/tips-changes.htm (reproducing the text of the official Operation TIPS Web site, dated July 16, 2002).

36. *Id.*

37. *See* Editorial, *Ashcroft v. Americans*, BOS. GLOBE, July 17, 2002, at A22 (stating that Operation TIPS targets "letter carriers, meter readers, cable technicians, and other workers with access to private homes as informants to report to the Justice Department any activities they think suspicious"); STANLEY, *supra* note 1, at 3 ("Many of those targeted for inclusion in the scheme were workers with access to Americans' homes—utility workers, letter carriers and cable technicians—who were to report to the government anything that they considered an 'unusual or suspicious activity.'"). *Compare* Katz v. United States, 389 U.S. 347, 351 (1967) ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."), *with* United States v. Kyllo, 533 U.S. 27, 37 (2001) ("There is certainly no exception to the warrant requirement for the officer who barely cracks open the front door . . . . In the home . . . all details are intimate details, because the entire area is held safe from prying government eyes."); Silverman v. United States, 365 U. S. 505, 511 (1961) ("At the very core [of the Fourth Amendment] stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.").

participants were to be given access to special toll-free reporting numbers and their calls would be directly routed to the proper government agency.[38]

Privacy concerns first forced the Justice Department to scale back Operation TIPS,[39] and, soon after, prompted Congress to defund the program.[40] TIPS's essence was nevertheless preserved through an array of more modest programs at the federal, state, and local levels.[41] Some of those programs predated TIPS, taking on heightened significance in the wake of TIPS's cancellation. Others were fashioned anew.

First, maritime programs, one of the cornerstones of Operation TIPS, were detached and refashioned as more regional or local, stand-alone initiatives.[42] For instance, Maine established Coastal Beacon, and recruited workers in the fishing and shipping industries to be vigilant and report on suspicious activities in the water and on the docks.[43] And, in the Midwest, Ohio created Eyes on the Water,[44] and Michigan developed River Watch.[45]

A second program is Highway Watch.[46] Highway Watch enlisted the help of over three million truck drivers, creating "a potential army of eyes

---

38. The Memory Hole, *supra* note 35.

39. *See, e.g.*, MARTIN ALAN GREENBERG, CITIZENS DEFENDING AMERICA: FROM COLONIAL TIMES TO THE AGE OF TERRORISM 72–74 (2005) (quoting Senator Orrin Hatch as stating with respect to Operation TIPS that "[w]e don't want to see a 1984 Orwellian-type situation here"); STANLEY, *supra* note 1, at 3 (noting that "the TIPS proposal was . . . met by a storm of outrage" that led the government to narrow its scope).

40. Homeland Security Act of 2002, Pub. L. No. 107-296, § 880, 116 Stat. 2135, 2245 (codified at 6 U.S.C. § 460 (2006)); *cf.* Department of Defense Appropriations Act, 2004, Pub. L. No. 108-87, § 8131, 117 Stat. 1054, 1102 (2003) (defunding the Terrorism Information Awareness data-mining project).

41. *See* Donohue, *supra* note 21, at 1133 (noting that "a plethora of programs" emerged in the wake of Operation TIPS's demise). For instance, Florida reproduced key features of the disbanded TIPS program within its boundaries. *See, e.g.*, Brian Baskin, *Workers Recruited in War on Terror*, ORLANDO SENTINEL, July 8, 2004, at A1 (noting that Florida's programs are similar to the disbanded federal program); STANLEY, *supra* note 1, at 5 (noting that key aspects of Operation TIPS have been replicated at the state level by Florida).

42. *See* STANLEY, *supra* note 1, at 5 n.10. Stanley notes that whereas Operation TIPS would have created a centralized maritime program, subsequent efforts by the Coast Guard have aimed for far more decentralized operations. *Id.*

43. *Id.* at 4. Acknowledging the program's lineage, President Bush called Coastal Beacon "one of the most innovative TIP[S] programs in the country." Press Release, White House, President Promotes Citizen Corps for Safer Communities (Apr. 8, 2002), http://georgewbush-whitehouse.archives.gov/news/releases/2002/04/20020408-4.html.

44. STANLEY, *supra* note 1, at 5.

45. *Id.*; Michigan State Police: Homeland Security River Watch Program, http://www.michigan.gov/msp/0,1607,7-123-1589_3492-73050--,00.html.

46. GREENBERG, *supra* note 39, at 224–25; OFFICE OF INSPECTOR GEN., *supra* note 4, at 1–2. Highway Watch, a private–public partnership, actually predates what is commonly called the Global War on Terror. In 1998, the Trucking Association started the program, with funding from the Department of Transportation, to report generally on transportation emergencies, such as hazardous road conditions and vehicle crashes. After 9/11, its scope was expanded in recognition of the threats of terrorist attacks on U.S. soil, and its governmental responsibilities were transferred to the new Department of Homeland Security. *See* OFFICE OF INSPECTOR GEN., *supra* note 4, at 2 (noting the post-9/11 expansion and re-orientation of Highway Watch).

and ears to monitor for security threats."[47] At its height, more than 800,000 truckers were considered "active" members patrolling the nation's highways.[48]

A third initiative taps into the general aviation network of airplane pilots and airport workers.[49] It was these workers who had contact with, and some suspicious interactions with, the al Qaeda hijackers prior to the attacks of 9/11.[50] Dubbed Airport Watch, the joint Transportation Security Administration–Aircraft Owners and Pilots Association program provides specialized training in detecting and reporting on suspicious activities.[51]

A fourth set of partnerships brings doormen and building maintenance workers into the counterterrorism fold.[52] To date, tens of thousands of doormen, superintendents, and other building workers have received training and instruction regarding the detection and reporting of suspicious activities.[53] Supported by the building-owners industry as well as the unions representing building workers,[54] the workers-*turned*-deputies have been called "natural allies" of the police.[55] They are expected to alert the police to any suspicious packages or vehicles; and, they are encouraged to file reports on tenants with little or no furniture as well as on would-be renters seeking to pay in cash or via newly opened bank accounts.[56]

---

47. STANLEY, *supra* note 1, at 5.

48. OFFICE OF INSPECTOR GEN., *supra* note 4, at 4. The program has been temporarily suspended while DHS shifts resources away from the Trucking Association and to a government contractor that will help administer the program. Samuel Lowenberg, *Truckers Lose DHS Contract*, POLITICO, May 16, 2008, http://www.politico.com/news/stories/0508/10412.html.

49. ELIAS, *supra* note 33, at 35; Alonso-Zaldivar, *supra* note 3; Goo, *supra* note 33.

50. *See* 9/11 COMMISSION REPORT, *supra* note 9, at 221–27 (describing suspicious behavior exhibited by some of the 9/11 hijackers during their flight-training programs); *see also* Transcript of Record at 747–62, United States v. Moussaoui, No. 1:01cr455 (E.D. Va. Mar. 9, 2006), *available at* http://cryptome.org/usa-v-zm-030906-01.htm (statement of Moussaoui's flight school instructor) (recounting suspicious behavior of Zacarias Moussaoui in flight school); ELIAS, *supra* note 33, at 1, 12–17 (noting that the 9/11 hijackers were trained on general aviation planes and made suspicious inquiries regarding the purchase of small aircraft).

51. *See* ELIAS, *supra* note 33, at 22 (noting that Airport Watch involves the "cooperation and participation of pilots, airport tenants, and airport workers to observe and report suspicious activity"); *see also* AOPA's Airport Watch, http://aopa.org/airportwatch/ (describing the general aviation community's partnership with the Transportation Security Administration that involves more than 600,000 private pilots and airport workers acting as the government's "eyes and ears for observing and reporting suspicious activity").

52. *See* Goldman, *supra* note 8 (describing surveillance training and reporting responsibilities for doormen and other residential-building workers); Swanson, *supra* note 2 (noting the incorporation of doormen and other residential-building workers into the homeland security fold).

53. Goldman, *supra* note 8.

54. *Id.*

55. *Id.* (quoting New York City Police Commissioner Raymond Kelly).

56. *See id.* (reporting that "doormen are advised to be on the lookout for cars and trucks that seem out of place or are parked too long near buildings" and "[s]uperintendents are told to be vigilant in monitoring people with little or no furniture or newly opened bank accounts who move into apartments."). As the 9/11 Commission reported, some of the 9/11 terrorists revealed telltale signs of being suspicious tenants, including attempting to pay deposits for apartment rentals with

B. Management-Oriented Programs

The government has not only reached out to employee groups. It has also forged ties with business executives and managers to acquire data, surveillance footage, tips on suspicious customers, and physical evidence. From what we know, some relationships are driven by a convergence of patriotic interests.[57] Others have been secured through a carrots-and-sticks approach. Reportedly, the promise of government contracts,[58] the offer to share privileged, advanced information,[59] and the placement of corporate executives on high-profile private–public task forces[60] have at times been held forth as rewards for private cooperation.[61]

Among the collaborations that have trickled into the public domain is the Terrorist Surveillance Program (TSP).[62] Under the TSP, the NSA "secretly arranged with top officials of major telecommunications companies to gain access to large telecommunications switches carrying the bulk of

---

cash and owning little furniture. *See* 9/11 COMMISSION REPORT, *supra* note 9, at 219 (reporting that a real-estate agent rejected an attempt by two of the hijackers to pay cash for a deposit on an apartment rental and noting that two hijackers moved into an apartment with no furniture and no possessions). Whether those practices provide significantly sensitive guidance in exposing terrorists is, of course, a debatable proposition; but having workers focus on such tenant practices speaks to the enthusiasm and, perhaps, hubris of being able to discern terrorist patterns from atypical behavioral cues.

57. *See, e.g.*, SUSKIND, *supra* note 21, at 209–11 (describing how then-CIA Director George Tenet appealed to the patriotism of Western Union executives to secure their cooperation).

58. In particular, there have been allegations that the government has canceled or withheld contracts in retaliation against firms that refused to cooperate in intelligence operations. *See* Leslie Cauley, *NSA Has Massive Database of Americans' Phone Calls*, USA TODAY, May 11, 2006, at A1 ("In one meeting, an NSA representative suggested that . . . . Qwest's footdragging 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."); Ellen Nakashima & Dan Eggen, *Former CEO Says U.S. Punished Phone Firm*, WASH. POST, Oct. 13, 2007, at A1 (citing a Qwest executive's claim that the NSA canceled contracts worth hundreds of millions of dollars as punishment for the telecom refusing to participate in the call-data program).

59. For examples of firms receiving strategically important information in exchange for their participation, see Infragard: Public–Private Partnership, *supra* note 22; Matthew Rothschild, *The FBI Deputizes Business*, PROGRESSIVE, Mar. 20, 2008, *available at* https://www.progressive.org/mag_rothschild0308.html; and, Block, *supra* note 7. Rothschild notes that upon learning of a possible terrorist threat to some bridges in California, federal officials informed Enron and Morgan Stanley—both members of the corporate–FBI strategic partnership (called Infragard)—well before notifying state officials, including the Governor. Rothschild, *supra*, at 21–22.

60. *See* Block, *supra* note 7 (noting that FedEx has been named to the FBI's regional terrorism task force).

61. At other times, it appears that companies are selling access to information in ways that make them appear more like profiteers than partners, let alone coerced accomplices. *See* Kim Zetter, *Yahoo Issues Takedown Notice for Spying Price List*, WIRED, Dec. 4, 2009, http://www.wired.com/threatlevel/2009/12/yahoo-spy-prices (reporting on the comprehensive pricing scheme that Yahoo has established for facilitating law enforcement search requests).

62. *See* OFFICE OF INSPECTOR GEN., *supra* note 4, at 1; *see generally* James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A1 (describing the TSP).

America's telephone calls."[63] The access, granted "without warrants or court orders,"[64] enabled government eavesdroppers to monitor the content of millions of international telephone calls and electronic correspondence, including those where one of the parties was on U.S. soil.[65] Because access to this information typically would have required the government to secure court authorization pursuant to the terms of the Foreign Intelligence Surveillance Act of 1978 (FISA),[66] the deputization arrangement has been described as "open[ing] up America's domestic telecommunications network to the NSA in unprecedented and deeply troubling new ways, and represent[ing] a radical shift in the accepted policies and practices of the modern U.S. intelligence community."[67]

Second, the so-called "NSA call-data program" involved major telecommunications companies agreeing to provide the NSA with stores of telephonic and electronic metadata, including metadata generated from domestic calls and e-mails.[68] Metadata includes telephone numbers, IP addresses, and e-mail accounts of correspondents and the times that communications took place.[69] The NSA then crunches that information through sophisticated data-mining programs with the aim of piecing together relationships and patterns of relationships in a way that reveals terrorist activity and terrorists themselves.[70]

---

63. JAMES RISEN, STATE OF WAR: THE SECRET HISTORY OF THE CIA AND THE BUSH ADMINISTRATION 48 (2006).

64. Cauley & Diamond, *supra* note 1. One federal district court declared the program illegal. ACLU v. NSA, 438 F. Supp. 2d 754 (E.D. Mich. 2006). That decision was reversed by a divided panel for want of standing. ACLU v. NSA, 493 F.3d 644 (6th Cir. 2007), *cert. denied*, 552 U.S. 1179 (2008); *see also* Al-Haramain Islamic Found. v. Obama, MDL Docket No. 06-1791, 2010 WL 1244349 (N.D. Cal. Mar. 31, 2010) (rejecting the government's state-secrets barrier to reviewing the TSP and entering summary judgment in favor of the plaintiffs in light of the Government's failure to oppose plaintiffs' merits arguments).

65. RISEN, *supra* note 63, at 48; Cauley & Diamond, *supra* note 1.

66. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended in scattered titles of U.S.C.). In the aftermath of the TSP, FISA has been amended several times. *See* Protect America Act of 2007, Pub. L. No. 110-55, 121 Stat. 552 (to be codified at 50 U.S.C. §§ 1803, 1805a–1805c); FISA Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2468 (to be codified in scattered sections of 50 U.S.C.).

67. RISEN, *supra* note 63, at 44.

68. Cauley, *supra* note 58; Saul Hansell & Eric Lichtblau, *U.S. Wants Internet Companies To Keep Web-Surfing Records*, N.Y. TIMES, June 2, 2006, at A15. It is worth noting that Qwest's former CEO reported first being approached by the government in early 2001, months before the attacks of September 11. Scott Shane, *Former Phone Chief Says Spy Agency Sought Surveillance Help Before 9/11*, N.Y. TIMES, Oct. 14, 2007, at A27.

69. *See* Orin S. Kerr, *Internet Surveillance Law After the USA PATRIOT Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 607, 611 (2003).

70. *See* Michaels, *supra* note 9, at 912; Ira S. Rubinstein, Ronald D. Lee & Paul M. Schwartz, *Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches*, 75 U. CHI. L. REV. 261, 261 (2008); K.A. Taipale, *Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data*, 5 COLUM. SCI. & TECH. L. REV. 1, 33–35 (2003). Though the bulk of legal and academic attention is typically focused on the content of communications (and thus on eavesdropping), see, for example, Orin S. Kerr, *A User's Guide to the Stored Communications Act,*

Third, another recently disclosed telecom program began as a contractual arrangement to facilitate the processing of FBI subpoenas (specifically, National Security Letters,[71] or NSLs).[72] Evidently, it soon morphed into something far more open-ended, accommodating, and, perhaps, legally dubious.[73] With representatives of the major telecommunications firms detailed to FBI offices, assigned FBI e-mail accounts, granted access to FBI computer networks, and invited to socialize after work with the government agents,[74] the telecoms soon dispensed with asking to be served with NSLs as a condition of processing the data queries.[75] Indeed, the telecoms reportedly informed FBI officials that the government could bypass the requirements for producing a valid NSL and instead invoke its so-called "exigent-letter" authority[76] to acquire the sought-after information more quickly (and with a lower evidentiary showing).[77] The telecoms even generated the exigent-letter authority forms for the FBI to sign.[78] It appears as if even this shortcut was eventually circumvented, as the telecoms subsequently agreed to give the FBI "sneak peeks" at data to see if the underlying information would be worth the agents' time to initiate formal requests (via exigent letters or NSLs).[79] More interesting, at least for present purposes, than this gradual erosion of legal protocols was the proactive engagement of the telecom employees. The telecom workers not only

---

and a Legislator's Guide to Amending It, 72 GEO. WASH. L. REV. 1208, 1229 n. 142 (2004), scholars have also recognized the exceptional utility of compiling virtual dossiers and piecing together virtual itineraries of suspects' communications over months or even years. *See, e.g.*, Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264, 1287–88 (2004).

71. *See, e.g.*, 18 U.S.C. § 2709(a) (2006), *since limited by* John Doe, Inc. v. Mukasey, 549 F.3d 861, 862 (2d Cir. 2008). For a more detailed discussion of NSLs, 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, at x–xiv (2007), http://www.usdoj.gov/oig/special/s0703b/final.pdf [hereinafter FBI USE OF NATIONAL SECURITY LETTERS].

72. OFFICE OF INSPECTOR GEN., U.S. DEP'T OF JUSTICE, A REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION'S USE OF EXIGENT LETTERS AND OTHER INFORMAL REQUESTS FOR TELEPHONE RECORDS 12 (2010), http://www.justice.gov/oig/special/s1001r.pdf [hereinafter FBI USE OF EXIGENT LETTERS]. For an earlier instance of reported improprieties involving the FBI's use of NSLs, see FBI USE OF NATIONAL SECURITY LETTERS, *supra* note 71.

73. *See* John Solomon & Carrie Johnson, *FBI Broke Law for Years in Phone Record Searches*, WASH. POST, Jan. 20, 2010, at A1.

74. FBI USE OF EXIGENT LETTERS, *supra* note 72, at 25; Ryan Singel, *FBI, Telecoms Teamed To Breach Wiretap Laws*, WIRED, Jan. 21, 2010, http://www.wired.com/threatlevel/2010/01/fbi-att-verizon-violated-wiretapping-laws/#ixzz0e3YLimPT.

75. FBI USE OF EXIGENT LETTERS, *supra* note 72, at 33.

76. *See* 18 U.S.C. § 2702(c)(4) (2006) (authorizing emergency exceptions to the usual NSL requirements in cases where the government has a good-faith belief that a delay in acquiring the information could result in serious injury or the loss of life).

77. *See* FBI USE OF EXIGENT LETTERS, *supra* note 72, at 31–32 (noting that the FBI agent in charge of the program first learned of exigent-letter authority from "Company A" and that based on the information provided by "Company A" the agents began invoking exigent-letter authority).

78. *Id.* at 33.

79. *Id.* at 47–50.

proposed and facilitated the shortcuts (which presumably were outside of the terms of the government contracts[80]) but also took the initiative regarding what they saw as "very interesting" patterns of use among phone numbers and "strongly suggest[ed]" that the FBI investigate certain leads further.[81] Tellingly, at least one of the telecom employees created an e-mail folder entitled "TEAM USA" and sent out e-mails to FBI agents that "began with a greeting to 'Team.'"[82]

Fourth, soon after 9/11 the CIA approached Western Union executives and told them "this country is in a fight for its survival. What [we're] asking is that you and your company be patriots."[83] Ever since, Western Union has reportedly been alerting the government to suspicious wire transfers, turning over data detailing transactions by persons of interest to the government, and sending intelligence officials real-time video images of those wiring money from Western Union storefronts.[84]

Fifth, FedEx, which prior to 9/11 steadfastly denied law enforcement requests for assistance,[85] has since committed itself fully to U.S. counterterrorism efforts.[86] Its ready cooperation, which includes opening and inspecting packages at the government's behest,[87] stands in contrast to that of its main competitors, United Parcel Service and the United States Postal Service—both of which refuse to service government requests absent legal compulsion.[88]

Sixth, through Operation Nexus, the New York City Police Department has established collaborative relationships with businesses that may be of particular interest to terrorists.[89] Defining "interest" broadly, police have reached out to more than 30,000 businesses—including scuba shops, plastic

80. And, which were presumably not in the financial interests of the firms, in no small part because such informal facilitation may have exposed the telecoms to legal liabilities. Many of the actual terms of the contracts are censored in the Inspector General's published report. Based on the nonredacted portions of the report, the contracts do not appear to call for the fluid exchange of information that appears to have taken place. *See id.* at 20–24.

81. *Id.* at 47–49.

82. *Id.* at 25.

83. SUSKIND, *supra* note 21, at 211. Western Union has a long history of providing such support for the government. *See supra* note 21 and accompanying text.

84. SUSKIND, *supra* note 21, at 208–11; Michaels, *supra* note 9, at 914.

85. Block, *supra* note 7.

86. *See id.* (quoting FedEx's CEO as committing his company to cooperate with the government "up to and including the line on which we would be doing a disservice to our shareholders").

87. *Id.*

88. *See* Corky Siemaszko, *FedEx Delivers—Info to the Feds*, N.Y. DAILY NEWS, June 5, 2005, at 24 (citing both UPS and the USPS as unwilling to provide customer information to the government without a warrant); *see also* Dan Eggen, *Bush Warned About Mail-Opening Authority*, WASH. POST, Jan. 5, 2007, at A3; Isaac Baker, *Little Support for TIPS*, NEWSDAY, July 21, 2002, at A25.

89. *See* NYPD Shield: Operation Nexus, http://www.nypdshield.org/public/nexus.nypd (detailing a program designed to foster counterterrorism collaboration between the police department and the private sector).

surgeons, hardware stores, and self-storage facilities, located within and outside of the five boroughs.[90] One of the program's goals is to encourage businesses to be sensitive to suspicious inquiries and transactions and to file reports with the authorities.[91]

II. Underregulation and Uncertainty in the Deputized Space

The descriptive accounts offered above identify cartographic information about how two landscapes—that of homeland security and that of civil and corporate society—intersect and overlap through deputization programs and practices. They also provide us with the tools to do more: first, to locate the legal uncertainties that underlie the transformation of private actors into deputies who participate in the exercise of sovereign authority (often without fully bearing the legal responsibility commensurate with that exercise); second, to understand the challenges—e.g., disruptions to civil society, the market economy, the rule of law, and even the counterterrorism operations themselves—engendered or exacerbated by the legal uncertainties clouding the deputized space; and, third, to begin the process of developing a framework for differentiating acceptable from intolerable manifestations of deputization that take place in unregulated or underregulated space. This Part of the Article takes up the first two tasks. Sketching an evaluative framework will be reserved for Part III.

A. Deputization's Legal-Status Uncertainties

Status is critical to the deputization agenda, especially where deputization is something more than simply an exercise in force multiplication. Deputy relationships that provide something more—e.g., special access or the bypassing of legal restrictions imposed exclusively on government actors—pivot in no small part on the diffusion, distortion, and re-invention of traditional status designations of the private actors-*turned*-deputies. To develop these arrangements, deputization's architects frequently build in unregulated or underregulated space, gaps in the legal landscape where statutory, regulatory, and decisional law have not fully defined the scope of government or private-sector conduct. The architects then deploy the deputies and direct them to perform (or to support) a range of state-security duties in this space. In turn, the deputies find themselves in a form of identitarian limbo: no longer confined to the boundaries of their civilian and corporate existence, but far from being full-fledged government agents; no longer driven exclusively by market pressures, but far from being inattentive to profits or their employment responsibilities.

---

90. *See* William Finnegan, *The Terrorism Beat: How is the N.Y.P.D. Defending the City?*, NEW YORKER, July 25, 2005, at 58; Judith Miller, *On the Front Line in the War on Terrorism*, CITY J., Summer 2007, *available at* http://www.city-journal.org/html/17_3_preventing_terrorism.html; Rashbaum, *supra* note 25.

91. *See* Miller, *supra* note 90.

The deputies' limbo—and the legal ambiguities and uncertainties surrounding their status and the status of the hybrid, private–public space they occupy—is empowering, frustrating, and dangerous, sometimes all at once. Because of their ostensible private status (and the stickiness of that status notwithstanding the realities of deputies crossing over into public, sovereign domains), these civilians-*turned*-deputies at times are able to further government aims with less notice, resistance, or legal consequence than if they were actually to join the governmental ranks or otherwise shed their private personas. This is precisely why deputization is not simply about force multiplication: There are special benefits that accompany the marshaling and martialization of the private sector (qua private sector), and one of the chief benefits is the government's ability to leverage this status ambiguity in favor of deeper reaching (and not just more numerous) homeland security programs.

This legal uncertainty or ambiguity also opens the door to coercive, discriminatory, or destructive practices within largely unregulated private–public space. Among them, there are newfound opportunities for the government to pressure deputies, as well as opportunities for deputies to go beyond what the government wants or expects them to do vis-à-vis exercising sovereign discretion, either in furtherance of the deputies' business aims or in furtherance of the deputies' own conception of the public good. Moreover, the uncertainty may deter conscientious would-be deputies and simultaneously attract the more risk-seeking civilians; it thus suggests the likelihood of selection and recruitment problems that may undermine deputization's homeland security goals.

B. The Challenges of Ambiguity

In what follows, I discuss some of the challenges created or exacerbated by the ambiguous and uncertain status issues that surface in deputized space. These challenges span a wide range of policy and legal domains including national and homeland security, due process, separation of powers, and market competition.[92] Specifically, I highlight four types of ambiguity and work through their effects vis-à-vis the deputization agenda: (1) government actors conflating how they interact and negotiate with would-be deputies and how they generally interact and negotiate with private firms and industries, what I call the Market Distortion Challenge; (2) deputies conflating their own public and private roles, what I call the Misappropriation Challenge; (3) deputies' uncertain assessment of uncertain legal space, what I call the Risk Selection Challenge; and, (4) the legal regime's uncertainty in distinguishing deputies from nondeputized civilians, what I call the De Facto

92. Because there is no shortage of discussions regarding privacy, either in this Symposium or in the scholarly literature in general, I do not focus on the privacy encroachments even though they are broadly implicated and likely exacerbated by the legal uncertainty undergirding most of the deputization arrangements under examination.

State Action Challenge. Hardly constituting an exhaustive list, these four issues are just a sampling of some of the procedural and substantive challenges that deputization invites.[93]

1. The Market Distortion Challenge: Government Actors Conflating Treatment of Deputies and Private Firms.—As alluded to above, the government solicits deputy participation through a number of channels. It might apply moral suasion, appealing to patriotism and volunteerism to induce private firms to enter into deputy relationships.[94] Or, it might resort to doling out perks or threatening punitive action.[95]

Outside of the voluntary deputization context, the government can compel participation by invoking statutory and regulatory authority to require[96] or encourage disclosures;[97] government officials can also enter into contracts and thus purchase support services from the private sector or

93. A few notes before proceeding. First, although identitarian limbo and the uncertain legal status of deputies lie at the heart of the concerns to be discussed in this section, it does not follow that the converse—a deputization regime grounded in legal certainty—is a necessary or sufficient antidote. This issue will be addressed in greater detail in Part III. Second, although I recognize that what I term a "challenge" incident to deputization is subject to some normative contestation, the scope of this Symposium contribution limits the depth with which I can thoroughly defend the challenges as normatively charged phenomena. Third, deputization, even as narrowly addressed in this inquiry, operates along a spectrum between some regulatory foundation and no regulatory foundation. Some programs are, at the very least, publicly announced and funded, with congressional appropriations going to conduct outreach and training and to pay for the dedicated hotlines and other support measures that facilitate deputization. *See, e.g.*, *supra* notes 46–48 and accompanying text (discussing Highway Watch); *supra* notes 49–51 and accompanying text (discussing Airport Watch). These programs may be audited regularly (as a practical reality, if not a statutory imperative) and not only in response to a front-page scandal. *See, e.g.*, OFFICE OF INSPECTOR GEN., *supra* note 4. Others are largely (and intentionally) under the radar, and within that category we have some programs—such as the TSP—that seem to violate existing laws, and also programs that simply avail themselves of the opportunity to operate in unregulated space. *See, e.g.*, *supra* subpart I(B); *cf.* Adrian Vermeule, *Our Schmittian Administrative Law*, 122 HARV. L. REV. 1095, 1103–31 (2009) (describing "black" and "grey" holes in the administrative state). Thus, my analysis sometimes encompasses all deputization programs, and sometimes just a particular subset. Fourth, the distinctions drawn in Part I between employee and corporate-oriented deputization programs are relevant here, too. By and large, many of the corporate-oriented arrangements are likely to implicate all four sets of challenges described in this section. Employee programs, on the other hand, are more likely to implicate only the latter two.

94. *See supra* note 57 and accompanying text.

95. *See supra* notes 58–60 and accompanying text.

96. For a canvassing of some such legal authorities to compel assistance, see Paul M. Schwartz, *Reviving Telecommunications Surveillance Law*, 75 U. CHI. L. REV. 287, 289–305 (2008).

97. *See, e.g.*, Critical Infrastructure Information Act (CIIA) of 2002, 6 U.S.C. §§ 131–134 (2006). The CIIA includes a blueprint for private–public cooperation and for private–public quid pro quos. Among other things, the Act immunizes corporations from civil liability for weaknesses in their infrastructure, provided those weaknesses are first disclosed to the government. *Id.* § 133(a)(1). The government encourages and rewards such disclosures as a way of increasing the likelihood of its knowing what corporate vulnerabilities exist and how they might endanger national, economic, or homeland security.

simply buy privately held information.[98] Through these legal and contractual channels, the government has (1) some flexibility in terms of how best to structure partnership relationships; (2) express authority to encroach on the autonomy of the market economy; [99] and, (3) greater legal clarity as to what roles the private participants will play. But what is different about deputization in contrast to legal compulsion or contract—even though the difference may be more a matter of degree than kind—is that where deputization lacks regulatory authority, guidance, and transparency, it opens the hybrid private–public space to an inordinate amount of ad hoc horse trading. This horse trading not only influences private-sector participation in counterterrorism efforts. It may also spill out of the homeland security deputization space altogether and more generally distort markets and market decisions.

Consider the carrots and sticks reportedly used to entice cooperation and punish refusals to participate. Less efficient firms willing to play ball in matters of homeland security could gain a comparative advantage in the marketplace over more efficient firms hesitant to cooperate. Indeed, if the market is otherwise competitive and the perks of participation are significant, the latter group of companies will face a difficult decision: forgo government contracts and access to strategic information—at some risk to profits and market share—or go against their business obligations (e.g., contractual assurances of consumer privacy protections) or legal misgivings in order to stay viable.[100]

---

98. For discussions of data brokering, see Michaels, *supra* note 9, at 917–19; and Joshua L. Simmons, Note, *Buying You: The Government's Use of Fourth-Parties to Launder Data About "the People,"* 2009 COLUM. BUS. L. REV. 950.

99. *See, e.g.*, Communications Assistance for Law Enforcement Act (CALEA) of 1994, Pub. L. No. 103-414, 108 Stat. 4279 (codified at 47 U.S.C. §§ 1001–1010 and in scattered sections of 18 U.S.C.) (requiring telecommunications providers to ensure that their technologies are compatible with those the government uses to engage in lawful surveillance and monitoring efforts); Davis–Bacon Act, ch. 411, 46 Stat. 1494 (1931) (requiring government contractors to pay prevailing wages for public-works projects).

100. Perhaps a firm such as UPS might experience such pressure. As noted above, FedEx, UPS's chief rival, has received a range of national security perks, which might be viewed as compensation for the courier company's steadfast and public support of government intelligence operations. *See supra* Michaels, *supra* note 9, at 914–16; notes 60, 85–88 and accompanying text. Among other things, FedEx was the first private company to be named to a seat on the FBI's regional terrorism task force. It was also awarded an exceptional license to establish its own police force with investigatory and arrest powers. *See supra* Michaels, *supra* note 9, at 914–15, Block, *supra* note 7. As a dutiful deputy, FedEx receives information early. *See* Gary Fields, *FedEx Takes Direct Approach to Terrorism*, WALL ST. J., Oct. 9, 2003, at A4 (noting that members of the regional task forces are given "more-sensitive and specific data regarding terrorist threats than businesses usually receive"). Might UPS, which reportedly rejected at least some of the government's requests for counterterrorism assistance, be left out in the cold? If so, it likely incurs greater risk by not having the same access FedEx does to counterterrorism intelligence. For instance, if UPS facilities aren't as carefully safeguarded (or if UPS has to expend more of its own resources on *private* security initiatives because it isn't receiving courtesy tips from the government), might that be a reason for customers and shareholders to switch to FedEx? *See id.* ("[T]he FedEx representative [receiving the more sensitive and specific information] can signal the company to take preventative actions. If the task force learns certain kinds of explosives are being

The distortions might not end there. Shareholders—the firms' *principals*—might become uneasy about managers—the firms' *agents*—entering into these voluntary relationships, or uneasy about managers forgetting about the market incentives altogether when approached by the government and told to put country ahead of corporation.[101] These principals might then seek to lessen the delegated discretion accorded to their agents.[102] But keeping management on a tighter leash in response to the fear that the executives will otherwise commit too fully to deputization could lead to an inefficient allocation of principal–agent discretion and responsibility in terms of general strategic planning or day-to-day operations, thus introducing additional distortions into the market economy.

Whether deputization's horse trading strikes a better or worse balance on the security–liberty continuum than if the government used its existing statutory authorities (or sought new power) to compel and contract for assistance is, for present purposes, beside the point. What instead matters is twofold. First, on the substance, we may be discomforted by the government tipping the scales of market competition based on which firms cozy up with the intelligence agencies. In essence, the government is using deputies' dual status against them by striking at their private, nondeputy interests. The government does so not only in a way that can warp market competition, but also in a way that is contrary to how it tends to approach the private sector in, for example, the ordinary government-contracting context, perhaps a close alternative to deputization arrangements. When soliciting and then evaluating bids for government contracts, agencies are ordinarily required to ensure nondiscriminatory treatment among competitors such that "winners" and "losers" are designated as such on the basis of price and quality[103]—not, say,

---

used by terrorists in Asia, for instance, the representative can alert the company to install specialized explosives detectors there.").

101. *See supra* note 57 and accompanying text.

102. For seminal discussions of principal–agent concerns, see Michael C. Jensen & William H. Meckling, *Theory of the Firm: Managerial Behavior, Agency Costs, and Ownership Structure*, 3 J. FIN. ECON. 305, 312–30, 333–43 (1976); and Armen A. Alchian & Harold Demsetz, *Production, Information Costs, and Economic Organization*, 62 AM. ECON. REV. 777, 785–90 (1972).

103. *See, e.g.*, Competition In Contracting Act (CICA) of 1984, Pub. L. No. 98-369, 98 Stat. 1175 (codified at 40 U.S.C. § 471 et seq.; 41 U.S.C. § 251 et seq.). Some exceptions to the general rule that winners are chosen based entirely on the strength of their bid proposals exist; by and large, however, those bases for discriminating among firms on non-market terms have been authorized by statute or regulation. *See, e.g.*, Veterans Benefit Act of 2003, Pub. L. No. 108-183, 117 Stat. 2662 (codified at 15 U.S.C. § 657f (2003)) (authorizing preferences for contract bids from small businesses owned by service-disabled veterans). It is also true that, for better or worse, the government could—and sometimes might need to—tailor its contracting specifications such that certain firms are likely to be the only ones qualified to handle delegated responsibilities. *See, e.g.*, Dan Baum, *Nation Builders for Hire*, N.Y. TIMES, June 22, 2003, § 6 (Magazine), at 32 ("KBR got the Iraqi oil-field contract without having to compete for it because, according to the Army's classified contingency plan for repairing Iraq's infrastructure, KBR was the only company with the skills, resources, and security clearances to do the job on short notice.").

Moreover, it is of course the case that the government could impose legal conditions on firms selectively, serving some with onerous subpoenas and court orders, while simply asking other firms

on whether firms contributed to the President's campaign coffers or funneled information to the intelligence agencies. In addition, the government's commodification of vital security information is yet another way of complicating and confusing the dual roles of deputies and private businesses. Here too, by rationing information[104] and giving advanced notice only to cooperative firms,[105] which then are in a better position to safeguard their assets and customers (and save money by not having to independently analyze security threats), the government is affecting the private market.

Second, as a procedural matter, there is the question of democratic legitimacy in how the government interacts with would-be deputies. With the advent of deputization and the informality associated with many of its non-statutory, non-regulatory arrangements, there are now two scripts for engaging the private sector: the official script that contains a variety of authorized inducements and coercive directives[106] and the unofficial script that leaves the inducements and the coercive strategies to the imagination and discretion of the intelligence officials.[107] That is to say, however much the government already reaches into the day-to-day business of corporate America, and however much discretion it has in making those interventions,[108] it does so typically constrained by the scope of democratic authority, an insistence on transparency, procedural regularity, nondiscrimination, and the imperatives of reasoned public administration.[109] It can

---

to comply. Thus, my point is not that the government is otherwise—outside of deputization, that is—entirely evenhanded; rather, simply that deputization may exacerbate the potential for unequal treatment across firms.

104. Assuming the firms aren't themselves security risks, there is little justification for not sharing this nonscarce information with other American businesses (other than to hold it out as a reward or in-kind payment).

105. *See supra* notes 59, 100 and accompanying text.

106. *E.g.*, Critical Infrastructure Information Act (CIIA) of 2002, Pub. L. No. 107-296, §§ 211–215, 116 Stat. 2135, 2150 (2002) (codified at 6 U.S.C. §§ 131–134 (2002)).

107. *Cf.* HBO v. FCC, 567 F.2d 9, 53–54 (D.C. Cir. 1977) (criticizing ex parte contacts in the course of agency rulemaking and noting that "[e]ven the possibility that there is here one administrative record for the public and this court and another for the Commission and those 'in the know' is intolerable").

108. *See, e.g.*, Heckler v. Chaney, 470 U.S. 821, 834–35 (1985) (declaring agency decisions as against whom to bring enforcement actions generally unreviewable); FTC v. Standard Oil Co. of Cal., 449 U.S. 232, 238–46 (1980) (finding FTC issuance of a complaint was not judicially reviewable before the conclusion of the administrative adjudication, notwithstanding the complaint's immediate disruptive effects on business).

109. *See Heckler*, 470 U.S. at 848 (Marshall, J., concurring). Justice Marshall states:

> [T]he *sine qua non* of the APA [Administrative Procedure Act] was to alter inherited judicial reluctance to constrain the exercise of discretionary administrative power—to rationalize and make fairer the exercise of such discretion. Since passage of the APA, the sustained effort of administrative law has been to "continuously narro[w] the category of actions considered to be so discretionary as to be exempted from review." Discretion may well be necessary to carry out a variety of important administrative functions, but discretion can be a veil for laziness, corruption, incompetency, lack of will, or other motives, and for that reason, "*the presence of discretion should not bar a court from considering a claim of illegal or arbitrary use of discretion.*" Judicial

hardly be assured that these commitments will carry over into the deputization context. Indeed, the concerns associated with ad hoc interactions with corporations are especially acute in the secretive world of intelligence, where external scrutiny and effective oversight are often wanting,[110] and where firms are in a weaker position to cry foul (both because the classified nature of the proposed arrangements prevents them from speaking out and because the firms will be fearful that their speaking out in opposition to government entreaties will be viewed as unpatriotic). Thus, the shift from even a relatively flexible but law-based paradigm to one where deputization occurs in the gaps and shadows of regulation is that much more significant.

2. The Misappropriation Challenge: Deputies Conflating Their Deputy and Private Roles.—A different concern, but one that also stems from the fluidity and ambiguity of status roles, is the possibility that businesses agreeing to serve as deputies will misappropriate the intelligence information they are receiving from the government to deny services to customers who are targets of investigations. In many cases, the government needs to disclose some information to the corporations to facilitate the processing of surveillance queries; indeed, that's likely the sole purpose of the government's disclosure. For the firms to take the information and use it for business decisions is in one respect to be expected given the firms' dual identities as facilitators of counterterrorism operations and also as for-profit

---

> review is available under the APA in the absence of a clear and convincing demonstration that Congress intended to preclude it precisely so that agencies, whether in rulemaking, adjudicating, acting or failing to act, do not become stagnant backwaters of caprice and lawlessness.

Id. (internal citations omitted). *See* Ethyl Corp. v. EPA, 541 F.2d 1, 68 (D.C. Cir. 1976) (Leventhal, J. concurring) ("Congress has been willing to delegate . . . broadly and courts have upheld such delegation because there is court review to assure that the agency exercises its delegated power within statutory limits, and that it fleshes out objectives within those limits by an administration that is not irrational or discriminatory."); *see also* Massachusetts v. EPA, 549 U.S. 497, 533–34 (2007) (requiring agency to provide reasoned justification for refusing to render a scientific judgment relevant to whether greenhouse gases should be regulated); Motor Vehicle Mfrs. Ass'n v. State Farm Mut. Auto. Ins. Co., 463 U.S. 29, 56–57 (1983) (invalidating agency recission of rule where the agency fails to articulate a reasoned explanation for the recission); Citizens To Preserve Overton Park, Inc. v. Volpe, 401 U.S. 402, 417–20 (1971) (rejecting agency decision where Secretary failed to make findings in support of agency decision); Jody Freeman & Adrian Vermeule, Massachusetts v. EPA: *From Politics to Expertise*, 2007 SUP. CT. REV. 51, 87–92, 97 (highlighting an expertise-forcing approach by courts reviewing agency decisions and non-decisions).

110. *See* James A. Baker, *Intelligence Oversight*, 45 HARV. J. ON LEGIS. 199, 205 (2008); Neal Kumar Katyal, *Internal Separation of Powers: Checking Today's Most Dangerous Branch from Within*, 115 YALE L.J. 2314, 2318–22 (2006) (emphasizing that foreign affairs and national security are domains where legislative and judicial scrutiny is often lacking); Memorandum from Alfred Cummings, Specialist in Intelligence and Nat'l Sec., Cong. Research Serv., to Senator Dianne Feinstein (Dec. 14, 2005), *available at* http://feinstein.senate.gov/crs-intel.htm (noting Congress's comparative inability, because of the limited information the Executive provides, to independently assess the quality of intelligence and the operations).

enterprises.[111] But it is also highly problematic as a matter of due process and also substantively, as the private appropriation of that information may undercut national security objectives.

For a variety of reasons, the government might give firms a list of named targets (or phone numbers, bank account numbers, or IP addresses) without distinguishing among sure-fire terrorists, likely terrorists, possible confederates, and friends, family, and colleagues not themselves suspected of involvement in terrorist conspiracies. The government might simply not be at liberty, or otherwise inclined, to share that information with the firms. Or it might not yet know enough to draw such distinctions.[112] Indeed, as has been reported, the government might know so little that it asks companies to do their own analysis to ascertain a target's "community of interest."[113] The government's casting of a wide net might be particularly likely in deputization contexts if the reason for the request being channeled through a deputization partnership is that the government lacks the evidentiary basis to compel disclosure through court orders or administrative subpoenas.[114]

In some settings, firms are legally required to deny services to individuals named on government watch lists. The No-Fly list is of that

---

111. The decision to mix the government search request with the business bottom line is an almost unavoidable outcome when deputies are asked to occupy hybridized space and must, at the end of the day, prioritize their private (business) responsibilities over their public charges. *See* Dodge v. Ford Motor Co., 170 N.W. 668, 684 (Mich. 1919) (emphasizing the primary duty of corporate managers to maximize shareholder profits); *see also* AUDIT DIV., 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 (describing a particularly cold-blooded business decision by a telecom working very closely with the FBI on counterterrorism operations that resulted in a temporary disabling of the government's access to electronic surveillance and lost evidence); *cf.* Daniel I. Gordon, *Organizational Conflicts of Interest: A Growing Integrity Challenge*, 35 PUB. CONT. L.J. 25 (2005). Of course, an argument could be made that prioritizing the government requests in the context of homeland security would be in the long-term financial interests of the corporations. *Cf.* Shlensky v. Wrigley, 237 N.E.2d 776, 777–78 (Ill. App. 2d 1968); A.P. Smith Mfg. Co. v. Barlow, 98 A.2d 581, 583–86 (N.J. 1953).

112. *See* Eric Lichtblau, *F.B.I. Made 'Blanket' Demands for Phone Records*, N.Y. TIMES, Mar. 14, 2008, at A1.

113. *See* Eric Lichtblau, *F.B.I. Data Mining Reached Beyond Initial Targets*, N.Y. TIMES, Sept. 9, 2007, at A1 ("The scope of the demands for information could be seen in an August 2005 letter seeking the call records for particular phone numbers under suspicion. The letter closed by saying: 'Additionally, please provide a community of interest for the telephone numbers in the attached list.'"); *see also* FBI USE OF EXIGENT LETTERS, *supra* note 72, at 47–49 (detailing corporate involvement in developing a list of names associated with a particular target).

114. *See* FREDERICK A.O. SCHWARZ, JR. & AZIZ Z. HUQ, UNCHECKED AND UNBALANCED: PRESIDENTIAL POWER IN A TIME OF TERROR 132 (2007) (describing efforts by the intelligence agencies to proceed informally on the basis of "thinner evidence"); Carol D. Leonning & Dafna Lanzer, *Judges on Surveillance Court To Be Briefed on Spy Program*, WASH. POST, Dec. 22, 2005, at A1 (noting the Bush Administration's contentions that the statutory and regulatory evidentiary hurdles were often too great for the intelligence agencies to secure the desired authorization they needed to conduct electronic surveillance).

vein,[115] as are lists generated by Treasury's Office of Foreign Assets Control.[116] But in other contexts, and absent the regulatory directives that give effect to those official lists (that is to say, the government generates the suspect list internally and then orders private companies to refuse access or service to would-be customers named to the list), when the government provides names to private firms to facilitate data-mining or surveillance operations, it isn't intending for the companies to use that information as they see fit in their business dealings. Yet, as some suspect, firms might be using those lists to deny services to customers included on the government query sheets.[117]

Decisions by the companies to deny services might be efforts to mete out private justice: the bank, telecom, or travel company takes matters into its own hands, doing its part to punish the perceived evildoers. Thus, it cancels lines of credit, disconnects Internet service, or makes it more difficult for the named individuals to arrange transportation or secure employment. Or, the misappropriation and denial of services are acts of self-interest: firms might not want to, among other things, extend credit to someone about to be deported or detained. More to the point, what company wants to be known for furnishing a group of terrorists with the rental car used to set off a bomb, or to have hosted on its servers the Jihadist chat room out of which emerged a lethal band of terrorists.[118]

Yet in denying often-essential services,[119] the companies are working off scant information and making decisions without any solid grounding in due process[120] or factual substantiation.[121] For all the firms know, the

115. *See* 49 U.S.C. § 114(h) (Supp. I 2001) (providing authority for the imposition of No-Fly lists on commercial airlines); *see also* Jeffrey Kahn, *International Travel and the Constitution*, 56 UCLA L. REV. 271, 321–23 (2008); Justin Florence, Note, *Making the No Fly List Fly*, 115 YALE L.J. 2148, 2155–59 (2006). *See generally* Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249, 1274 (2008) (noting the No-Fly list's high incidence of false positives).

116. Exec. Order 13,224, 66 Fed. Reg. 49,079 (Sept. 23, 2001); *see also* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, § 314, 115 Stat. 272, 307–08 (codified at 31 U.S.C. § 5311 (2006)).

117. *See* Sara B. Miller, *Blacklisted by the Bank*, CHRISTIAN SCI. MONITOR, Aug. 25, 2003, http://www.csmonitor.com/2003/0825/p15s01-wmcn.html; Kim Zetter, *Big Business Becoming Big Brother*, WIRED, Aug. 9, 2004, http://wired.com/news/conflict/0,2100,64492,00.html?tw=wn_tophead_1 (describing the possibility that firms are cross-checking government surveillance lists to deny services and offers of employment to individuals named to those lists).

118. Indeed, firms might find themselves in a Catch-22: assuming a company does not appropriate the information, subsequent revelations that government security agencies gave the company the names of the individuals who later perpetrated an attack will lead to questions why the firm continued to do business with those individuals.

119. These decisions will no doubt disproportionately affect certain, already vulnerable communities.

120. Historically, common carriers under the common law and regulated industries under the Interstate Commerce Act have been sanctioned for engaging in discriminatory practices or arbitrary denials of service. *See* Joseph Kearney & Thomas Merrill, *The Great Transformation of Regulated Industries*, 98 COLUM. L. REV. 1323, 1325, 1331–32 (1998) (noting that the 1887 Interstate

"target" is simply a person who has communicated with the real suspect or just happens to have the same name as someone suspected of being involved in terrorism. In those cases, there is no moral or strategic basis for denying service. Or, the government is monitoring a bunch of guppies in an effort to lure and reel in the big fish—and cutting off services to those guppies might tip off a terrorist cell and force it to go deeper underground.[122] In that situation, there might well be plausible reasons for the firms to terminate service as a matter of justice and financial and reputational self-interest. But there obviously are also national security reasons why the government might want these "guppy" customers to continue going about their business. Accordingly, the misappropriation is not just an issue of insufficient due process and discriminatory business practices, but also an issue of undermining security objectives.

3. The Risk Selection Challenge: Deputies' Uncertain Assessment of Uncertain Space.—Uncertainty surfaces, too, with respect to how deputies view themselves, their status, and their responsibilities in hybridized space. Some may be drawn to the apparent freedom afforded to step outside of the confines of civilian life; they can aid in counterterrorism operations without truly having to give themselves over to a public calling (by formally entering government service)—and perhaps without incurring the same legal liabilities for acting overzealously that government officials would face. For others, stepping outside of civilian life may be unnerving. Without clearly defined duties and without clear legal guidance regarding their responsibilities in this private–public space, they might not be willing to take the chance that they will in fact be beyond sanction.

The ambiguity regarding the hybridized space invites something somewhat akin to an adverse selection problem,[123] and thus threatens to

---

Commerce Act imposed a nondiscrimination obligation on firms in industries covered by the Act); Joseph William Singer, *No Right To Exclude: Public Accommodations and Private Property*, 90 NW. U. L. REV. 1283, 1439 (1996) (describing common law obligations imposed on common carriers).

In addition to there likely being little meaningful process prior to the businesses' decisions to, say, terminate services, the issue of private appropriation of government information—and the effect of that appropriation—also touches upon long-contested questions about what remedies individuals have when the government furthers, but does not carry out or compel, a private injury or deprivation of rights. *Cf., e.g.*, Paul v. Davis, 424 U.S. 693 (1976).

121. *See* Miller, *supra* note 117 (noting businesses' continued reliance on outdated government lists of suspected terrorists that the government itself has since updated, revised, or withdrawn).

122. This concern has been voiced with respect to Internet vigilantes, concerned citizens typically working on their own (i.e., without government support or knowledge) to disable Jihadist Web sites and chat rooms. The Internet vigilantes' efforts have drawn the ire of government officials, who lose access to valuable information when the vigilantes take matters into their own hands and shut down sites that are, oftentimes, already carefully being monitored by the intelligence agencies. For a more extensive discussion, see *infra* notes 124–25.

123. *Cf.* George A. Akerlof, *The Market for "Lemons": Quality Uncertainty and the Market Mechanism*, 84 Q.J. ECON. 488, 493–94 (1970).

undermine security policy. Specifically, responsible actors (ordinarily, the very ones we want heeding the deputization call) will be risk adverse in light of this uncertainty and commit only modestly and tentatively. Risk-seeking, perhaps even reckless, actors will, on the other hand, be far less deterred by the potential liabilities incident to deputization, and this group might come to occupy a disproportionately large and active segment of the deputy pool. In the case, say, of doormen or repairmen, the careful, cautious employees may forswear or shirk deputy responsibilities precisely because their snooping around might subject them to legal liability or even physical retaliation. Those with more bravado and fewer reservations would push forward, not only willing to search and investigate, but also willing to search and investigate in a relatively aggressive fashion.[124] As a substantive matter, this

124. Perhaps an extreme version of the risk-seeking deputy is the vigilante. We have seen private individuals and groups decide, on their own initiative, to insert themselves into the world of deputization and into this hybridized space. Among them are the civilian border patrols that have begun organizing, monitoring and, at times, capturing and detaining those trying to enter the country illegally. These groups, which include the Minutemen, are often motivated largely by anti-immigrant sentiments having mostly to do with economics and culture, by worries that terrorists are sneaking into the country through porous borders, and by their belief that the U.S. Border Patrol is ill-equipped or ill-disposed to stop them. Accordingly, various militia groups have staged public demonstrations and set up armed outposts in Arizona and California, as well as along the nation's northern border with Canada. *See* David A. Fahrenthold, *On Patrol in Vt., Minutemen Are the Outsiders*, WASH. POST, Oct. 31, 2005, at A2 (reporting on the New England branch of the Minutemen); Anna Gorman, *Volunteers To Patrol Border Near San Diego*, L.A. TIMES, May 5, 2005, at B1 [hereinafter Gorman, *Volunteers*] (attributing the upswing in volunteer border patrol membership in part to the members' perception that the Bush Administration was failing to secure the nation's borders); Michael Leahy, *Crossing the Line*, WASH. POST, Mar. 19, 2006, (Magazine), at 14 (chronicling efforts by private anti-immigration groups to mount border patrols and monitor labor sites suspected of employing undocumented aliens). Such groups have been criticized and labeled "vigilantes" by the likes of then-President George W. Bush for their excessive use of violence and their interference with the official Border Patrol operations. Leslie Berestein, *Legal Groups to Watch County "Minutemen*," S.D. UNION-TRIB., July 1, 2005, at B4; Anna Gorman, *Patrol Delays Launch*, L.A. TIMES, June 9, 2005, at B6. But, Governor Schwarzenegger of California and even Bush's own chief immigration enforcement official have expressed greater enthusiasm for their efforts. *See* Gorman, *Volunteers*, *supra* (noting Governor Schwarzenegger's support for the Minutemen group, which he said had "done a terrific job" in contrast to the federal government that was "not doing [its] job"); Solomon Moore, *Immigration Official Praises Citizen Patrols*, L.A. TIMES, July 21, 2005, at B6 (reporting on then-Customs and Border Protection Commissioner Robert Bonner's praise of citizen patrols on the U.S.–Mexico border).

A second group is the so-called Internet vigilantes, who were briefly mentioned above. *See supra* notes 15, 122. Some Internet watchdogs go no further than alerting the government to the existence (and substantive content) of extremist Web sites. *See, e.g.*, Erika Hayasaki, *Tracking Terrorists from Her Home Computer*, L.A. TIMES, Jan. 11, 2009, at A17; Nadya Labi, *Jihad 2.0*, ATLANTIC MONTHLY, July–Aug. 2006, at 102; Benjamin Wallace-Wells, *Private Jihad*, NEW YORKER, May 29, 2006, at 28. Others take it a step or two further. Among this cohort is Internet Haganah, an organization with a moniker that harkens back to the Jewish paramilitary group operating under the British mandate in Palestine prior to Israeli independence. Haganah takes a more activist approach, committing itself to monitoring and *disabling* Jihadist Web sites. Typically, Haganah is able to disable a Web site by overloading the servers or by pressuring the Web sites' Internet service providers to take down the site. Howard Altman, *Web Warriors Track Down, Close Jihadist Internet Sites*, TAMPA TRIB., Nov. 17, 2005, at 12; Michael Snider, *On Osama's Trail*, MACLEAN'S, Nov. 15, 2004, at 94.

phenomenon seems to make deputization less attractive to at least some government officials. The "responsible" would-be participants retreat, and the most aggressive participants dominate the landscape—potentially sapping resources as government officials must keep a close watch on them to make sure they do not harass suspects or otherwise frustrate ongoing investigations by dispensing their own forms of justice (on their own timetables).[125]

4. De Facto State-Action Challenge: The Legal Regime's Uncertainty in Distinguishing Deputies from Nondeputized Civilians.—As stated above, there is more to deputization than its force-multiplying effects. Of seemingly greater practical and normative purchase than deputization's force multiplication is deputization's leveraging of the private sector to gain faster, deeper, or less legally encumbered access to people, places, and data. That is to say, faster, deeper, or less legally encumbered than what the government could do were it limited to using its own personnel.

The private sector's comparative advantage is an artifact of a predeputized landscape.[126] In some important respects, private actors' conduct is not subject to as strict regulatory, statutory, or constitutional limitations. In part this is because private actors are not assumed to be exercising

---

125. As one terrorism expert, expressing concerns with the counterproductive role being played by Internet vigilantes, notes:

> From a law enforcement perspective, it is better to keep those sites online. If you really want to shut them down, don't go after some pimply faced Web master, who is a low-level member. Do what you do in a mafia case. Pull in the small guy to reel in bigger fish.

Altman, *supra* note 124, at 12; *see also* Cha, *supra* note 30 (quoting a federal official who called Haganah "a grave threat to national security"); Snider, *supra* note 124, at 94 (characterizing the work of Haganah and others as "hacktivism" and counterproductive); Carmen Gentile, *Cyber Vigilantes Track Extremist Web Sites, Intelligence Experts Balk at Effort*, FOXNEWS.COM, Mar. 22, 2008, http://www.foxnews.com/story/0,2933,340613,00.html (citing experts' frustration with Internet vigilantes for interfering with government investigations); Brad Stone, *Heroes or Nettlesome Hacks?*, NEWSWEEK.COM, July 2005, http://www.newsweek.com/id/50330 (noting the Intelligence Community's annoyance over vigilantes' efforts that "scuttle ongoing surveillance . . . and eventually force terrorists to find less observable ways of spreading their message").

Likewise, concerns have been raised regarding the counterproductive and abusive role played by private border patrols. *See, e.g.*, Randal C. Archibold, *A Border Watcher Finds Himself Under Scrutiny*, N.Y. TIMES, Nov. 24, 2006, at A1 (reporting on allegations that a self-appointed border patrolman in Arizona falsely imprisoned, threatened, and physically abused undocumented aliens as well as lawful U.S. residents who he assumed entered the country illegally); Tim Gaynor, *Border Vigilantism Alleged in Ariz. Case: Rancher Accused of Holding Mexican American Family at Gunpoint*, WASH. POST, Nov. 15, 2006, at A3 (highlighting the increase in "vigilante violence" along the U.S.–Mexico border); Jesse McKinley & Malia Wollan, *New Border Fear: Violence by a Rogue Militia*, N.Y. TIMES, June 27, 2009, at A9 (discussing border violence believed to be perpetrated by members of the Minutemen militia); *see also* Nick Madigan, *Police Investigate Killings of Illegal Immigrants in Arizona Desert*, N.Y. TIMES, Oct. 23, 2002, at A15 (discussing the accusation that a militia group funds its border-patrol activities by robbing drug dealers).

126. It is probably more accurate to say the artifact of a preprivatized landscape. *See, e.g.*, Michaels, *supra* note 20.

or facilitating state power.[127] By contrast, the ordinarily more stringent rules placed on government actors may be justified precisely in terms of the apprehensions associated with their capacity to exercise state sovereignty. Amazon.com can do a lot with the information it gathers. It can botch your order, improperly customize your "favorites" settings, sell information about your preferences to marketers or other retailers, and even reveal your credit card information. But—unlike the State—it is not capable of using that information to order criminal investigations, terminate government benefits, or designate you as a suspicious person. Given the relative innocuousness of private power (not to mention the commercial benefits to firms and customers alike that come with businesses trafficking in consumers' personal information), there are legitimate reasons not to overly limit the ability of private actors to collect, analyze, and even sell personal information.[128]

Deputization thus comes as a wolf in sheep's clothing and creates problems for the durability of this private–public distinction.[129] But, for now, so long as deputization has taken root and these legal distinctions perdure, opportunities for exploitation abound. Using private proxies increases the government's legal scope of counterterrorism activities.[130] For example, FedEx may in its ostensibly private capacity open customers' packages. A

127. *See, e.g.*, NCAA v. Tarkanian, 488 U.S. 179, 191 (1988) ("Embedded in our Fourteenth Amendment jurisprudence is a dichotomy between state action, which is subject to strict scrutiny . . . and private conduct, against which the Amendment affords no shield, no matter how unfair that conduct may be.").

128. *See* James P. Nehf, *Recognizing the Societal Value in Information Privacy*, 78 WASH. L. REV. 1, 13 (2003) (noting that businesses that collect information are "looking for better and more efficient ways" to operate); Anita Ramasastry, *Data Mining, National Security and the "Adverse Inference" Problem*, 22 SANTA CLARA COMPUTER & HIGH TECH. L.J. 757, 758 (2006) (stating that the collection of personal data by businesses helps "to maximize profit and to improve consumer experience"); *see also* Stan Karas, *Privacy, Identity, Databases*, 52 AM. U. L. REV. 393, 415 (2002) (noting the public's willingness to disclose personal information to businesses to facilitate commercial endeavors); Declan McCullagh, *It's Been 10 Years: Why Won't People Pay for Privacy?*, CNET NEWS, Jan. 28, 2010, http://news.cnet.com/8301-13578_3-10443575-38.html (describing studies indicating that people readily disclose personal information, including passwords, in exchange for nominal commercial benefits).

129. Needless to say, deputization is hardly the only phenomenon that creates problems for the durability of private–public distinction. For example, some instances of government contracting do as well. *See, e.g.*, Jody Freeman, *Extending Public Law Norms Through Privatization*, 116 HARV. L. REV. 1285, 1289–90 (2003); Minow, *supra* note 10, at 994–95.

130. Deputization is not novel here. Far from it. Landmark cases have long allowed third-party transfers of information to the government in the absence of the target's express consent. Smith v. Maryland, 442 U.S. 735, 743–45 (1979); United States v. Miller, 425 U.S. 435, 440–41 (1976); *see also* United States v. Matlock, 415 U.S. 164, 171 (1974) ("[C]onsent of one who possesses common authority over premises or effects is valid as against the absent, nonconsenting person with whom that authority is shared."); Coolidge v. New Hampshire, 403 U.S. 443, 484–90 (1971) (holding that a wife could search and seize her husband's property and voluntarily turn it over to the police absent a warrant). What is important with respect to the homeland security deputies is the greater potential for institutionalizing these relationships—that is, not just the occasional call by the authorities to the bank for third-party records or the sporadic request made to spouses or other household residents by police and prosecutors to obtain information absent warrants or express consent, but instead the systematic harnessing of private resources in service of long-term relationships.

FedEx–government operation might not trigger the same constitutional warrant requirements that attach where government officials directly seek such access. This is because state action is not consistently ascribed to private parties, even those working with the government.[131] To date, the applicability of the Fourth Amendment to nongovernmental personnel tends to be limited to situations where the private party is acting as an agent of, or in conjunction with, the police.[132] Depending on how the FedEx–government arrangement is actually structured,[133] there may be opportunities to *encourage*—rather than *direct*—FedEx activism that leads the company to exercise ostensibly independent judgment in opening up suspicious packages. That is, unlike an unambiguous agent of the government, FedEx's status as an occupier of amorphous public and private space—and as a business still looking out for its own commercial interests (when it, among other things, decides to seize packages)—may create enough of a break from the state-action nexus to permit it to act without the attendant constitutional liability.[134]

---

131. *See, e.g.*, Correctional Servs. Corp. v. Malesko, 534 U.S. 61, 63 (2001) (declining to recognize a *Bivens* claim against a private prison facility operating pursuant to a federal contract); Rendell-Baker v. Kohn, 457 U.S. 830, 843 (1982) (refusing to allow a § 1983 suit to lie against a private school funded almost entirely by government to educate "maladjusted" students). *But see* Lugar v. Edmondson Oil Co., 457 U. S. 922, 936–37 (1982) (authorizing a § 1983 suit against a private firm acting jointly with the Commonwealth of Virginia in exercising "state action").

132. *See* United States v. Jacobsen, 466 U.S. 109, 113 (1984) ("This Court has . . . consistently construed [Fourth Amendment] protection as proscribing only governmental action; it is wholly inapplicable to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government or with the participation or knowledge of any governmental official." (internal citations omitted)); s*ee also* United States v. Momoh, 427 F.3d 137, 141 (1st Cir. 2005) (considering for purposes of determining constitutional liability the government's role in instigating or directing the private search, the government's control over the private actor's search, and whether the private actor is primarily aiding the government or furthering its own objectives); 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) (listing among the factors to be considered in determining whether a private citizen was acting as an agent of the government "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").

133. *See* Block, *supra* note 7; Fields, *supra* note 100; Siemaszko, *supra* note 88, at 24. As mentioned above, both UPS and the Postal Service have refused entreaties to provide law enforcement and intelligence agencies with similar assistance. *See supra* note 88 and accompanying text.

Coincidentally, *Jacobsen* involved FedEx employees opening a package, finding contraband, and reporting their discovery to law enforcement officials—all without triggering a Fourth Amendment violation. 466 U.S. at 111, 114–17.

134. *See, e.g.*, United States v. Hall, 142 F.3d 988, 995 (7th Cir. 1988) (holding that an independent search by a computer repair firm that led the firm to contact authorities did not implicate the Fourth Amendment); *see also* Simmons, *supra* note 98, at 986–87 (describing informal private–public cooperation on searches that led to criminal prosecution). *But see* United States v. Walther, 652 F.2d 788, 793 (9th Cir. 1981) (finding state action in an airline-carrier search

Similarly, government partnerships with the private sector create a channel that enables the bypassing of otherwise applicable statutory restrictions on the gathering of personal information. For example, certain foundational federal privacy laws focus primarily on limiting what the government can acquire.[135] With the exception of a few named industries expressly included in the statutes' coverage, private actors are unencumbered by such laws and can acquire the information and freely pass it on to the government.[136] A private–public partnership thus gives the government access to more expansive searches than would be permissible were the government forced to rely exclusively on its own personnel.[137]

In terms of physical surveillance, the deputization of workers might give the government greater warrantless entrée to private space. Cable repairmen are admitted where the police likely are refused, presumably on the reasonable understanding that the repairmen's purpose is to install HBO, not scope out the living room for Jihadist literature. This isn't a legal evasion per se, because a police officer invited to enter a home could just as readily scan the bookshelves in search of militant tracts.[138] But it is far more likely that a resident will freely admit a cable repairman into her home but not a police officer. The greater comfort with the technician is predicated in part on the desire to have a commercial service performed, and in part on perhaps now-naive and outdated assumptions about status—about the ostensibly exclusive business nature of the technician's visit, and about the technician's ostensibly limited ability to generate law enforcement problems for the resident.[139]

Deputization in these contexts changes the nature of consent. As suggested, surely the government could similarly bypass the extant legal limitations on opening packages, acquiring data, or entering homes by first obtaining permission from the package senders or recipients, from those whose data is sought, and from the residents whose homes it wants to search. But, with deputies, a different, easier brand of consent can be obtained. Consent is displaced onto third parties—the volunteer firms and employees—

---

where the government "had knowledge of a particular pattern of search activity . . . and had acquiesced in such activity").

135. *See, e.g.*, Privacy Act of 1974, 5 U.S.C. § 552a (2006).

136. *See* Danielle Keats Citron, *The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. CAL. L. REV. 241, 255 (2007). Citron notes that "the private sector's collection of sensitive personal information remains largely unregulated by federal law. While federal legislation governs the security of personal data stored by federal agencies, similar federal restrictions apply only to a narrow set of private entities, such as financial institutions, credit agencies, and health care providers." *Id.*; *see* Michaels, *supra* note 20, at 721–23; Michaels, *supra* note 9, at 908–09 & n.23 (2008); *see also* Daniel J. Solove & Chris Jay Hoofnagle, *A Model Regime of Privacy Protection*, 2006 U. ILL. L. REV. 357, 365–67 (describing how statutory restrictions imposed on the government when collecting data covered under the Privacy Act of 1974 and the Fair Credit Reporting Act of 1970 can be bypassed if information is first privately gathered).

137. *See* Michaels, *supra* note 20, at 741–42.

138. The observation of what might be considered suspicious materials is likely to prompt, if anything, additional surveillance or investigatory work, rather than an actual, immediate seizure.

139. *See supra* note 18 and accompanying text.

who likewise must be convinced to accede to the government's request. The convincing is far easier, however, given that these third parties, unlike the suspects, do not personally bear the brunt of the costs of the invasion or encroachment.

Leveraging the private sector in this respect no doubt increases the number and severity of privacy encroachments.[140] But this practice has broader consequences as well. The first such consequence has to do with private–public relationships writ large and the law's uncertainty vis-à-vis occupants of this dualist space; that is, deputies straddling the private–public divide work in the interstices of legal rules that assume—perhaps too readily—a more complete divide between private and public action. Thus, the deputization relationships blur the boundary of state action. They complicate the roles and responsibilities not only of deputies but also other private actors assisting the government in various capacities.[141] The second consequence has to do with the Executive Branch's ability to deploy private-sector resources in efforts to overcome restrictions placed by Congress and the courts on its (public) power.[142] We typically think of outsourcing and reliance on the private sector as the government *ceding* sovereignty and abrogating its own authority.[143] In practice, however, elements of deputization are clearly power aggrandizing to Executive Branch officials and implicate important separation of powers concerns.[144]

III. Situating Deputization

Having described deputization practices and examined some challenges brought about by these distinctively underregulated collaborations, this Part offers three concluding discussions.

A. Contemporary Analogues

First, deputization is not unique to homeland security. Besides its historical forerunners noted above,[145] there are contemporary analogues in more conventional areas of law enforcement as well as in other contexts entirely

---

140. *See supra* note 92.

141. An obvious set of private actors potentially affected by such line-blurring is government contractors. Contracting out for government services is so pervasive today that the annual expenditures for contractors at the federal, state, and local levels combined is now in excess of $1 trillion. Jeffrey L. Dunoff, *Linking International Markets and Global Justice*, 107 MICH. L. REV. 1039, 1041, nn.5–6 (2009).

142. We see similar efforts outside of the intelligence-gathering context as well. *See* Michaels, *supra* note 10; *see also* Matthew Diller, *The Revolution in Welfare Administration: Rules, Discretion, and Entrepreneurial Government*, 75 N.Y.U. L. REV. 1121, 1182–83 (2000).

143. *See* VERKUIL, *supra* note 10, at 102–14; Gillian E. Metzger, *Privatization as Delegation*, 103 COLUM. L. REV. 1367, 1400–06 (2003).

144. *Cf.* Michaels, *supra* note 20 *passim* (addressing this claim in the context of government contractors).

145. *See supra* notes 21–22 and accompanying text.

divorced from criminal justice and national security. In the law enforcement setting, the largely opaque, unregulated police practice of employing informants to provide tips, assist in sting operations, and elicit confessions and other admissions is not altogether unlike the homeland security deputization protocols. Though their employment has long vexed legal analysts,[146] informants continue to occupy dualist space—certainly not police, but something more than (or different from) civic-minded citizens.[147] For their cooperation, informants may receive benefits in the form of monetary compensation,[148] more lenient sentencing for their own infractions, or outright immunity for past or ongoing criminality.[149] The analogy isn't perfect, however. The lack of clear standards for regulating the informants' role in matters of criminal justice might not be readily attributable to emergency conditions, which are often invoked as a justification for the ad hoc nature of some post-9/11 counterterrorism practices.[150] Nor might the explanation for the general failure to regulate informants in a systematic fashion—or for the related reluctance to make the informant agreements more transparent—be as easily grounded in the need for secrecy as is the case with homeland security deputization. Important as it likely is to conceal the identities of individual informants in active criminal investigations (at least for some stretch of time), there nevertheless seems to be comparatively little need to conceal informant programs' goals and protocols in the same way that counterterrorism agencies must protect their "sources and methods."[151]

A variant of deputization seems to have arisen in another contemporary context: in efforts to manage the global financial meltdown of 2008. Numerous reports have pointed to a series of meetings where top government officials sat down with the titans of Wall Street, and—at times, without clear

---

146. *See, e.g.*, George C. Harris, *Testimony for Sale: The Law and Ethics of Snitches and Experts*, 28 PEPP. L. REV. 1, 57 (2000); Alexandra Natapoff, *Snitching: The Institutional and Communal Consequences*, 73 U. CIN. L. REV. 645 (2004); Daniel Richman, *Cooperating Defendants: The Costs and Benefits of Purchasing Information from Scoundrels*, 8 FED. SENT'G REP. 292 (1996); Ian Weinstein, *Regulating the Market for Snitches*, 47 BUFF. L. REV. 563, 564–65 (1999); Mark Curriden, *The Informant Trap: Secret Threat to Justice*, NAT. L.J., Feb. 20, 1995, at A1.

147. *See* Natapoff, *supra* note 146, at 675 n. 140 (emphasizing that in the majority of cases surveyed "courts find that informant activities take place at arms length from government handlers and therefore do not qualify as state action"). *But see* Arizona v. Fulminante, 499 U.S. 279, 287–88 (1991) (finding a jailhouse informant working with FBI to have engineered a coerced confession).

148. Curriden, *supra* note 146.

149. *See* Natapoff, *supra* note 146, at 653.

150. *See* Adrian Vermeule, *Emergency Lawmaking After 9/11 and 7/7*, 75 U. CHI. L. REV. 1155, 1164, 1175–76 (2008) (emphasizing that lawmakers faced with the uncertainties associated with still-evolving emergencies cannot foresee how events will unfold and thus tend to give the Executive broad, open-ended discretion and flexibility to confront both likely and unexpected challenges).

151. *See* CIA v. Sims, 471 U.S. 154, 167 (1985) (describing "'sources and methods'" as the "heart of all intelligence operations"); Webster v. Doe, 486 U.S. 592, 604 (1988) (noting the extraordinary need in the intelligence context "for confidentiality and the protection of . . . methods, sources, and mission").

legal authority—proceeded to request, pressure, and conscript America's bankers to help stabilize the markets in a variety of ways.[152] The government officials struck deals,[153] engaging in freewheeling negotiations, exacting concessions, and conditioning government bailouts on managerial control (or input in executive decisions), all the while emphasizing the need for firms to think beyond the immediate financial interests of their specific principals and work generally to avoid economic chaos and panic.[154] Whereas the deputization here looks quite different from what we see in the counterterrorism and law enforcement contexts, this is another manifestation of private–public regulation and coordinated action outside the scope of traditional administrative law or contractual channels:[155] the legal uncertainties,[156] the demands of crisis management,[157] the procedural informality associated with how the government approaches various private actors,[158] and the market distortions that might be generated (even if the distortions are "corrective")[159] all suggest an important linkage in terms of the benefits and challenges of private–public partnerships hatched on the fly. More problematic in this context than perhaps others, the ad hoc negotiations might be viewed as especially disconcerting given the appearance of

152. *See* James B. Stewart, *Eight Days: The Battle To Save the American Financial System*, NEW YORKER, Sept. 21, 2009, at 59, 67–68 (describing pressure the SEC and Treasury placed on Lehman Brothers regarding the timing of its bankruptcy filing); *see also* Ben Hallman, *A Moment's Notice for Lehman*, AM. LAW., Dec. 1, 2008, at 87, 88 (reporting that government officials urged Lehman Brothers to file for bankruptcy protection at a specific time because it was a "critical part of a program [the government] wanted to roll out").

153. *See* Steven Davidoff & David Zaring, *Regulation by Deal*, 61 ADMIN. L. REV. 463, 466–68, 493–512 (2009).

154. *See* ANDREW ROSS SORKIN, TOO BIG TO FAIL 401–03 (2009) (noting the government's demand that AIG executives resign as a condition of the federal government bailing out the company); James Bandler, *Hank's Last Stand*, FORTUNE, Oct. 7, 2008, at 112. *See generally* U.S. GOV'T ACCOUNTABILITY OFFICE, TROUBLED ASSET RELIEF PROGRAM: THE U.S. GOVERNMENT ROLE AS SHAREHOLDER IN AIG, CITIGROUP, CHRYSLER, AND GENERAL MOTORS AND PRELIMINARY VIEWS ON ITS INVESTMENT MANAGEMENT ACTIVITIES 10–15 (2009) (describing the government's management of its equity stakes in bailed-out corporations).

155. *See* Davidoff & Zaring, *supra* note 153, at 468 ("[T]he government structured deals that pushed its legal authority to the very edge and beyond in pursuit of, and bound by, its own political, economic, and, perhaps, sociological interests."); *id.* at 535–36 (noting the government's departure from traditional administrative law practices throughout the financial-crisis negotiations).

156. *See id.* at 468. *But see* Eric A. Posner & Adrian Vermeule, *Crisis Governance in the Administrative State: 9/11 and the Financial Meltdown of 2008*, 76 U. CHI. L. REV. 1613, 1638 (2009) (noting that the bailouts were rendered pursuant to existing statutory authority for the government to extend loans to institutions "whose failure threatens the health of the financial system").

157. *See generally* Posner & Vermeule, *supra* note 156.

158. *See* Stewart, *supra* note 152, at 72; *see also* Richard W. Painter, *Bailouts: An Essay on Conflicts of Interest and Ethics when Government Pays the Tab*, 41 MCGEORGE L. REV. 131, 142 (2009) (characterizing "[t]he apparent arbitrariness of bailout decisions in 2008 and 2009").

159. *See* Brady Dennis, *Fed Criticized for Not Negotiating Harder with AIG*, WASH. POST, Nov. 17, 2009, at A24; Joe Nocera, *Lehman Had To Die, It Seems, So Global Finance Could Live*, N.Y. TIMES, Sept. 12, 2009, at A1 (noting the apparent dissimilar treatment Lehman Brothers received vis-à-vis other firms that the government helped prop up).

conflicts of interest between high-ranking government officials and the private financial institutions, firms where some of the chief government decisionmakers previously worked and where they might seek employment after completing their public service.[160]

B. Legal Certainty's Challenges

Second, though legal uncertainty introduces or exacerbates the challenges considered in Part II, it is not clear that the converse—legal certainty—would necessarily be a categorical improvement. Some of the uncertainty that attaches to a regime of unregulated or underregulated practices in homeland security is inevitable. After all, we might be hard-pressed to design a system that creates a *third* legal regime (i.e., neither private nor state actor) for all deputies, across the board. Such a system might make sense with respect to telecom workers essentially embedded with the FBI on long-term assignments,[161] but not vis-à-vis, say, deputized truckers, any one of whom will, in all likelihood, never actually witness a terrorism-related suspicious activity. Moreover, whatever this third, hybrid regime might look like for deputies facilitating government operations, it would assuredly create new line-drawing problems, even if it were to resolve the ones discussed in Part II.

Nor would a system that imposed greater legal requirements on the private sector necessarily be welcomed (even if it is clarifying). For instance, the non-statutory, ostensibly voluntary practices described above permit deputies a modicum of choice in terms of whether and how to participate. This is true especially where the government isn't applying coercive pressure on would-be deputies to get involved. Where partnerships are open-ended and voluntary, the deputies likely view their efforts as public service rather than regulatory conscription. That service orientation might be considerably more civically meaningful, and politically legitimate, to the participants.[162] In addition, legislation and regulatory rules are sticky. There

---

160. *See* Painter, *supra* note 158, at 140–42 (describing widespread appearances of conflicts of interest); Jim Puzzanghera, *Paulson Takes Heat for Role in Bailouts*, L.A. TIMES, July 17, 2009, at B1 (quoting a member of Congress accusing former-Treasury Secretary Paulson of taking $700 billion and "giv[ing] it to [his] pals"); Andrew Ross Sorkin, *Paulson's Calls to Goldman May Have Tested Ethics*, N.Y. TIMES.COM, Aug. 10, 2009, http://dealbook.blogs.nytimes.com/2009/08/10/paulsons-calls-to-goldman-tested-ethics/ (noting that questions are still being raised about then-Secretary Paulson's participation in decisions "to prop up the teetering financial system with tens of billions of taxpayer dollars, including aid that directly benefited his former firm").

161. *Cf. supra* subpart I(B) (describing long-term, institutionalized deputization relationships between the telecoms and the government).

162. *Cf.* Jody Freeman, *Collaborative Governance in the Administrative State*, 45 UCLA L. REV. 1, 54 (1997) (describing the advantages of labor agreements reached through consensus, as opposed to judicial or agency decree); Philip J. Harter, *Negotiating Regulations: A Cure for the Malaise*, 71 GEO. L.J. 1, 31 (1981) (advocating the use of negotiation in rulemaking because, among other reasons, it adds legitimacy and interest-group "buy in"); Orly Lobel, *The Renew Deal: The Fall of Regulation and the Rise of Governance in Contemporary Legal Thought*, 89 MINN. L.

is the often-voiced complaint that measures enacted during times of emergency are difficult to get off the books, even after the crisis abates. Their effective permanence thus contributes to a one-way ratchet of security measures that persist long beyond the period for which they are needed (and are themselves then augmented when a new threat arises).[163] On the other hand, practices not ossified via statutes and rules might be subject to more rapid termination once the need for private assistance lessens.[164]

C. Distinguishing Acceptable from Unacceptable Deputization Practices

These claims about the potential limitations associated with certainty are not advanced to promote or endorse a brand of purposive uncertainty; rather, they are advanced simply to acknowledge that the (perhaps) intuitively attractive alternative might carry with it no shortage of its own baggage. These claims, coupled with the recognition that deputization implicates policy space far broader than just post-9/11 homeland security efforts, take us to the third discussion: we need to do more careful thinking about the nature of ad hoc deputization arrangements to gauge where they ought to be allowed to continue unaltered (notwithstanding the concomitant legal uncertainties) and where they should be harnessed within a regulatory framework that has a stronger legal foundation. That is a big project, and any comprehensive treatment is beyond the scope of this contribution. Here, however, I will provide preliminary thoughts on how we might go about distinguishing between acceptable and unacceptable deputization practices.

The discussion in Part I, highlighting differences between employee and organizational assistance, provides us with some clues, as do the assessments of the challenges identified in Part II. In thinking more broadly, we might want to build on those understandings, among others, and consider the acceptability of unregulated or underregulated deputization along three

---

REV. 342, 371–404 (2004) (describing a shift in regulatory governance toward a more participatory, collaborative, and flexible decisionmaking model).

163. *See* BRUCE ACKERMAN, BEFORE THE NEXT ATTACK: PRESERVING CIVIL LIBERTIES IN AN AGE OF TERRORISM 2–3 (2006) (noting that emergency measures enacted during a crisis are often not repealed after the crisis abates and indicating that those measures are further supplemented by an additional wave of emergency authorizations when a new crisis arises); Oren Gross, *Chaos and Rules: Should Responses to Violent Crises Always Be Constitutional?*, 112 YALE L.J. 1011, 1090 (2003) ("It is commonplace to find on statute books legislative acts that had originally been enacted as temporary emergency or counterterrorism measures, but that were subsequently transformed into permanent legislation."); *id.* at 1095–96 (describing the ratcheting up of emergency powers as new crises arise); Jules Lobel, *Emergency Power and the Decline of Liberalism*, 98 YALE L.J. 1385, 1397–1421 (1989). *But see* Eric A. Posner & Adrian Vermeule, *Accommodating Emergencies*, 56 STAN. L. REV. 605, 610–26 (2003) (questioning the ratchet theory).

164. Indeed, even if government officials are not inclined to decrease the scope or intensity of operations when the circumstances seem objectively to warrant such downscaling, the private partners might serve as an independent check—refusing to cooperate, or limiting their cooperation, in light of the changed (and seemingly less dire) circumstances. Needless to note, this check is hardly perfect. Among other things, the private partners are not in the best position to make assessments regarding the relevant threats facing the United States.

planes: (1) the interests served by the government's preference for deputization over more conventional, legally grounded forms of private–public cooperation; (2) the compatibility or consistency of the deputization project (and the concomitant legal uncertainties that go along with it) with preexisting legal and institutional norms and understandings; and, (3) the tangible and distributional effects of the deputization arrangements.

With respect to the interests promoted by the government's preference for unregulated or underregulated collaborations, the question is whether an ad hoc arrangement is pursued because it is the most feasible way to proceed, because it is easier than adhering to the alternative, but *feasible*, legal protocols (e.g., warrants, subpoenas, contracts, or regulatory directives), or because proceeding in such a fashion confers an otherwise unobtainable legal advantage to carry out an assignment. Admittedly, there likely will be times when "most feasible" and "easier" blend together, and times when "easier" seems little more than a euphemism for "circumventing the law." Admittedly, too, the prospect of making objective determinations as to what is driving an arrangement is a daunting one. But for purposes of this initial sketch, we can leave those complications to the side and consider the legitimacy of a deputization program as a function of whether the non-statutory, non-regulatory arrangement is practical, reasonable, and perhaps necessary, or whether it is structured that way to enable an apparent power grab.[165]

With respect to the issue of fidelity to or consistency with preexisting understandings, the question is how much of a departure are the deputies' roles—vis-à-vis both the government and their commercial clients—from those the corporations and corporate employees played prior to entering into the hybridized space. In other words, what were the legal and social expectations absent deputization? For instance, some private actors already have preexisting relationships with law enforcement, relationships that stem from legal requirements or professional obligations.[166] Duties of certain medical professionals to report instances of suspected domestic violence[167] or of lawyers and psychologists to take steps if they think their clients are about to commit violent acts come to mind as some additional examples.[168] By

165. I address similar questions with respect to privatization and the contracting out of government responsibilities in Michaels, *supra* note 20.

166. *See, e.g.*, Bank Secrecy Act of 1970, 31 U.S.C. §§ 5311–5330 (2006) (requiring banks to maintain specific records for use in criminal, tax, and regulatory investigations and proceedings and to file Suspicious Activity Reports, or SARs).

167. *See, e.g.*, Lois A. Weithorn, *Protecting Children from Exposure to Domestic Violence: The Use and Abuse of Child Maltreatment Statutes*, 53 HASTINGS L.J. 1, 28 (2001) (referencing various reporting requirements for medical personnel).

168. *See* Tarasoff v. Regents of Univ. of Cal., 551 P.2d 334, 348 (Cal. 1976) (acknowledging affirmative duties for mental-health practitioners to recognize patients' violent inclinations and to take steps to prevent the patients from acting on those inclinations); MODEL CODE OF PROF'L RESPONSIBILITY DR 4-101(C) (1980) (permitting attorney disclosure of confidential communications with a client in order to help prevent crime); *see also* Stephen Gillers, *A Duty To Warn*, N.Y. TIMES, July 26, 2001, at A25.

contrast, the baseline understandings regarding the professional and legal duties imposed on (or embraced by) service technicians or building supervisors upon entering the homes of their customers or tenants might be very different.[169] Moreover, where government interactions with certain industries are already relatively free-wheeling and informal (on matters, say, of domestic regulation), opting for homeland security deputization arrangements over statutory or regulatory means of compelling assistance might make considerable sense; where government-industry interactions have largely been at arm's length, however, the introduction of informal homeland security deputization protocols might be quite a departure from past practices. In addition, if firms or industries have a track record of informing their customers in accessible and transparent ways that their privacy is not being safeguarded, that too would suggest less confusion or opportunity for novel exploitation if and when those firms assume roles as full-fledged deputies. Finally, if a deputization relationship were publicly announced—rather than hashed out in secret behind closed doors—even though the deputization program may traffic in legal uncertainties on the ground, there would be a modicum of notice alerting customers (not to mention legislators and judges, too) to adjust to the ensuing practices accordingly. If, on the other hand, deputization appears to be a stark reversal, and undertaken without any public disclosure acknowledging and giving advanced warning of the shift,[170] that might be a basis for looking at the arrangements with greater skepticism, perhaps with a view to impose requirements that increase everyone's legal certainty regarding the relevant practices.

With respect to concerns about deputization's effects on, among other things, homeland security, civil liberties, and private industry, an accounting of the potency of the programs is in order. Potency could be a function of the number of deputies mobilized, and the invasiveness of deputies' reach (in terms of physical space and aggregation of data). Potency might (also or alternatively) reflect the market distortions deputization engenders. Arrangements that turn on coercive, unregulated interactions with firms or industries might invite greater scrutiny than those collaborations that truly are voluntary in nature. Further, a program's potency might be measured in terms of the potential for deputies to act abusively in a given arrangement—and thus be inversely related to how much control the government can exert over their private partners to keep them in line.

This rough sketch cannot fully do justice to the detailed analysis that is required to map out the private–public collaborations along axes that would

169. *See supra* note 18 and accompanying text.

170. *See, e.g.*, *AT&T Revises Privacy Policy for Customer Data*, N.Y. TIMES, June 22, 2006, at C7; Barbara Ortutay, Associated Press, *Facebook Backtracks on Terms of Use After Protests*, LAW.COM, Feb. 18, 2009, http://www.law.com/jsp/article.jsp?id=1202428366838 (describing strong opposition mounted by Facebook users after the social networking site sought to make unilateral and retroactively applicable changes to its user privacy policies).

inform whether regulatory interventions would be helpful in addressing, among other things, exploitative, undemocratic, and counterproductive practices in legally ambiguous deputized space. Nor does it provide foundational benchmarks that would ensure that this scrutiny is not simply ad hoc review of ad hoc arrangements.[171] That said, this sketch offers some analytical and normative tools for recognizing the diversity of deputization practices and thinking carefully about such interventions, principally in the context of homeland security but perhaps more broadly as well. By way of conclusion, as we approach the second decade of what is popularly termed the Global War on Terror, one hopes that this and the related contributions to this Symposium will spark continued debate and further research to address the institutional challenges brought about in the course of mobilizing an effective response to the terrorist threat.

171. Most balancing tests are susceptible to such claims—levied perhaps most forcefully by Justice Scalia—that they are unprincipled and results oriented. *See, e.g.*, Morrison v. Olson, 487 U.S. 654, 734 (1988) (Scalia, J., dissenting) (arguing that the "'totality of the circumstances' mode of analysis . . . is . . . guaranteed to produce a result, in every case, that will make a majority of the Court happy with the law. The law is, by definition, precisely what the majority thinks, taking all things into account, it *ought* to be"); United States v. Mead, 533 U.S. 218, 241 (2001) (Scalia, J., dissenting) (describing "th'ol' 'totality of the circumstances' test" as the "test most beloved by a court unwilling to be held to rules (and most feared by litigants who want to know what to expect)"). While not unpersuasive, the fact of the matter is that the landscape for deputization is quite varied and whatever benefits accompany bright-line rules are more than overshadowed by the costs such an inflexible approach would impose on policymakers or judges. Indeed, the rejoinder to Justice Scalia's broadside in *Mead* is instructive. In noting the diversity of authorized agency activity (ranging from formal adjudication to informal opinion letters), the Court rejected Justice Scalia's *either–or* approach whether to defer to agency interpretations of statutory authority. *Id.* at 235–37. Instead it accepted the patchwork of regulatory actors and activities involved in statutory interpretation and acknowledged that a broad array of factors must be considered in developing a coherent understanding of where—and to what degree—deference ought to be accorded. *See id.* Unless one takes a categorical approach in support of or entirely against a similarly diverse range of deputization arrangements operating in the interstices of the law, then a more nuanced, albeit at times unwieldy, totality-like metric appears warranted here.